Ε Θ Ν Ι Κ Ο Μ Ε Τ Σ Ο Β Ι Ο Π Ο Λ Υ Τ Ε Χ Ν Ε Ι Ο
Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων
Τομεας Μαθηματικων

ΣΥΝΔΥΑΣΤΙΚΗ ΘΕΩΡΙΑ ΣΧΕΔΙΑΣΜΩΝ, ΚΩΔΙΚΩΝ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Διδακτορικη Διατριβη

ΔΗΜΗΤΡΙΟΥ Ε. ΣΙΜΟΥ

ΕΠΙΒΛΕΠΩΝ: ΚΑΘΗΓΗΤΗΣ Χ. ΚΟΥΚΟΥΒΙΝΟΣ

ΑΘΗΝΑ © 2011

Ε Θ Ν Ι Κ Ο Μ Ε Τ Σ Ο Β Ι Ο Π Ο Λ Υ Τ Ε Χ Ν Ε Ι Ο
Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων
Τομεας Μαθηματικων

Συνδυαστική Θεωρία Σχεδιασμών, Κωδίκων και Κρυπτογραφίας

Διδακτορική Διατριβή

Δημητρίου Ε. Σίμου

dsimos@math.ntua.gr

Αθήνα © 2011

Ε Θ Ν Ι Κ Ο Μ Ε Τ Σ Ο Β Ι Ο Π Ο Λ Υ Τ Ε Χ Ν Ε Ι Ο
Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων
Τομεας Μαθηματικων

Συνδυαστική Θεωρία Σχεδιασμών, Κωδίκων και Κρυπτογραφίας

Διδακτορική Διατριβή
Δημητρίου Ε. Σίμου
18 Ιουλίου 2011, Αθήνα

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Χρηστος Κουκουβινος
Καθηγητής Ε.Μ.Π. (Επιβλέπων Καθηγητής)

Αλεξανδρος Παπαϊωαννου
Αναπληρωτής Καθηγητής Ε.Μ.Π. (Μέλος της Τριμελούς Επιτροπής)

Πετρος Στεφανεας
Λέκτορας Ε.Μ.Π. (Μέλος της Τριμελούς Επιτροπής)

Μιχαλης Βραχατης
Καθηγητής Πανεπιστημίου Πατρών

Παναγιωτης Κατερινης
Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών

Παναγιωτης Σταματοπουλος
Επίκουρος Καθηγητής Ε.Κ.Π.Α.

Παναγιωτης-Γεωργιος Τσικουρας
Καθηγητής Πανεπιστημίου Πειραιώς

Στους Γονείς μου

και

στη μνήμη της
Ν. Πάλλα,
Λέκτορα Ε.Μ.Π.

Περιεχόμενα

Πρόλογος - Ευχαριστίες

Η Συνδυαστική Θεωρία Σχεδιασμών αλληλεπιδρά με αρκετές περιοχές των Μαθηματικών, αναφέρουμε ενδεικτικά τη Θεωρία Αριθμών, τη Θεωρία Πεπερασμένων Σωμάτων και τη Γραμμική Άλγεβρα. Οι εφαρμογές της εκτείνονται σε διάφορους εφαρμοσμένους τομείς των επιστημών, όπως είναι για παράδειγμα η Θεωρία Κωδίκων και Κρυπτογραφίας, και η Πληροφορική. Η ραγδαία ανάπτυξη της τεχνολογίας και των ηλεκτρονικών υπολογιστών τις τελευταίες δεκαετίες, σε συνδυασμό με την αλληλεπίδραση των προηγούμενων περιοχών των Διακριτών Μαθηματικών, αξιοποίησε ως επί το πλείστον τη νέα τεχνογωσία που προέκυψε και βελτίωσε τον τρόπο αντίληψης που έχουμε για αυτές τις επιστήμες. Για παράδειγμα, η ασφαλής μετάδοση δεδομένων μέσα από ένα δίαυλο επικοινωνίας και η λήψη φωτογραφιών από το διάστημα, αντικείμενα της Θεωρίας Κωδίκων και της Κρυπτογραφίας, θεωρούνταν σενάριο επιστημονικής φαντασίας μέχρι πριν κάποια χρόνια. Αυτά τα πλεονεκτήματα, δεν μας παρέχονται όμως χωρίς κόστος. Αυτή η ραγδαία ανάπτυξη των Διακριτών Μαθηματικών έφερε και αρκετά ανοιχτά προβλήματα, για τα οποία αναπτύσσονται συνεχώς νέες μεθοδολογίες και βρίσκονται νέες εφαρμογές. Η παρούσα διατριβή, θεραπεύει κάποια από αυτά τα προβλήματα (σίγουρα όχι όλα) μέσω εκτεταμένης μελέτης της Συνδυαστικής Θεωρίας Σχεδιασμών, της Θεωρίας Κωδίκων και της Κρυπτογραφίας.

Ίσως, η πιο σημαντική ηθική ανταμοιβή, κατά τη διάρκεια της συγγραφής αυτής της διδακτορικής διατριβής, είναι ότι τελικά μου δίνεται η ευκαιρία να γράψω το υπόλοιπο μέρος αυτής της ενότητας. Κατά την διάρκεια των διδακτορικών μου σπουδών στο Εθνικό Μετσόβιο Πολυτεχνείο (Ε.Μ.Π.), αρκετοί άνθρωποι συνέβαλαν, ο καθένας με τον τρόπο του, στο να αποκτήσω το μορφωτικό επίπεδο που έχω σήμερα και θα ήθελα σε αυτό το σημείο να τους εκφράσω τις ευχαριστίες μου, με την πεποίθηση ότι φάνηκα αντάξιος των προσδοκιών τους.

Η εκπόνηση αυτής της διατριβής θα ήταν αδύνατη χωρίς τη συμβολή του Επιβλέποντος κ. Χρήστου Κουκουβίνου, Καθηγητή της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π. Η καθοδήγησή του υπήρξε αρωγός στην ερευνητική μου δραστηριότητα, καθώς μέσω των ιδεών, προτάσεων και στοχευμένων παρατηρήσεών του, που μπορούν να βρεθούν με τη μορφή ερευνητικών προβλημάτων στην αρχή κάθε κεφαλαίου της διατριβής, συνέβαλε καθοριστικά στο να εμβαθύνω και να παρουσιάσω αρτιότερα τα ερευνητικά μου αποτελέσματα. Συγχρόνως, η διαρκής υποστήριξη και αδιάκοπη ενθάρρυνση που μου παρείχε αποτέλεσαν κινητήριο μοχλό για την επιτυχή ολοκλήρωση της διατριβής αυτής. Για αυτόν το λόγο, όπως και για τη δυνατότητα που μου έδωσε να ασχοληθώ ερευνητικά με τις δύο μεγάλες επιστημονικές μου αγάπες, τις επιστήμες των Μαθηματικών και της Πληροφορικής, τον ευχαριστώ θερμά.

Τις ευχαριστίες μου θα ήθελα επίσης να εκφράσω στα μέλη της τριμελούς επιτροπής, τον κ. Αλέξανδρο Παπαϊωάννου, Αναπληρωτή Καθηγητή της

Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π. και τον κ. Πέτρο Στεφανέα, Λέκτορα της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π., καθώς και στα υπόλοιπα μέλη της επταμελούς επιτροπής, τον κ. Μιχάλη Βραχάτη, Καθηγητή του Τμήματος Μαθηματικών του Πανεπιστημίου Πατρών, τον κ. Παναγιώτη Κατερίνη, Καθηγητή του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, τον κ. Παναγιώτη Σταματόπουλο, Επίκουρο Καθηγητή του Τμήματος Πληροφορικής & Τηλεπικοινωνιών του Ε.Κ.Π.Α. και τον κ. Παναγιώτη-Γεώργιο Τσικούρα, Καθηγητή του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς, για το χρόνο που αφιέρωσαν στην ανάγνωση της διατριβής, καθώς και για τις χρήσιμες υποδείξεις τους.

Ευχαριστήρια οφείλω προς τον Τομέα Μαθηματικών της Σ.Ε.Μ.Φ.Ε. του Ε.Μ.Π., για τη χορήγηση υποτροφίας από τον Ειδικό Λογαριασμό Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.) του Ε.Μ.Π. κατά την διάρκεια εκπόνησης της διδακτορικής μου διατριβής, υποστηρίζοντας οικονομικά την έρευνά μου.

Επίσης, θα ήθελα να ευχαριστήσω τον κ. Zlatko Varbanov, Assistant Professor του Department of Mathematics & Informatics του Veliko Tarnovo University για την εποικοδομητική συνεργασία σε θέματα Κρυπτογραφίας. Εκφράζω επίσης τις ευχαριστίες μου, στους συναδέλφους, συνεργάτες και φίλους, κ. Παναγιώτη Αγγελόπουλο, διδάκτορα του Ε.Μ.Π., και κα. Άννα Σκούντζου, υποψήφια διδάκτορα Ε.Μ.Π., για την αρμονική συνεργασία, ενθάρρυνση και υποστήριξη, καθώς και για την προσεκτική διόρθωση της παρούσας διατριβής. Τους συναδέλφους και φίλους, κ. Ελευθέριο Λάππα, διδάκτορα Ε.Μ.Π., και κ. Ιωάννη Διαμαντή, υποψήφιο διδάκτορα Ε.Μ.Π., για τις εποικοδομητικές συζητήσεις που είχαμε στα πλαίσια της Κρυπτογραφίας, τον πρώτο χρόνο των διδακτορικών μου σπουδών, και για τη συμπαράσταση και υποστήριξη του, αντίστοιχα.

Ευχαριστίες εκφράζω στους συναδέλφους και φίλους, κ. Γεώργιο Κορμαρή, κ. Ζαφειράκη Ζαφειρακόπουλο, κ. Γεώργιο Μαρκομανώλη και κ. Στυλιανό Ομήρου για την καθημερινή συμπαράσταση, ενθάρρυνση και υποστήριξη, καθόλη τη διάρκεια εκπόνησης αυτής της διατριβής. Τον κ. Ζαφειρακόπουλο, ευχαριστώ επιπρόσθετα για τη βοήθειά του σε θέματα υπολογιστικής πολυπλοκότητας που αφορούν συνδυαστικούς αλγορίθμους.

Ιδιαίτερη μνεία, θα ήθελα να κάνω στο πρόσωπο της κ. Νίκης Πάλλα, Λέκτορα Ε.Μ.Π., αρχικό μέλος της τριμελούς επιτροπής, η οποία δυστυχώς δε βρίσκεται πλέον ανάμεσα μας.

Τέλος, οφείλω να ευχαριστήσω τους γονείς μου, Ευάγγελο και Δέσποινα, για την αμέριστη ηθική συμπαράσταση, υλική υποστήριξη και καθημερινή ενθάρρυνση τους, σε όλη τη διάρκεια των διδακτορικών μου σπουδών και ως ένα ελάχιστο δείγμα ευγνωμοσύνης η παρούσα διατριβή αφιερώνεται σε αυτούς.

Αθήνα 2011 Δημήτριος Ε. Σίμος

Ερευνητικό Έργο

Κατά τη διάρκεια εκπόνησης αυτής της διδακτορικής διατριβής προέκυψαν οι παρακάτω δημοσιευμένες ή προς δημοσίευση επιστημονικές εργασίες, στα ακόλουθα πεδία έρευνας:

Συνδυαστική Θεωρία Σχεδιασμών

- "On the Computation of the Non-Periodic Autocorrelation Function of two Ternary Sequences and its Related Complexity Analysis", (με Χ. Κουκουβίνο). Journal of Applied Mathematics & Informatics **29** (2011), 547–562.

- "Improving the Lower Bounds on Inequivalent Hadamard Matrices through Orthogonal Designs and meta-Programming Techniques", (με Χ. Κουκουβίνο). Applied Numerical Mathematics **60** (2010), 370–377.

- "Inequivalent Hadamard Matrices from Near Normal Sequences", (με Η. Κοτσιρέα και Χ. Κουκουβίνο). Journal of Combinatorial Mathematics and Combinatorial Computing **75** (2010), 105–115.

- "New Classes of Orthogonal Designs and Weighing Matrices derived from Near Normal Sequences", (με Χ. Κουκουβίνο). The Australasian Journal of Combinatorics **47** (2010), 11–20.

- "New Infinite Families of Orthogonal Designs constructed from Complementary Sequences", (με Χ. Κουκουβίνο). International Mathematical Forum. Journal for Theory and Applications **5** (2010), 2655–2665.

- "Further Results on Ternary Complementary Sequences, Orthogonal Designs and Weighing Matrices", (με Χ. Κουκουβίνο). The Australasian Journal of Combinatorics **50** (2011), 97–112.

- "Combinatorial Optimization for Weighing Matrices with the Ordering Messy Genetic Algorithm", (με Χ. Κουκουβίνο). Proceedings of the 10th International Symposium on Experimental Algorithms (SEA '11), Lecture Notes in Computer Science **6630** (2011), pp. 148–156.

Θεωρία Κωδίκων

- "Construction of New Self-dual Codes over GF(5) using skew-Hadamard Matrices", (με Χ. Κουκουβίνο). Advances in Mathematics of Communications **3** (2009), 251–263.
- "Self-dual Codes over Small Prime Fields from Combinatorial Designs", (με Χ. Κουκουβίνο). Proceedings of the 3rd International Conference on Algebraic Informatics (CAI '09), Lecture Notes in Computer Science **5725** (2009), pp. 278–287.
- " MDS and near-MDS Self-dual Codes over Large Prime Fields", (με Η. Κοτσιρέα και Χ. Κουκουβίνο). Advances in Mathematics of Communications **3** (2009), 349–361.
- "Quasi-cyclic Codes from Cyclic-structured Designs with Good Properties", (με Χ. Κουκουβίνο). Discrete Mathematics, Algorithms and Applications **3** (2011), 1–21.

Κρυπτογραφία

- "Encryption Schemes using Plotkin Arrays", (με Χ. Κουκουβίνο). Applied Mathematics & Information Sciences **5** (2011), 500–510.
- "Encryption Schemes based on Hadamard Matrices with Circulant Cores", (με Χ. Κουκουβίνο). Έχει υποβληθεί για δημοσίευση.
- "Hadamard Matrices, Designs and their Secret-sharing Schemes", (με Χ. Κουκουβίνο και Ζ. Varbanov). Proceedings of the 4th International Conference on Algebraic Informatics (CAI '11), Lecture Notes in Computer Science **6742** (2011), pp. 216–229.

Περίληψη

Στη διδακτορική αυτή διατριβή, μελετώνται συνδυαστικές κατασκευές διαφόρων κλάσεων σχεδιασμών καθώς και η ανάπτυξη σχετικών αλγορίθμων που βρίσκουν εφαρμογή στους κλάδους της Θεωρίας Κωδίκων και της Κρυπτογραφίας.

Η διατριβή αποτελείται από τρία μέρη και συνολικά οκτώ κεφάλαια, τέσσερα για το πρώτο μέρος, δύο για το δεύτερο μέρος και δύο για το τρίτο μέρος. Στο πρώτο μέρος της διατριβής, "Συνδυαστική Θεωρία Σχεδιασμών", μελετώνται διάφορα είδη ακολουθιών με σταθερή αυτοσυσχέτιση και συνδυαστικών σχεδιασμών, εισάγονται νέες οικογένειες, αποδεικνύονται ορισμένα θεωρήματα σχετικά με τις αναγκαίες και ικανές συνθήκες ύπαρξης, και υλοποιείται ένα σχετικό λογισμικό για την εύρεση αυτών. Επιπλέον, αναπτύσσεται μια σειρά συνδυαστικών αλγορίθμων βελτιστοποίησης για την εύρεση νέων ακολουθιών και σχεδιασμών. Στο δεύτερο μέρος, "Θεωρία Κωδίκων", μελετώνται ορισμένες ειδικές οικογένειες κωδίκων, όπως είναι για παράδειγμα οι αυτοδυϊκοί και πολυκυκλικοί κώδικες, προτείνονται μέθοδοι κατασκευής αυτών από διάφορες κλάσεις σχεδιασμών, και υλοποιούνται γενετικοί αλγορίθμοι για την εύρεση των τιμών των παραμέτρων τους, στην περίπτωση των πολυκυκλικών κωδίκων. Στο τρίτο και τελευταίο μέρος της διατριβής, "Κρυπτογραφία", προτείνονται κρυπτοσυστήματα ιδιωτικού κλειδιού που προέρχονται από κλάσεις ορθογωνίων σχεδιασμών και κρυπτογραφικά σχήματα διαμοιρασμού μυστικού μηνύματος που κατασκευάζονται με τη χρήση σχεδιασμών Hadamard.

Συγκεκριμένα στο πρώτο κεφάλαιο παρουσιάζεται μια νέα μέθοδος υπολογισμού της συνάρτησης αυτοσυσχέτισης για συμβατές ακολουθίες. Με βάση αυτήν τη μέθοδο, σχεδίαστηκαν συνδυαστικοί αλγορίθμοι για τον έλεγχο της προαναφερθείσας συνάρτησης και μελετήθηκε η υπολογιστική πολυπλοκότητα χείριστης περιπτώσεως. Αποδεικνύεται ότι η νέα μέθοδος είναι ιδιαίτερα αποδοτική για ακολουθίες μικρού βάρους.

Στο δεύτερο κεφάλαιο παρουσιάζεται η κατασκευή νέων μη-ισοδύναμων πινάκων Hadamard από συμπληρωματικές ακολουθίες και ορθογώνιους σχεδιασμούς. Για την εύρεση των μη-ισοδύναμων πινάκων αναπτύχθηκε κατάλληλο λογισμικό, το οποίο διέπεται από διάφορες αυτοματοποιήσεις κάνοντας χρήση προχωρημένων υπολογιστικών τεχνικών. Επιπλέον, παρουσιάζεται μια πλήρης ταξινόμηση σχεδόν-κανονικών ακολουθιών για πρώτη φορά και αντίστοιχα μελετάται η παραγωγή μη-ισοδύναμων πινάκων Hadamard με τη χρήση του προηγούμενου λογισμικού. Οι νέοι μη-ισοδύναμοι πίνακες έχουν αποθηκευτεί σε μια βάση δεδομένων κατάλληλη για χρήση στο υπολογιστικό πακέτο, Magma.

Στο επόμενο κεφάλαιο, αποδεικνύονται θεωρήματα που αφορούν την κατασκευή νέων ορθογώνιων σχεδιασμών από διάφορες κλάσεις συμπληρωματικών ακολουθιών. Ιδιαίτερα, αποδεικνύεται η σχέση μεταξύ σχεδόν-κανονικών και κατευθυνόμενων ακολουθιών και η οποία παίζει καθοριστικό ρόλο στην κατασκευή ορθογώνιων σχεδιασμών τριών και τεσσάρων μεταβλητών. Επιπλέον, νέοι ορθογώνιοι σχεδιασμοί κατασκευάζονται από ακολουθίες με μηδενική αυτοσυσχέτιση και ακολουθίες Golay. Ιδιαίτερα, νέες άπειρες οικογένειες πινάκων στάθμισης παράγονται από τις προηγούμενες κλάσεις συμπληρωματικών ακολουθιών και οι οποίες ανανεώνουν το Εγχειρίδιο των Συνδυαστικών Σχεδιασμών (Handbook of Combinatorial Designs) σε πολλές περιπτώσεις. Στο τέλος αυτού του κεφαλαίου, εισάγεται ένα νέο κριτήριο για τριαδικές ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης, η ζ-αποδοτικότητα, και αποδεικνύονται διάφορες ιδιότητές της. Στη συνέχεια, με την εφαρμογή της ζ-αποδοτικότητας αποδεικνύεται ένα νέο πολλαπλασιαστικό θεώρημα για ακολουθίες με μηδενική περιοδική συνάρτηση αυτοσυσχέτισης και μελετώνται οι συνέπειες του στη Θεωρία Σχεδιασμών.

Στο τέταρτο και τελευταίο κεφάλαιο του πρώτου μέρους, αναπτύσσονται εξελικτικοί αλγόριθμοι βελτιστοποίησης τελευταίας γενιάς για διάφορες κλάσεις σχεδιασμών. Ιδιαίτερα, παρουσιάζονται για πρώτη φορά εξελιγμένοι γενετικοί αλγόριθμοι για την κατασκευή και εύρεση νέων πινάκων στάθμισης. Η μοντελοποίηση του προβλήματος αυτού, ως προβλήματος συνδυαστικής βελτιστοποίησης κατέστη δυνατή με τη χρήση της νέας μεθόδου υπολογισμού της συνάρτησης αυτοσυσχέτισης που δόθηκε στο πρώτο κεφάλαιο. Η εφαρμογή αυτή συνεισφέρει στον αποδοτικό σχεδιασμό των αλγορίθμων καθώς οι ακολουθίες χρησιμοποιούνται ως ένα ενδιάμεσο βήμα στην κατασκευή των πινάκων στάθμισης.

Στο πέμπτο κεφάλαιο προτείνονται νέες μέθοδοι κατασκευής αυτοδυϊκών κωδίκων πάνω από το $GF(p)$ με τη χρήση πινάκων skew-Hadamard. Παρουσιάζεται μια πλήρης μελέτη αυτοδυϊκών κωδίκων πάνω από μικρά πεπερασμένα σώματα, για $p = 3, 5, 7$ κάνοντας χρήση των γνωστών μη-ισοδύναμων πινάκων skew-Hadamard για διάφορες τάξεις μέχρι 28. Βρίσκονται νέοι αυτοδυϊκοί κώδικες πάνω από το $GF(5)$, και ιδιαίτερα παρουσιάζονται αυτοδυϊκοί κώδικες με μεγάλο μήκος στο ίδιο σώμα για πρώτη φορά. Επιπρόσθετα, πάνω από το $GF(7)$ παρουσιάζεται ένας νέος $[56, 28, 17]$ αυτοδυϊκός κώδικας που βελτιώνει το κάτω φράγμα στην ελάχιστη απόσταση όλων των αυτοδυϊκών κωδίκων με τις ίδιες παραμέτρους. Στο τέλος αυτού του κεφαλαίου, μελετάται η συστηματική κατασκευή μέγιστης απόστασης διαχωρίσιμων αυτοδυ-

ϊκών κωδίκων για μεγάλα πρώτα σώματα που προέρχονται από λύσεις συστημάτων διοφαντικών εξισώσεων. Βρίσκονται νέοι μέγιστης απόστασης διαχωρίσιμοι αυτοδυϊκοί κώδικες σε πολλές περιπτώσεις για πρώτα σώματα $GF(p)$. Επιπλέον, αποδεικνύεται ότι τα νέα αυτά αποτελέσματα στους αυτοδυϊκούς κώδικες βελτιώνουν το Pless-Pierce φράγμα που αναφέρεται στο ελάχιστο βάρος των αυτοδυϊκών κωδίκων.

Στο έκτο κεφάλαιο και τελευταίο του δεύτερου μέρους μελετώνται δυαδικοί πολυκυκλικοί κώδικες χρησιμοποιώντας πειραματικούς σχεδιασμούς. Προτείνεται μια νέα μέθοδος κατασκευής αυτών των κωδίκων έχοντας ως αφετηρία μια ειδική κλάση πειραματικών σχεδιασμών, τους υπερκορεσμένους σχεδιασμούς. Αποδεικνύεται μια θεμελιώδης σχέση μεταξύ κυκλικά δομημένων $E(s^2)$-βέλτιστων υπερκορεσμένων σχεδιασμών και συμπληρωματικά δυϊκών δυαδικών πολυκυκλικών κωδίκων. Επιπλέον, υλοποιείται ένας απλός γενετικός αλγόριθμος για την εύρεση των προηγούμενων κωδίκων που έχουν καλές ιδιότητες. Επιπρόσθετα αποδεικνύεται και μια αντιστοιχία μεταξύ πολυκυκλικών και οπτικών ορθογώνιων κωδίκων.

Στο έβδομο κεφάλαιο προτείνονται νέα συμμετρικά κρυπτοσυστήματα (ιδιωτικού κλειδιού) με χρήση ορθογώνιων σχεδιασμών, όπως για παράδειγμα πινάκων Hadamard και σχηματισμών Plotkin. Η μαθηματική δομή των προηγούμενων σχεδιασμών επιτρέπει το σχεδιασμό κατάλληλων κρυπτογραφικών αλγορίθμων για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος. Επίσης, παρουσιάζεται μια εκτεταμένη μελέτη κρυπτανάλυσης για διαφόρους τύπους επιθέσεων σε αυτά τα κρυπτοσυστήματα, και αποδεικνύεται η ασφάλεια αυτών κάτω από συγκεκριμένες προϋποθέσεις.

Στο όγδοο και τελευταίο κεφάλαιο της διατριβής παρουσιάζονται νέα κρυπτογραφικά σχήματα διαμοιρασμού μυστικού μηνύματος από ορθογώνιους πίνακες που προέρχονται από σχεδιασμούς Hadamard. Επιπλέον, επιδεικνύεται πως ορισμένες έννοιες της Κρυπτογραφίας διαμοιρασμού μυστικού μηνύματος αντιστοιχούν σε όρους της Συνδυαστικής Θεωρίας Σχεδιασμών, όπως για παράδειγμα είναι η δομή πρόσβασης και η ασφάλεια των κρυπτογραφικών σχημάτων.

Η στοιχειοθεσία της παρούσας διδακτορικής διατριβής πραγματοποιήθηκε με το LaTeX2ε, κάνοντας χρήση των πανέμορφων γραμματοσειρών κειμένου, GFSArtemisia, και μαθηματικών, EulerVirtualMath, της Εταιρείας Ελληνικών Τυπογραφικών Στοιχείων (GreekFontSociety).

Μέρος Ι

Συνδυαστική Θεωρία Σχεδιασμών

Science is what we understand well enough to explain to a computer. Art is everything else we do.

Donald E. Knuth (1996)

1 Συμβατές Ακολουθίες

Στο πρώτο αυτό κεφάλαιο παρουσιάζεται μια νέα μέθοδος υπολογισμού της συνάρτησης αυτοσυσχέτισης δύο πεπερασμένων τριαδικών ακολουθιών. Αποδεικνύεται ότι η νέα αυτή κωδικοποίηση της συνάρτησης αυτοσυσχέτισης είναι ιδιαίτερα αποδοτική για ακολουθίες με μικρό βάρος. Επιπλέον, παρουσιάζεται μια ανάλυση της υπολογιστικής πολυπλοκότητας της χειρότερης περιπτώσεως (worst-case analysis) βασιζόμενη σε συνδυαστικούς αλγορίθμους που προέκυψαν από τη νέα μέθοδο κωδικόποιησης. Ιδιαίτερα, ο έλεγχος της συνάρτησης αυτοσυσχέτισης για δύο ακολουθίες μήκους n και βάρους w μπορεί να αποφασιστεί σε χρόνο $\mathcal{O}(\mathrm{n} + w^2 \log w)$. Στην περίπτωση όπου $\mathrm{n} > w^2 \log w$ η πολυπλοκότητα είναι τάξεως $\mathcal{O}(\mathrm{n})$ και κατά συνέπεια δεν αναμένουμε ασυμπτωτικά αποδοτικότερους αλγορίθμους.

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στην επιστημονική εργασία [161].

§1.1 Βασικοί Ορισμοί και Ιδιότητες

Σε αυτό το κεφάλαιο, παρουσιάζεται μια νέα κωδικοποίηση της συνάρτησης αυτοσυσχέτισης δυο πεπερασμένων τριαδικών ακολουθιών, η οποία επιδεικνύει την αλληλεπίδραση της Συνδυαστικής με τη Θεωρητική Πληροφορική. Παραθέτουμε τους ορισμούς της περιοδικής και μη-περιοδικής συνάρτησης αυτοσυσχέτισης όπως αυτοί αναφέρονται στις [122, 143].

Ορισμός 1 *Για μια ακολουθία* $A = [a_1, a_2, \ldots, a_n]$ *μήκους* n *η περιοδική συνάρτηση αυτοσυσχέτισης, εν συντομία PAF, και η μη-περιοδική συνάρτηση αυτοσυσχέτισης, εν συντομία NPAF, συμβολίζονται με* $PAF_A(s)$ *ή* $P_A(s)$ *και* $NPAF_A(s)$ *ή* $N_A(s)$*, ορίζονται ως*

$$PAF_A(s) := P_A(s) = \sum_{i=1}^{n} a_i a_{i+s} \, , s = 0, 1, \ldots, n-1 \qquad \textit{και}$$

$$NPAF_A(s) := N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s} \, , s = 0, 1, \ldots, n-1$$

αντίστοιχα, όπου στο PAF θεωρούμε το (i+s) modulo n.

Ορισμός 2 *Δύο ακολουθίες,* $A = [a_1, \ldots, a_n]$ *και* $B = [b_1, \ldots, b_n]$*, μήκους* n *θα λέμε ότι έχουν PAF (αντίστοιχα NPAF) ίσο με* α*, αν* $P_A(s) + P_B(s) = \alpha$ *(αντίστοιχα* $N_A(s) + N_B(s) = \alpha$*) για* $s = 1, \ldots, n-1$*.*

Από την [50] οι ακολουθίες A και B θα καλούνται συμβατές (compatible), αν το α είναι μια σταθερά. Σημειώνουμε ότι, τέτοια ζεύγη ακολουθιών λέγονται ότι έχουν σταθερή (μη) περιοδική συνάρτηση αυτοσυσχέτισης, αν και είναι το άθροισμα των συναρτήσεων αυτοσυσχέτισης που είναι ίσο με μια σταθερά.

Συμβολισμός 1

- *Ο συμβολισμός* $AF_A(s)$*, θα συμβολίζει είτε το* $PAF_A(s)$ *είτε το* $NPAF_A(s)$*.*
- *Θα συμβολίζουμε με* $AF_{A,B}(s)$ *το άθροισμα* $AF_A(s) + AF_B(s)$*.*
- *Αν δεν υπάρχει κίνδυνος σύγχυσης για τις ακολουθίες* A *και* B*, τότε θα συμβολίζουμε το* $AF_{A,B}(s)$ *με* $AF(s)$*.*

Ορίζουμε στη συνέχεια τα διανύσματα αυτοσυσχέτισης (AF vectors) για τις ακολουθίες A και B:

$$AF(A) = [AF_A(1), \ldots, AF_A(n-1)] \text{ και } AF(B) = [AF_B(1), \ldots, AF_B(n-1)] \quad (1.1)$$

Συνεπώς, μπορούμε να αποφασίσουμε αν οι ακολουθίες A και B έχουν AF ίση με α από την ισοδύναμη διανυσματική τους μορφή $AF(A) + AF(B) = \overline{\alpha}$, όπου με $\overline{\alpha}$ συμβολίζουμε το διάνυσμα $[\alpha, \ldots, \alpha]$ μήκους $n-1$. Ενδιαφερομάστε για την ομαδοποίηση των θέσεων των στοιχείων των ακολουθιών που έχουν ίδιο πρόσημο. Αυτό δίνει το κίνητρο για τους ακόλουθους ορισμούς:

Ορισμός 3 *Το στήριγμα (support) μιας ακολουθίας* $A = [a_1, \ldots, a_n]$ *μήκους* n *είναι το σύνολο των θέσεων όπου τα στοιχεία της είναι μη-μηδενικά. Συνεπώς, το στήριγμα της ακολουθίας,* A*, ορίζεται ως* $SUP(A) = \{\pm i : i, a_i > 0 \ \vee \ -i, a_i < 0 \mid i = 1, \ldots, n\}$.

Ορισμός 4 *Το θετικό και αρνητικό στήριγμα μιας ακολουθίας* $A = [a_1, \ldots, a_n]$*, που συμβολίζονται με* $POS(A)$ *και* $NEG(A)$*, αντίστοιχα, ορίζονται ως* $POS(A) = \{i : a_i > 0, \ i = 1, \ldots, n\}$ *και* $NEG(A) = \{j : a_j < 0, \ j = 1, \ldots, n\}$*, ενώ το βάρος αυτής* $w(A)$ *ορίζεται ως* $w(A) = |POS(A)| + |NEG(A)|$.

Ορισμός 5 *Ορίζουμε τη συνάρτηση καταμέτρησης εμφανίσεων (occurrences counting function)* $[S]_e$ *για ένα πολυσύνολο (multiset)* S *και ένα στοιχείο του* S *ως* $[S]_e = |[x \in S \ : \ x = e]|$.

Για παράδειγμα, έστω S το πολυσύνολο $S = [1, 1, 2, 2, 2, 4]$. Τότε $[S]_1 = 2, [S]_2 = 3, [S]_3 = 0$ και $[S]_4 = 1$.

Λήμμα 1 (Knuth [128]) *Έστω δυο πολυσύνολα* A, B *και με* $A \uplus B$ *συμβολίζουμε την ένωση των* A *και* B*, διατηρώντας όλες τις πολλαπλότητες (των στοιχείων). Τότε* $[A \uplus B]_e = [A]_e + [B]_e$.

Για χρήση των πολυσυνόλων στη μελέτη των συμβατών ακολουθιών παραπέμπουμε στις [161, 209, 210], ενώ για σχετικές πράξεις σε αυτά βλ. [128].

Ερευνητικό Πρόβλημα 1 *Η κωδικοποίηση της συνάρτησης αυτοσυσχέτισης δυο τριαδικών ακολουθιών με βάση το στήριγμά τους, και ο αντίστοιχος υπολογισμός της μέσω κατάλληλων συνδυαστικών αλγορίθμων.*

§1.1.1 Στοιχεία Θεωρίας Πινάκων Στάθμισης

Ένας πίνακας στάθμισης (weighing matrix) $W = W(n, w)$ είναι ένας $n \times n$ τετραγωνικός πίνακας με στοιχεία από το σύνολο $\{0, \pm 1\}$ που έχει w μη-μηδενικά στοιχεία ανά γραμμή και στήλη, και το εσωτερικό γινόμενο δυο διακεκριμένων γραμμών του είναι ίσο με μηδέν. Συνεπώς, ο W ικανοποιεί τη σχέση $WW^T = wI_n$ όπου ο αριθμός w καλείται το βάρος του W. Οι πίνακες στάθμισης έχουν μελετηθεί εκτεταμένα, βλ. [33], [35] και [153], για μια ακριβή περιγραφή αυτών. Μια γνωστή αναγκαία συνθήκη για την ύπαρξη $W(n, w)$ πινάκων δίνεται από το ακόλουθο λήμμα.

Λήμμα 2 (Geramita and Seberry [70]) *Αν υπάρχει ένας $W(n, w)$ και $n \equiv 2 \pmod 4$, τότε το w είναι άθροισμα δύο τετραγώνων. Επιπλέον, $w < n$ εκτός αν $n = 2$.*

Σε αυτήν την ενότητα, επικεντρώνουμε την προσοχή μας σε $W(2n, w)$ πίνακες στάθμισης που κατασκευάζονται από δυο κυκλικούς πίνακες. Δύο ακολουθίες μήκους n, θα λέμε ότι είναι τύπου $(0, \pm 1)$ και βάρους w αν έχουν συνολικά w μη-μηδενικά στοιχεία και μπορούν να χρησιμοποιηθούν ως οι πρώτες γραμμές αντίστοιχων κυκλικών πινάκων για να παράγουν έναν $W(2n, w)$ (βλ. Θεώρημα 1).

Αυτές οι διπλά κυκλικές ακολουθίες (double circulant sequences) θα συμβολίζονται με $DC(n, w)$ αν έχουν PAF μηδέν. Σε περίπτωση που έχουν NPAF μηδέν καλούνται τριαδικά συμπληρωματικά ζεύγη ακολουθιών (Ternary Complementary Pairs, εν συντομία TCP) και συμβολίζονται με $TCP(n, w)$. Για περαιτέρω λεπτομέρειες που αφορούν τη Θεωρία των TCP, παραπέμπουμε στην [36]. Η κατασκευή των πινάκων στάθμισης από δυο κυκλικούς πίνακες (the two circulants construction) περιγράφεται από το ακόλουθο θεώρημα.

Θεώρημα 1 (Geramita and Seberry [70]) *Αν υπάρχουν δυο κυκλικοί πίνακες* A_1, A_2 *τάξης* n, *με στοιχεία από το σύνολο* $\{0, \pm 1\}$, *που ικανοποιούν τη σχέση* $A_1A_1^T + A_2A_2^T = wI_n$ *όπου το* w *είναι ένας ακέραιος, τότε υπάρχει ένας* $W(2n, w)$ *πίνακας στάθμισης, που παράγεται ως*

$$W(2n,w) = \begin{pmatrix} A_1 & A_2 \\ -A_2^T & A_1^T \end{pmatrix} \text{ ή } W(2n,w) = \begin{pmatrix} A_1 & A_2R \\ -A_2R & A_1 \end{pmatrix}$$

όπου R *είναι ο τετραγωνικός πίνακας τάξης* n *με* $r_{ij} = 1$ *αν* $i + j - 1 = n$ *και* 0 *διαφορετικά.*

§1.1.2 Εφαρμογές των Συμβατών Ακολουθιών

Σε αυτή την ενότητα δίνουμε μερικές αναφορές σε εργασίες που περιγράφουν τις εφαρμογές των συμβατών ακολουθιών. Δεν αποσκοπούμε στο να παρέχουμε μια ολοκληρωμένη, ή με κάθε τρόπο πλήρη, αντιμετώπιση του θέματος, καθώς αυτό δεν είναι ο σκοπός της παρούσας διατριβής. Απλά ενδιαφερόμαστε να δώσουμε μια εικόνα των πολλών εφαρμογών που συναντά κάποιος στις συμβατές ακολουθίες, προκειμένου να εκθέσουμε ότι οι ακολουθίες με σταθερή συνάρτηση αυτοσυσχέτισης διαδραματίζουν κεντρικό ρόλο στη Θεωρία των ακολουθιών, και ότι αυτές οι εφαρμογές είναι ευρύτερου ενδιαφέροντος.

Οι συμβατές ακολουθίες χρησιμοποιούνται για την κατασκευή ακολουθιών με επιθυμητές ιδιότητες για εφαρμογές σε ραδιοεντοπιστές ή όπως είναι γνωστότεροι με το διεθνές όνομα ραντάρ (radar), όπως αυτό περιγράφεται στην [232]. Επιπλέον, αυτές οι ακολουθίες παρεμβαίνουν στην κωδικοποιημένη απεικόνιση διαφράγματος (coded aperture imaging), [48], και σε εφαρμογές επεξεργασίας σημάτων (signal processing) υψηλότερης διάστασης όπως είναι η χρονική συχνότητα κωδικοποίησης (time frequency coding), [81], και η χωρική συσχέτιση (spatial correlation), [108]. Επιπρόσθετα, η χρήση των τριαδικών συσχετισμένων ακολουθιών επιτρέπει τη διαμόρφωση υβριδικών απορροφητικών διαχυτών (hybrid absorber-diffusers) που επιτυγχάνουν καλύτερη διασπορά των επιδόσεων χωρίς πρόσθετη απορρόφηση όπως σημειώνεται στην [31].

Η κρυπτογραφία [203, 221] και η Θεωρία κωδίκων [176] συχνά ενδιαφέρονται για ψευδό-τυχαίες (pseudo-random) ακολουθίες και για ακολουθίες που δεν επιδέχονται περαιτέρω συμπίεση. Τελικά, προκύπτει οτι η ψευδό-τυχαιότητα και η αποσυμπίεση είναι πολύ κόντα σχετι-

ζόμενες με την χαμηλή αυτοσυσχέτιση των εν γένει ακολουθιών. Το σύγγραμμα των Golomb και Gong, [80], είναι μια πλούσια πηγή πληροφόρησης για εφαρμογές ακολουθιών με χαμηλή αυτοσυσχέτιση, στις τηλεπικοινωνίες, σε εφαρμογές ραντάρ και κρυπτογραφίας.

Μια κλάση των συμβατών ακολουθιών, οι συμπληρωματικές ακολουθίες (complementary sequences) έχουν μελετηθεί ιδιαίτερα. Πρόσφατα, οι συμπληρωματικές ακολουθίες χρησιμοποιήθηκαν σε διάφορες εφαρμογές των ψηφιακών τηλεπικοινωνιακών συστημάτων όπως είναι ο κωδικός πρόσβασης ενός χρήστη για συστήματα πολλαπλής πρόσβασης (DS-CDMA systems) [207], και το πρόθεμα συστημάτων OFDM για να ελλατώσουν το παρεχόμενο σήμα στον μέσο συντελεστή ισχύος (power ratio) [17].

Οι συμβατές ακολουθίες παίζουν καθοριστικό ρόλο στην κατασκευή συνδυαστικών σχεδιασμών (combinatorial designs), όπως για παράδειγμα πίνακες στάθμισης (weighing matrices) και σχεδιασμούς στάθμισης (weighing designs). Οι πίνακες και οι σχεδιασμοί στάθμισης έχουν εκτεταμένως μελετηθεί για τη χρήση τους σε πειράματα Στατιστικής όπως παρατηρήθηκε αρχίκα από τον Hotelling [114] και στη συνέχεια από τον Raghavarao [199] και άλλους ερευνητές [33, 152]. Αυτοί οι πίνακες στάθμισης μπορούν στη συνέχεια να χρησιμοποιηθούν για σκοπούς της Θεωρίας κωδίκων, πιο συγεκριμένα για την κατασκευή γραμμικών κωδίκων με επιθυμητές ιδιότητες, ενδεικτικά παραπέμπουμε στην [3].

Κλείνοντας αυτήν την ενότητα, θα θέλαμε να ανάφέρουμε ότι οι συμβατές ακολουθιές είναι ενδιαφέρουσες μαθηματικές δομές που αξίζει να μελετηθούν σε εντελώς θεωρητική βάση [122, 143, 153, 208].

§1.2 Συνδυαστικοί Αλγόριθμοι για Συμβατές Ακολουθίες

Σε αυτήν την ενότητα, παρουσιάζουμε ένα νέο αλγόριθμο ο οποίος βασίζεται στο στήριγμα δύο ακολουθιών για να αποφασίσει αν αυτές είναι συμβατές. Η χρήση του στηρίγματος των ακολουθιών εφαρμόστηκε αρχικά στις [50] και [61], και πρόσφατα για τον υπολογισμό της συνάρτησης αυτοσυσχέτισης στις [56, 151, 161].

Η κινητήριος δύναμη πίσω από αυτήν την ερμηνεία που μας οδήγησε στην κωδικοποίηση της συνάρτησης αυτοσυσχέτισης μέσω του στηρίγματος των ακολουθιών, ήταν να αποβάλουμε τους περιττούς πολλαπλα-

σιασμούς μεταξύ μηδενικών στοιχείων των ακολουθιών που λαμβάνουν μέρος στον υπολογισμό της συνάρτησης αυτοσυσχέτισης.

Ενδιαφερόμαστε μόνο για τα μη-μηδενικά στοιχεία των ακολουθιών, δηλαδή αυτά που αποτελούν το στήριγμά τους. Στις ενότητες που ακολουθούν, επιδεικνύουμε ότι όλη η πληροφορία που χρειάζεται για να υπολογιστεί η συνάρτηση αυτοσυσχέτισης μπορεί να εκφραστεί ως μια συνάρτηση του βάρους των δυο ακολουθιών (βλ. και Ενότητα 1.3).

§1.2.1 Κλασική Περιγραφή της Συνάρτησης Αυτοσυσχέτισης

Αν αναπτύξουμε το άθροισμα στο PAF και NPAF μιας ακολουθίας $A = [a_1, \ldots, a_n]$, λαμβάνουμε τα ακόλουθα αθροίσματα:

$$P_A(s) = \sum_{i=1}^{n} a_i a_{i+s \pmod n} = a_1 a_{1+s \pmod n} + \ldots + a_n a_{s \pmod n} \quad (1.2)$$

$$N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s} = a_1 a_{1+s} + \ldots + a_{n-s} a_n \quad (1.3)$$

όπου $s = 0, 1, \ldots, n-1$. Στη συνέχεια θεωρούμε μόνο υποψήφιες συμβατές ακολουθίες (για παράδειγμα $DC(n, w)$ ή $TCP(n, w)$ ακολουθίες), και κατά συνέπεια τα στοιχεία τους παίρνουν τιμές από το σύνολο $\{0, \pm 1\}$. Συνεπώς, τα ζεύγη $(a_i, a_{i+s \pmod n}) = a_i a_{i+s \pmod n}$ και $(a_i, a_{i+s}) = a_i a_{i+s}$ έχουν πιθανές τιμές στο σύνολο $\{0, \pm 1\}$. Ορίζουμε τα διανύσματα PAF και NPAF για τις ακολουθίες A και B ως:

$$PAF(A) = [P_A(1), \ldots, P_A(n-1)] \qquad PAF(B) = [P_B(1), \ldots, P_B(n-1)]$$
$$NPAF(A) = [N_A(1), \ldots, N_A(n-1)] \quad NPAF(B) = [N_B(1), \ldots, N_B(n-1)]$$

Συνεπώς, μπορούμε να αποφασίσουμε αν οι ακολουθίες A και B είναι συμβατές, δηλαδή αν έχουν σταθερό PAF ή NPAF, από την ισοδύναμη διανυσματική τους μορφή $PAF(A)+PAF(B) = \overline{\alpha}$ ή $NPAF(A)+NPAF(B) = \overline{\alpha}$, όπου με $\overline{\alpha}$ συμβολίζουμε το διάνυσμα $[\alpha, \ldots, \alpha]$ μήκους $n-1$. Σημειώνουμε ότι τέτοια ζεύγη ακολουθιών έχουν σταθερό PAF ή NPAF, αν και είναι το άθροισμα των αντίστοιχων συναρτήσεων αυτοσυσχέτισης που είναι σταθερό.

§1.2.2 Κωδικοποίηση της Συνάρτησης Αυτοσυσχέτισης μέσω Προσημασμένων Συνόλων Διαφορών

Οι ακόλουθοι συμβολισμοί και δομές δεδομένων φάνηκαν αρκετά χρήσιμοι στην προσπάθειά μας να εκφράσουμε τη συνάρτηση αυτοσυσχέτισης μέσω του στηρίγματος των ακολουθιών.

Είναι αρκετά γνωστό ότι δύο συμβατές ακολουθίες, στην περίπτωση που $\alpha = 0$, είναι ισοδύναμες με συμπληρωματικά σύνολα διαφορών (supplementary difference sets, εν συντομία SDS βλ. [70]). Η κωδικοποίηση της συνάρτησης αυτοσυσχέτισης που δίνεται σε αυτήν την ενότητα μπορεί να θεωρηθεί ως η γενίκευση των SDS σε τρια επίπεδα $\{0, \pm 1\}$. Από τις [209, 210] θα θεωρήσουμε συλλογές μαθηματικών αντικειμένων, (που θα συμβολίζονται με $[\,]$) οριζόμενες στην ομάδα $\mathbb{Z}_n$ τάξης n, στην οποία μετράμε τις πολλαπλότητες των αντικειμένων, παρά σύνολα (που τα συμβολίζουμε $\{\,\}$). ο ισοδύναμος όρος στη Θεωρητική Πληροφορική είναι πολυσύνολο (για περαιτέρω λεπτομέρειες παραπέμπουμε στον Knuth [128]). Αν T_1 και T_2 είναι δύο λίστες τότε με $T_1 \uplus T_2$ θα συμβολίζουμε την λίστα η οποία παράγεται αν παραθέσουμε την T_1 με την T_2 (όπου διατηρούμε τις πολλαπλότητες των στοιχείων). Αν η παραχθείσα λίστα είναι ταξινοποιημένη (sorted) ως προς κάποια λεξικογραφική διάταξη, τότε αυτή η πράξη θα συμβολίζεται με $T_1 \& T_2$.

Παράδειγμα 1 Θεωρούμε τη διάταξη $a_1 < a_2 < a_3 \in \mathbb{Z}_n$ και τις λίστες $T_1 = [a_1, a_3, a_2]$ και $T_2 = [a_2, a_4, a_1]$. Τότε

$$T_1 \uplus T_2 = [a_1, a_3, a_2, a_2, a_4, a_1] \text{ και } T_1 \& T_2 = [a_1, a_1, a_2, a_2, a_3, a_4] \quad (1.4)$$

Ένας φυσικός τρόπος να εκφράσουμε τις πράξεις που συμβαίνουν στην AF, όταν έχουμε μια αναπαράσταση των στοιχείων των ακολουθιών μέσω των θέσεών τους, είναι με προσημασμένες διαφορές (signed differences). Μόνο οι παρακάτω τρείς περιπτώσεις μπορούν να συμβούν στην AF, ορισμένη μέσω του στηρίγματος, μιας ακολουθίας A:

(i) Έστω c_1 ο αριθμός των ζευγών (a_i, a_{i+s}) με $a_i = a_{i+s} = 1$.

(ii) Έστω c_2 ο αριθμός των ζευγών (a_i, a_{i+s}) με $a_i = a_{i+s} = -1$.

(iii) Έστω c_3 ο αριθμός των ζευγών (a_i, a_{i+s}) με $a_i a_{i+s} = -1$.

Τότε από τη βασική αρχή απαρίθμησης συμπεραίνουμε ότι $AF_A(s) = c_1 + c_2 - c_3,\ s = 0, 1, \ldots, n-1$, όπου $AF_A(s) = P_A(s)$ ή $AF_A(s) = N_A(s)$, και στο $P_A(s)$ θεωρούμε το (i+s) modulo n.

Προσημασμένα Σύνολα Διαφορών Για καθεμία από τις προηγούμενες περιπτώσεις ορίζουμε προσημασμένα (πολυ-)σύνολα διαφορών.

Ορισμός 6 *Έστω $A = [a_1, \ldots, a_n]$ μια ακολουθία μήκους n, με στοιχεία από το σύνολο $\{0, \pm 1\}$.*

(i) Αυτή η περίπτωση αντιστοιχεί στο $\mathrm{POS}(A)$. Ορίζουμε τις προσημασμένες διαφορές στο θετικό στήριγμα της A ως $D^{+}_{A,2} = [(x-y) \pmod n : x \neq y, x, y \in \mathrm{POS}(A)]$ για το PAF, ενώ για το NPAF ορίζουμε τις προσημασμένες διαφορές στο θετικό στήριγμα της A ως $D^{+}_{A,1} = [x - y : x > y \ \wedge \ x, y \in \mathrm{POS}(A)]$.

(ii) Αυτή η περίπτωση αντιστοιχεί στο $\mathrm{NEG}(A)$. Ορίζουμε τις προσημασμένες διαφορές στο αρνητικό στήριγμα της A ως $D^{-}_{A,2} = [(x-y) \pmod n : x \neq y, x, y \in \mathrm{NEG}(A)]$ για το PAF, ενώ για το NPAF ορίζουμε τις προσημασμένες διαφορές στο αρνητικό στήριγμα της A ως $D^{-}_{A,1} = [x - y : x > y \ \wedge \ x, y \in \mathrm{NEG}(A)]$.

(iii) Για να συμβεί το $a_i a_{i+s \pmod n} = -1$ στο PAF έχουμε δύο περιπτώσεις. Θα πρέπει $a_i = 1$, $a_{i+s \pmod n} = -1$ και αντίστροφα. Συνεπώς, πρέπει να ορίσουμε τις ετεροδιαφορές ή διασταυρούμενες διαφορές (cross-differences) μεταξύ του θετικού και αρνητικού στηρίγματος της A ως $D^{\pm}_{A,2} = [(x-y) \pmod n : x \in \mathrm{POS}(A), y \in \mathrm{NEG}(A)]$ και $D^{\mp}_{A,2} = [(x-y) \pmod n : x \in \mathrm{NEG}(A), y \in \mathrm{POS}(A)]$. Καθώς μετράμε την πολλαπλότητα των διαφορών σε δύο κατευθύνσεις ορίζουμε $C^{\rightleftarrows}_{A,2} = D^{\pm}_{A,2} \uplus D^{\mp}_{A,2}$. Όμοια, για να συμβεί το $a_i a_{i+s} = -1$ στο NPAF έχουμε δύο περιπτώσεις. Θα πρέπει $a_i = 1$, $a_{i+s} = -1$ και αντίστροφα. Συνεπώς, πρέπει να ορίσουμε τις διασταυρούμενες διαφορές μεταξύ του θετικού και αρνητικού στηρίγματος της A ως $D^{\pm}_{A,1} = [x - y : x > y \ \wedge \ x \in \mathrm{POS}(A), y \in \mathrm{NEG}(A)]$ και $D^{\mp}_{A,1} = [x - y : x > y \ \wedge \ x \in \mathrm{NEG}(A), y \in \mathrm{POS}(A)]$. Καθώς, μετράμε την πολλαπλότητα των διαφορών σε μια κατεύθυνση ορίζουμε $C^{\rightrightarrows}_{A,1} = D^{\pm}_{A,1} \uplus D^{\mp}_{A,1}$.

Παρατήρηση 1 *Χρησιμοποιήσαμε τα* $\pm, \mp$ *στον προηγούμενο ορισμό για να συμβολίσουμε τη χρήση των* $\mathrm{POS}(A), \mathrm{NEG}(A)$*, και το δείκτη* 2 *στα πολυσύνολα για να αναπαριστήσουμε το γεγονός οτί ορίσαμε τις διαφορές σε δύο κατευθύνσεις (*$\rightleftarrows$*) λόγω της περιοδικής ιδιότητας της συνάρτησης αυτοσυσχέτισης που αντιστοιχεί στη modulo πράξη στους δείκτες των στοιχείων της ακολουθίας* A*. Αντίστοιχα, με το δείκτη* 1 *στα πολυσύνολα αναπαριστούμε το γεγονός ότι τα πολυσύνολα ορίστηκαν σε μια κατεύθυνση (*$\rightrightarrows$*) λόγω της μη-περιοδικής ιδιότητας της συνάρτησης αυτοσυσχέτισης που αντιστοιχεί στους δείκτες των στοιχείων της ακολουθίας* A*.*

Στη γενικότερη περίπτωση της AF, τα προηγούμενα προσημασμένα σύνολα διαφορών μπορούν να γραφούν σε απλούστερη μορφή (από άποψης συμβολισμού).

Ορισμός 7 *Για μια ακολουθία* $A = [a_1, \ldots, a_n]$ *μήκους* n *ορίζουμε τα ακόλουθα πολυσύνολα:*

(i) Προσημασμένες διαφορές στο θετικό στήριγμα της A *ως* $D_A^+ = [x - y \ : \ x, y \in \mathrm{POS}(A), x > y]$*.*

(ii) Προσημασμένες διαφορές στο αρνητικό στήριγμα της A *ως* $D_A^- = [x - y \ : \ x, y \in \mathrm{NEG}(A), x > y]$*.*

(iii) Διασταυρούμενες διαφορές στο θετικό και αρνητικό στήριγμα της A *ως* $C_A = D_A^{\pm} \uplus D_A^{\mp}$*,*
όπου $D_A^{\pm} = [x - y \ : \ x \in \mathrm{POS}(A), y \in \mathrm{NEG}(A), x > y]$ *και* $D_A^{\mp} = [x - y \ : \ x \in \mathrm{NEG}(A), y \in \mathrm{POS}(A), x > y]$*.*

Το κίνητρο για τον ορισμό των πολυσυνόλων του Ορισμού 7 είναι να μετρήσουμε τη συνεισφορά κάθε ακολουθίας στον υπολογισμό του $\mathrm{AF}_{A,B}(s)$. Δίνουμε παρακάτω τη νέα κωδικοποίηση της συνάρτησης αυτοσυσχέτισης μέσω προσημασμένων συνόλων διαφορών.

Θεώρημα 2 *Έστω* A, B *δυο ακολουθίες μήκους* n*, βάρους* w *με στοιχεία από το σύνολο* $\{-1, 0, 1\}$*. Έστω* D *το πολυσύνολο* $D_A^+ \uplus D_A^- \uplus D_B^+ \uplus D_B^-$ *και* C *το πολυσύνολο* $C_A \uplus C_B$*. Για κάθε* $s \in \{1, 2, \ldots n-1\}$*, τα ακόλουθα είναι ισοδύναμα:*

(i) $\mathrm{AF}_{A,B}(s) = \alpha$

(ii) $[D]_s - [C]_s = \alpha$

Απόδειξη. Θεωρούμε σταθερό $s \in \{1, 2, \ldots n-1\}$. Θα αποδείξουμε το θεώρημα για το NPAF. Η περίπτωση του PAF είναι παρόμοια. Έχουμε ότι $AF_{A,B}(s) = AF_A(s) + AF_B(s)$. Συνεπώς πρέπει να υπολογίσουμε την $AF_C(s)$ για $C = A, B$. Έχουμε ότι $AF_C(s) = |P_C| - |N_C|$, όπου $P_C = [(c_i, c_{i+s}) \ : \ c_i c_{i+s} = 1, \ i = 1, 2 \ldots, n-s, \ c_i \in C]$ και $N_C = [(c_i, c_{i+s}) \ : \ c_i c_{i+s} = -1, \ i = 1, 2 \ldots, n-s, \ c_i \in C]$.

Θα πρέπει να θεωρήσουμε μόνο στοιχεία του στηρίγματος, καθώς όλα τα γινόμενα μηδενικών στοιχείων έχουν μηδενική συνεισφορά στο άθροισμα. Τα ζεύγη των στοιχείων του στηρίγματος που συνεισφέρουν "+1" είναι εκείνα όπου και τα δυο στοιχεία έχουν το ίδιο πρόσημο, δηλαδή είναι στοιχεία του P_C. Από τον ορισμό του D_C^+ (αντίστοιχα D_C^-), για κάθε εμφάνιση του s στο D_C^+ (αντίστοιχα D_C^-), υπάρχει ένα ζεύγος (c_i, c_{i+s}) για κάποιο i τέτοιο ώστε τα c_i και c_{i+s} να έχουν και τα δυο θετικό (αντίστοιχα αρνητικό) πρόσημο, κατά συνέπεια ανήκει στο P_C. Για την αντίστροφη κατεύθυνση, δηλαδή ότι για κάθε ζεύγος $(c_i, c_{i+s}) \in P_C$ υπάρχει μια εμφάνιση του s στο D_C^+ ή D_C^-, απορρέει άμεσα από τον ορισμό των D_C^+ και D_C^-. Συνεπώς, η πληθικότητα του P_C είναι ίση με τον αριθμό των εμφανίσεων του s στο D_C^+ και D_C^-.

Ομοίως, τα ζεύγη των στοιχείων του στηρίγματος που συνεισφέρουν ένα "−1" είναι εκείνα όπου τα στοιχεία τους έχουν αντίθετα πρόσημα. Από τον ορισμό του C_C, για κάθε εμφάνιση του s στο C_C, υπάρχει ένα ζεύγος (c_i, c_{i+s}) για κάποιο i τέτοιο ώστε τα c_i και c_{i+s} να έχουν αντίθετα πρόσημα και κατά συνέπεια ανήκουν στο N_C. Για την αντίστροφη κατεύθυνση, δηλαδή ότι για κάθε ζεύγος $(c_i, c_{i+s}) \in N_C$ υπάρχει μια εμφάνιση του s στο C_C, απορρέει άμεσα από τον ορισμό του C_C. Συνεπώς, η πληθικότητα του N_C είναι ίση με τον αριθμό των εμφανίσεων του s στο C_C.

Συνοψίζοντας για τις ακολουθίες A και B έχουμε

$$\begin{aligned} AF_{A,B}(s) &= AF_A(s) + AF_B(s) \\ &= |P_A| - |N_A| + |P_B| - |N_B| \\ &= (|P_A| + |P_B|) - (|N_A| + |N_B|) \\ &= ([D_A^+]_s + [D_A^-]_s + [D_B^+]_s + [D_B^-]_s) - ([C_A]_s + [C_B]_s) \\ &= [D_A^+ \uplus D_A^- \uplus D_B^+ \uplus D_B^-]_s - [C_A \uplus C_B]_s \\ &= [D]_s - [C]_s \end{aligned}$$

Συνεπώς,

$$AF_{A,B}(s) = \alpha \Leftrightarrow [D]_s - [C]_s = \alpha$$

□

Το ακόλουθο πόρισμα είναι άμεσο από το Θεώρημα 2 για την περίπτωση επαλήθευσης υποψηφίων $DC(n, w)$ ή $TCP(n, w)$ ζευγών ακολουθιών.

Πόρισμα 1 *Έστω* A, B *δύο ακολουθίες μήκους* n *και βάρους* w *με στοιχεία από το σύνολο* $\{0, \pm 1\}$. *Τότε, ισχύουν τα ακόλουθα:*

1. *Οι* A *και* B *σχηματίζουν ένα* $DC(n, w)$ *ζεύγος, δηλαδή έχουν PAF μηδέν αν και μόνον αν* $(D^{+}_{A,2} \uplus D^{-}_{A,2}) \& (D^{+}_{B,2} \uplus D^{-}_{B,2}) = C^{\rightleftarrows}_{A,2} \& C^{\rightleftarrows}_{B,2}$
2. *Οι* A *και* B *σχηματίζουν ένα* $TCP(n, w)$, *δηλαδή έχουν NPAF μηδέν αν και μόνον αν* $(D^{+}_{A,1} \uplus D^{-}_{A,1}) \& (D^{+}_{B,1} \uplus D^{-}_{B,1}) = C^{\rightrightarrows}_{A,1} \& C^{\rightrightarrows}_{B,1}$

Απόδειξη. Άμεση από το Θεώρημα 2, θέτοντας $\alpha = 0$.

□

§1.2.3 Επαλήθευση Διαφόρων Κλάσεων Συμβατών Ακολουθίων

Με βάση το Θεώρημα 2, μπορούμε να σχεδιάσουμε έναν αλγόριθμο για την επαλήθευση (verification) της ακόλουθης ιδιότητας,

"Οι ακολουθίες A και B μήκους n έχουν σταθερή (μη) περιοδική συνάρτηση αυτοσυσχέτισης ίση με α."

Τα βασικά βήματα του αλγορίθμου είναι:

- Υπολογισμός του στηρίγματος
- Υπολογισμός των πολυσυνόλων των προσημασμένων και διασταυρούμενων διαφορών
- Επαλήθευση της σχέσης $[D]_s - [C]_s = \alpha$ για $s \in \{1, 2, \ldots, n-1\}$

Αυτά τα βήματα επεκτείνουν τα αποτελέσματα του Πορίσματος 1 στην περίπτωση όπου $\alpha \neq 0$, και εκείνα της [56] για δύο τριαδικές ακολουθίες με AF μηδέν. Μια περιγραφή των παραπάνω βημάτων, σε μορφή ψευδοκώδικα δίνεται στον Αλγόριθμο 1.

Αναλόγως της τιμής του α και την επιλογή της $AF(s)$, μπορούμε να επαληθεύσουμε την AF ιδιότητα (βλ. Ορισμό 2) για έναν αριθμό συνδυαστικών αντικειμένων. Για παράδειγμα, το πρόβλημα (επαλήθευσης) αν δυο ακολουθίες A και B σχηματίζουν ένα $DC(n, w)$ ζεύγος, δηλαδή έχουν PAF μηδέν, είναι ένα πρόβλημα απόφασης. Θυμίζουμε ότι, ένα $DC(n, w)$ ζεύγος που σχηματίζεται από δυο ακολουθίες A και B

Algorithm 1 AFVerification Algorithm

```
procedure AFVerification(A, B, α)
Require: A, B are {0, ±1} sequences of length n and α ∈ {0, 1, ..., 2n}
    n ← |A|
    Compute POS(A), NEG(A), POS(B), NEG(B)
    Compute D_A^+, D_A^-, C_A, D_B^+, D_B^-, C_B
    Compute D = D_A^+ ⊎ D_A^- ⊎ D_B^+ ⊎ D_B^- and C = C_A ⊎ C_B
    for s = 1, 2, ..., n − 1 do
        if [D]_s − [C]_s ≠ α then return False
        end if
    end for
  return True
  end procedure
```

ορίζεται ως $DC(n, w) := \{(A, B) : A, B \in \{-1, 0, 1\}^n,\ w(A) + w(B) = w,\ PAF_{A,B}(s) = 0,\ s = 1, \ldots, n-1\}$. Τότε, μπορούμε απλά να ελέγξουμε για $PAF_{A,B}(s) = 0 \Leftrightarrow [D]_s = [C]_s$. Σημειώνουμε ότι, σε αυτήν την περίπτωση τα παραγόμενα πολυσύνολα είναι ίσα. Σχετικά έχουμε το ακόλουθο παράδειγμα.

Παράδειγμα 2 Θεωρούμε το ακόλουθο $DC(17, 9)$ ζεύγος ακολουθιών που παράγει έναν πίνακα στάθμισης $W(2 \cdot 17, 9)$ μέσω του θεωρήματος 1, και το οποίο μπορεί να βρεθεί στην [153]:

```
A=00++-000000+0+000
B=0-000-0+0+0000000
```

Μπορούμε να επαληθεύσουμε αν οι ακολουθίες A, B έχουν PAF μηδέν μέσω του Πορίσματος 1. Χρησιμοποιούμε την αναπαράσταση των ακολουθιών μέσω των στηρίγματων τους, ως ακολούθως.

$$SUP(A) = \{3, 4, -5, 12, 14\} \text{ και } SUP(B) = \{-2, -6, 8, 10\}$$

Τα σύνολα του στηρίγματος μπορούν να γίνουν διαχωρίσιμα ως

$$POS(A) = \{3, 4, 12, 14\}, NEG(A) = \{5\},\ POS(B) = \{8, 10\}, NEG(B) = \{2, 6\}$$

Πλέον, μπορούμε να σχηματίσουμε τα ακόλουθα έξι πολυσύνολα διαφορών για τις δύο ακολουθίες:

$$D^+_{A,2} = [1, 9, 11, 8, 10, 2, 16, 8, 6, 9, 7, 15] \qquad D^+_{B,2} = [2, 15]$$
$$D^-_{A,2} = [\,] \qquad D^-_{B,2} = [4, 13]$$
$$C^{\rightleftarrows}_{A,2} = [7, 9, 2, 1, 10, 8, 15, 16] \qquad C^{\rightleftarrows}_{B,2} = [6, 2, 8, 4, 11, 15, 9, 13]$$

Παράδειγμα 3 (Συνέχεια του Παραδείγματος 2) Θεωρώντας την παράθεση των στοιχείων των προηγούμενων πολυσυνόλων, έχουμε τα ακόλουθα πολυσύνολα:

$$\mathrm{D}^{+}_{A,2} \uplus \mathrm{D}^{-}_{A,2} = [1,9,11,8,10,2,16,8,6,9,7,15]$$
$$\mathrm{D}^{+}_{B,2} \uplus \mathrm{D}^{-}_{B,2} = [2,15,4,13]$$
$$\mathrm{C}^{\rightleftarrows}_{A,2} \uplus \mathrm{C}^{\rightleftarrows}_{B,2} = [7,9,2,1,10,8,15,16,6,2,8,4,11,15,9,13]$$

Είναι εύκολο να αποφανθούμε ότι το πρόβλημα επαλήθευσης, αν οι δύο ακολουθίες σχηματίζουν ένα $\mathrm{DC}(17,9)$ ζεύγος, έχει μετασχηματιστεί σε ένα συγκριτικό πρόβλημα ταξινόμησης, καθώς η πολλαπλότητα των προσημασμένων διαφορών στις δύο ακολουθίες εμφανίζεται τον ίδιο ακριβώς αριθμό φορών ως διασταυρούμενες διαφορές σε αυτές. Αυτό μπορεί να φανεί σχηματίζοντας τα πολυσύνολα:

$$(\mathrm{D}^{+}_{A,2} \uplus \mathrm{D}^{-}_{A,2}) \& (\mathrm{D}^{+}_{B,2} \uplus \mathrm{D}^{-}_{B,2}) = [1,2,2,4,6,7,8,8,9,9,10,11,13,15,15,16]$$
$$\mathrm{C}^{\rightleftarrows}_{A,2} \& \mathrm{C}^{\rightleftarrows}_{B,2} = [1,2,2,4,6,7,8,8,9,9,10,11,13,15,15,16]$$

Είναι προφανές, ότι οι ακολουθίες έχουν PAF μηδέν, αν η στοιχείο προς στοιχείο σύγκριση των προηγούμενων πολυσυνόλων είναι αληθής για όλες τις θέσεις. Με άλλα λόγια, αν η επαλήθευση είναι αληθής για όλες τις θέσεις, δηλαδή είναι ένα πρόβλημα απόφασης [216].
Παρέχουμε επίσης τα διανύσματα PAF των ακολουθιών A και B για μια ανεξάρτητη επαλήθευση:

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{P}_A(s)$	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0
$\mathrm{P}_B(s)$	0	0	0	0	0	-1	0	-1	-1	0	-1	0	0	0	0	0
$\mathrm{P}_A(s) + \mathrm{P}_B(s)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Αντίστοιχα, το πρόβλημα (επαλήθευσης) αν δυο ακολουθίες A και B σχηματίζουν ένα $\mathrm{TCP}(n,w)$ ζεύγος, δηλαδή έχουν NPAF μηδέν, είναι ένα πρόβλημα απόφασης. Θυμίζουμε ότι, ένα $\mathrm{TCP}(n,w)$ ζεύγος που σχηματίζεται από δυο ακολουθίες A και B ορίζεται ως $\mathrm{DC}(n,w) := \{(A,B) : A,B \in \{-1,0,1\}^n,\ w(A)+w(B)=w,\ \mathrm{NPAF}_{A,B}(s)=0,\ s=1,\ldots,n-1\}$. Τότε, μπορούμε απλά να ελέγξουμε για $\mathrm{NPAF}_{A,B}(s)=0 \Leftrightarrow [D]_s = [C]_s$. Σημειώνουμε ότι, και σε αυτήν την περίπτωση τα παραγόμενα πολυσύνολα είναι ίσα. Σχετικά έχουμε το ακόλουθο παράδειγμα.

Παράδειγμα 4 Θεωρούμε το ακόλουθο $\mathrm{TCP}(19,10)$ ζεύγος ακολουθιών που παράγει έναν πίνακα στάθμισης $W(2\cdot 19,10)$ μέσω του Θεωρήματος 1 και μπορεί να βρεθεί στην [37]:

```
A=00000+-00000-0000++
B=+000+0000+0+0-00000
```

Μπορούμε να επαληθεύσουμε αν οι ακολουθίες A, B έχουν NPAF μηδέν μέσω του Πορίσματος 1. Χρησιμοποιούμε την αναπαράσταση των ακολουθιών μέσω των στηρίγματων τους, ως ακολούθως.

$$\mathrm{SUP}(A) = \{6, -7, -13, 18, 19\} \text{ και } \mathrm{SUP}(B) = \{1, 5, 10, 12, -14\}$$

Τα σύνολα του στηρίγματος μπορούν να γίνουν διαχωρίσιμα ως

$$\mathrm{POS}(A) = \{6, 18, 19\}, \mathrm{NEG}(A) = \{7, 13\} \text{ και}$$
$$\mathrm{POS}(B) = \{1, 5, 10, 12\}, \mathrm{NEG}(B) = \{14\}$$

Πλέον, μπορούμε να σχηματίσουμε τα ακόλουθα έξι πολυσύνολα διαφορών για τις δύο ακολουθίες:

$$\mathrm{D}^{+}_{A,1} = [12, 13, 1] \qquad \mathrm{D}^{+}_{B,1} = [4, 9, 11, 5, 7, 2]$$
$$\mathrm{D}^{-}_{A,1} = [6] \qquad \mathrm{D}^{-}_{B,2} = [\,]$$
$$\mathrm{C}^{\rightrightarrows}_{A,1} = [11, 5, 12, 6, 1, 7] \qquad \mathrm{C}^{\rightrightarrows}_{B,1} = [13, 9, 4, 2]$$

Θεωρώντας την παράθεση των στοιχείων των προηγούμενων πολυσυνόλων, έχουμε τα ακόλουθα πολυσύνολα:

$$\mathrm{D}^{+}_{A,1} \uplus \mathrm{D}^{-}_{A,1} = [12, 13, 1, 6]$$
$$\mathrm{D}^{+}_{B,1} \uplus \mathrm{D}^{-}_{B,1} = [4, 9, 11, 5, 7, 2]$$
$$\mathrm{C}^{\rightrightarrows}_{A,1} \uplus \mathrm{C}^{\rightrightarrows}_{B,1} = [11, 5, 12, 6, 1, 7, 13, 9, 4, 2]$$

Είναι εύκολο να αποφανθούμε ότι το πρόβλημα επαλήθευσης, αν οι δύο ακολουθίες σχηματίζουν ένα $\mathrm{TCP}(19,10)$ ζεύγος, έχει μετασχηματιστεί σε ένα συγκριτικό πρόβλημα ταξινόμησης, καθώς η πολλαπλότητα των προσημασμένων διαφορών στις δύο ακολουθίες εμφανίζεται τον ίδιο ακριβώς αριθμό φορών ως διασταυρούμενες διαφορές σε αυτές. Αυτό μπορεί να φανεί σχηματίζοντας τα πολυσύνολα:

$$(\mathrm{D}^{+}_{A,1} \uplus \mathrm{D}^{-}_{A,1}) \& (\mathrm{D}^{+}_{B,1} \uplus \mathrm{D}^{-}_{B,1}) = [1, 2, 4, 5, 6, 7, 9, 11, 12, 13]$$
$$\mathrm{C}^{\rightrightarrows}_{A,1} \& \mathrm{C}^{\rightrightarrows}_{B,1} = [1, 2, 4, 5, 6, 7, 9, 11, 12, 13]$$

Παράδειγμα 5 (Συνέχεια του Παραδείγματος 4) Είναι προφανές, ότι οι ακολουθίες έχουν NPAF μηδέν, αν η στοιχείο προς στοιχείο σύγκριση των προηγούμενων πολυσυνόλων είναι αληθής για όλες τις θέσεις. Με άλλα λόγια, αν η επαλήθευση είναι αληθής για όλες τις θέσεις, δηλαδή είναι ένα πρόβλημα απόφασης [216].
Παρέχουμε επίσης τα διανύσματα NPAF των ακολουθιών A και B για μια ανεξάρτητη επαλήθευση:

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$N_A(s)$	0	0	0	0	-1	0	-1	0	0	0	-1	0	1	0	0	0	0	0
$N_B(s)$	0	0	0	0	1	0	1	0	0	0	1	0	-1	0	0	0	0	0
$N_A(s)+N_B(s)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Μέχρι στιγμής δώσαμε παραδείγματα επαλήθευσης συμβατών ακολουθιών όπου $\alpha = 0$, για τις περιπτώσεις PAF και NPAF. Υπάρχουν όμως κλάσεις συμβατών ακολουθιών, όπου $\alpha \neq 0$. Για παράδειγμα, ένα γενικευμένο ζεύγος Legendre (Generalized Legendre Pair, εν συντομία GL-Pair, βλ. επίσης και όγδοο κεφάλαιο), δυο ακολουθιών A και B μήκους ℓ ορίζεται ως $GL(\ell) := \{(A,B) : A,B \in \{-1,1\}^\ell,\ w(A)+w(B) = 2\ell,\ PAF_{A,B}(s) = -2,\ s = 1,\ldots,n-1\}$. Τότε, μπορούμε απλά να ελέγξουμε για $PAF_{A,B}(s) = -2 \Leftrightarrow [C]_s - [D]_s = 2$. Παρατηρούμε ότι και σε αυτήν την περίπτωση το πρόβλημα (επαλήθευσης) αν δυο ακολουθίες A και B σχηματίζουν ένα $GL(\ell)$ ζεύγος, δηλαδή έχουν PAF ίσο με -2, είναι ένα πρόβλημα απόφασης. Σημειώνουμε ότι, σε αυτήν την περίπτωση η διαφορά των συναρτήσεων καταμέτρησης εμφανίσεων, $[C]_s$ και $[D]_s$ (βλ. Ορισμό 5), για κάθε στοιχείο s των πολυσυνόλων C και D θα πρέπει να είναι ίση με 2. Σχετικά έχουμε το ακόλουθο παράδειγμα.

Παράδειγμα 6 Θεωρούμε το ακόλουθο GL(3) ζεύγος ακολουθιών που μπορεί να βρεθεί στην [50]:

```
A=++-
B=++-
```

Μπορούμε να επαληθεύσουμε αν οι ακολουθίες A, B έχουν PAF ίσο με -2 μέσω του Θεωρήματος 2. Χρησιμοποιούμε την αναπαράσταση των ακολουθιών μέσω των στηρίγματων τους, ως ακολούθως.

$$POS(A) = \{1,2\},\ NEG(A) = \{3\},\ \ POS(B) = \{1,2\},\ NEG(B) = \{3\}$$

Παράδειγμα 7 (Συνέχεια του Παραδείγματος 6) Πλέον, μπορούμε να σχηματίσουμε τα ακόλουθα έξι πολυσύνολα διαφορών για τις δύο ακολουθίες:

$$\begin{array}{cc} D_A^+ = [1,2] & D_B^+ = [1,2] \\ D_A^- = [\,] & D_B^- = [\,] \\ C_A = [2,1,1,2] & C_B = [2,1,1,2] \end{array}$$

Θεωρώντας την παράθεση και ταξινόμηση των στοιχείων των προηγούμενων πολυσυνόλων, έχουμε τα ακόλουθα πολυσύνολα:

$$D = (D_A^+ \uplus D_A^-)\&(D_B^+ \uplus D_B^-) = [1,1,2,2]$$
$$C = C_A \& C_B = [1,1,1,1,2,2,2,2]$$

Η διαφορά των συναρτήσεων καταμέτρησης εμφανίσεων $[C]_s$ και $[D]_s$ για $s \in \{1,2\}$ των πολυσυνόλων C και D είναι ίση με 2, δηλαδή $[C]_s = 4,\ [D]_s = 2,\ s \in \{1,2\} \Rightarrow [C]_s - [D]_s = 2,\ s \in \{1,2\}$. Συνεπώς, οι ακολουθίες A και B έχουν PAF ίσο με -2.
Παρέχουμε επίσης τα διανύσματα PAF των ακολουθιών A και B για μια ανεξάρτητη επαλήθευση:

s	1	2
$P_A(s)$	-1	-1
$P_B(s)$	-1	-1
$P_A(s) + P_B(s)$	-2	-2

Μια Ακραία Περίπτωση Επαλήθευση Συμβατών Ακολουθιών Στη συνέχεια, δίνουμε ένα ακραίο παράδειγμα επαλήθευσης της συμβατότητας δύο ακολουθιών A και B για NPAF μηδέν, και επιδεικνύουμε με αυτό τον τρόπο την ισχύ της νέας κωδικοποίησης της συνάρτησης αυτοσυσχέτισης μέσω του στηρίγματος των ακολουθιών. Τα τωρινά όρια των 32 και 64-bit υπολογιστικών μηχανών περιορίζουν την αναπαράσταση μιας λίστας τιμών στη διαθέσιμη μνήμη.

Με τη νέα κωδικοποίηση της συνάρτησης αυτοσυσχέτισης μπορούμε να επαληθεύσουμε τη συμβατότητα δύο ακολουθιών μήκους ίσο με 500 δισεκατομμύρια (billions), που αυτή τη στιγμή είναι ανέφικτο υπολογιστικά, αν υπολογίζαμε τη συνάρτηση αυτοσυσχέτισης μέσω της κλασικής περιγραφής της (βλ. [177] για προγραμματιστικές λεπτομέρειες).

Παράδειγμα 8 Έστω A, B δύο ακολουθίες μήκους $n = 500 \cdot 10^9$ και βάρους $w = 10$ με

$$SUP(A) = 10^9 \cdot [125, -150, -300, 425, 450]$$
$$SUP(B) = 10^9 \cdot [10, 100, 225, 275, -325]$$

Τα σύνολα του στηρίγματος μπορούν να γίνουν διαχωρίσιμα ως

$$POS(A) = 10^9 \cdot \{125, 425, 450\}, NEG(A) = 10^9 \cdot \{150, 300\}$$
$$POS(B) = 10^9 \cdot \{10, 100, 225, 275\}, NEG(B) = 10^9 \cdot \{325\}$$

Πλέον, μπορούμε να σχηματίσουμε τα ακόλουθα έξι πολυσύνολα διαφορών για τις δύο ακολουθίες:

$$D^+_{A,1} = 10^9 \cdot [300, 325, 25] \qquad D^+_{B,1} = 10^9 \cdot [100, 225, 275, 125, 175, 50]$$
$$D^-_{A,1} = 10^9 \cdot [150] \qquad D^-_{B,1} = [\,]$$
$$C^{\rightrightarrows}_{A,1} = 10^9 \cdot [275, 125, 300, 150, 25, 175] \qquad C^{\rightrightarrows}_{B,1} = 10^9 \cdot [325, 225, 100, 50]$$

Θεωρώντας την παράθεση των στοιχείων των προηγούμενων πολυσυνόλων, έχουμε τα ακόλουθα πολυσύνολα:

$$D^+_{A,1} \uplus D^-_{A,1} = 10^9 \cdot [300, 325, 25, 150]$$
$$D^+_{B,1} \uplus D^-_{B,1} = 10^9 \cdot [100, 225, 275, 125, 175, 50]$$
$$C^{\rightrightarrows}_{A,1} \uplus C^{\rightrightarrows}_{B,1} = 10^9 \cdot [275, 125, 300, 150, 25, 175, 325, 225, 100, 50]$$

Θεωρώντας τα απαιτούμενα πολυσύνολα όπως στο Πόρισμα 1, τα παραγόμενα πολυσύνολα είναι ίσα μετά από τη στοιχείο προς στοιχείο σύγκριση των στοιχείων τους,

$$(D^+_{A,1} \uplus D^-_{A,1}) \& (D^+_{B,1} \uplus D^-_{B,1}) = 10^9 \cdot [25, 50, 100, 125, 150, 175, 225, 275, 300, 325]$$
$$C^{\rightrightarrows}_{A,1} \& C^{\rightrightarrows}_{B,1} = 10^9 \cdot [25, 50, 100, 125, 150, 175, 225, 275, 300, 325]$$

και συνεπώς μπορούμε να αποφανθούμε ότι οι A, B σχηματίζουν ένα $TCP(500 \cdot 10^9, 10)$ ζεύγος ακολουθιών, καθώς έχουν NPAF μηδέν.

Κλείνουμε αυτήν την ενότητα, με την ακόλουθη παρατήρηση που αφορά την μέθοδο υλοποίησης της κωδικοποίησης της συνάρτησης αυτοσυσχέτισης σε μια υπολογιστική μηχανή.

Παρατήρηση 2 *Για μια άμεση επαλήθευση του Θεωρήματος 2 σε μια υπολογιστική μηχανή, είναι πιο βολικό να θεωρούμε τα παραγόμενα πολυσύνολα* C *και* D *ταξινομημένα, δηλαδή* $D = (D^+_A \uplus D^-_A) \& (D^+_B \uplus D^-_B)$ *και* $C = C_A \& C_B$.

§1.3 Ανάλυση Πολυπλοκότητας της Συνάρτησης Αυτοσυσχέτισης Συμβατών Ακολουθιών

Σε αυτήν την ενότητα, πραγματοποιείται μια μελέτη της πολυπλοκότητας του προβλήματος απόφασης αν δυο τριαδικές ακολουθίες έχουν σταθερή αυτοσυσχέτιση. Για να μπορέσουμε να συγκρίνουμε την αποδοτικότητα της προτεινόμενης κωδικοποιήσης της συνάρτησης αυτοσυσχέτισης, που αναπτύξαμε στην προηγούμενη ενότητα, θα αναλύσουμε τους αλγορίθμους που χρειάζονται κατά των υπολογισμό της AF. Υπάρχουν τρεις διακεκριμένες φάσεις, που λαμβάνουν μέρος, σε αυτόν τον υπολογισμό (βλ. και Αλγόριθμο 1):

- Φάση Αναπαράστασης (Representation Phase) (Μέσω ακολουθιών ή του στηρίγματος αυτών)
- Φάση Υπολογισμού (Computation Phase) (Μέσω των αθροισμάτων ή των διαφορών)
- Φάση Επαλήθευσης (Verification Phase) (Μέσω διανυσμάτων AF ή ταξινόμησης λιστών)

Η ανάλυση ενός αλγορίθμου εμπεριέχει τον καθορισμό των βημάτων που απαιτούνται για την εκτέλεση αυτού (του αλγορίθμου). Θα κάνουμε χρήση βασικών εργαλείων της ασυμπτοτικής ανάλυσης, όπως είναι ο ασυμπτωτικός συμβολισμός big-$\mathcal{O}$ notation, βλ. [87], έτσι ώστε να κατανοήσουμε το ρυθμό αύξησης (growth rate) του χρόνου εκτέλεσης του αλγορίθμου, καθώς η είσοδος του μεγαλώνει. Από τις [87, 130], θα προσπαθήσουμε να εκφράσουμε το χρόνο εκτέλεσης του αλγορίθμου ως μια συνάρτηση των πράξεων που απαιτούνται κατά τη διάρκεια εκτέλεσης τους. Καθώς το πρόβλημά μας περιλαμβάνει δύο παραμέτρους για ένα υποψήφιο ζεύγος συμβατών ακολουθιών (το μήκος και το βάρος αυτών), η πολυπλοκότητα θα εκφραστεί ως μια συνάρτηση του μήκους n και του βάρους w που είναι και οι παράμετροι εισόδου. Ενδιαφερόμαστε για την πολυπλοκότητα χείριστης περίπτωσης (worst-case complexity), δηλαδή εκείνης όπου εξάγουμε ένα άνω φράγμα στο χρόνο εκτέλεσης ενός αλγορίθμου, για κάθε δυνατό στιγμιότυπο εισόδου. Μια μελέτη

πολυπλοκότητας μέσης περίπτωσης (average-case complexity) για συμβατές ακολουθίες, πρόσφατα παρουσιάστηκε στην [151]. Συνεπώς, η αποδοτικότητα των αλγορίθμων αυτής της ενότητας θα συγκριθεί μέσω των αντιστοίχων πολυπλοκοτήτων αυτών.

Είναι προφανές ότι για να μπορέσουμε να συγκρίνουμε την αποδοτικότητα των αλγορίθμων, θα πρέπει αυτή η σύγκριση να πραγματοποιηθεί στο ίδιο στιγμιότυπο εισόδου. Στην περίπτωση μας, το πρόβλημα απόφασης θα πρέπει να έχει ως είσοδο είτε δύο υποψήφιες συμβατές ακολουθίες ή τα στηρίγματα αυτών. Όταν ως είσοδος μας δίνονται υποψήφιες συμβατές ακολουθίες θα αναφερόμαστε στο πρόβλημα, ως το *πρόβλημα ακολουθιών (sequence problem)*, ενώ αν μας δίνονται τα στηρίγματα των ακολουθιών θα αναφερόμαστε στο πρόβλημα ώς το *πρόβλημα στηρίγματος (support problem)*. Σημειώνουμε ότι, για την μελέτη της πολυπλοκότητας δεν θα λάβουμε υπόψιν κάποιο συγκεκριμένο αριθμητικό μοντέλο υπολογισμού και κατά συνέπεια θα μετράμε όλες τις βασικές πράξεις (συγκρίσεις, προσθετικούς και πολλαπλασιαστικούς τελεστές, ανάθεση και καταχώρηση μεταβλητής) που εκτελεί ο αλγόριθμος το ίδιο.

§1.3.1 Φάση Αναπαράστασης

Σε αυτήν την ενότητα, δίνουμε δυο αλγορίθμους που μετασχηματίζουν το στιγμιότυπο εισόδου από τη μια μορφή στην άλλη, δηλαδή, το πρόβλημα ακολουθιών στο πρόβλημα στηρίγματος και αντίστροφα.

Algorithm 2 SEQUENCE2SUPPORT ALGORITHM

```
  function SEQ2SUP(A)
Require: A is a {0, ±1} sequence of length n
    j ← 0
    k ← 0
    n ← |A|
    for i ← 1 to n do
      if A[i] = 1 then
        POS(A)[j] ← i
        j ← j + 1
      else if A[i] = −1 then
        NEG(A)[k] ← i
        k ← k + 1
      end if
    end for
  return (POS(A), NEG(A))
  end function
```

Εξάγουμε μια ασυμπτωτική εκτίμηση της χείριστης περίπτωσης που τρέχει ο Αλγόριθμος 2, δηλαδή ενδιαφερόμαστε για την εύρεση ενός άνω φράγματος στο χρόνο εκτέλεσης του αλγοριθμου (ανάλυση χείριστης περίπτωσης, [87, 130]) .

Πρόταση 1 *Ο αλγόριθμος* SEQUENCE2SUPPORT *εκτελεί* $T_{SEQ2SUP}(n) = 4n + \mathcal{O}(1)$ *πράξεις και τρέχει σε* $\mathcal{O}(n)$ *χρόνο.*

Απόδειξη. Για κάθε βήμα του αλγορίθμου έχουμε το πολύ 2 συγκρίσεις και 2 καταχωρήσεις μεταβλητών. Αρά ο συνολικός αριθμός των πράξεων που χρείαζονται, κατά την εκτέλεση του αλγορίθμου είναι $T_{SEQ2SUP}(n) = 3 + 4n$. □

Παρόμοια, δίνουμε τον Αλγόριθμο 3 για να παράγουμε τις ακολουθίες από τα στηρίγματα τους.

Algorithm 3 SUPPORT2SEQUENCE ALGORITHM

```
  procedure Sup2Seq(SUP(A))
Require: SUP(A) is a set of integer values of length ≤ w
    w ← max|SUP(A)|
    for i ← 1 to w do
      if SUP(A)[i] < 0 then
        A[SUP(A)[i]] ← −1
      else if SUP(A)[i] > 0 then
        A[SUP(A)[i]] ← 1
      else
        A[i] ← 0
      end if
    end for
  return A
  end procedure
```

Πρόταση 2 *Ο αλγόριθμος* SUPPORT2SEQUENCE *εκτελεί* $T_{SUP2SEQ}(w) = 3w + \mathcal{O}(1)$ *πράξεις και τρέχει σε* $\mathcal{O}(w)$ *χρόνο.*

Απόδειξη. Για κάθε βήμα του αλγορίθμου έχουμε το πολύ 2 συγκρίσεις και 1 καταχώρηση μεταβλητής. Άρα ο συνολικός αριθμός των πράξεων που χρείαζονται, κατά την εκτέλεση του αλγορίθμου είναι $T_{SUP2SEQ}(w) = 1 + 3w$. Σημειώνουμε ότι, ο χρόνος εκτέλεσης του αλγορίθμου είναι συνάρτηση του βάρους w της παραγόμενης ακολουθίας. □

§1.3.2 Φάση Υπολογισμού

Στην επόμενη βάση του υπολογισμού της συνάρτησης αυτοσυσχέτισης δίνουμε αλγορίθμους, που υπολογίζουν το διάνυσμα AF μιας ακολουθίας μέσω της σχέσης (1.1). Ιδιαίτερα, θα δώσουμε αλγορίθμους για τον υπολογισμό του PAF αλλά και του NPAF μιας ακολουθίας και στη συνέχεια θα εξάγουμε έναν αλγόριθμο για τη γενική περίπτωση της AF. Θα θέλαμε να παρατηρήσουμε σε αυτό το σημείο ότι θα επαρκούσε ο σχεδιασμός αλγορίθμων μόνο για την περίπτωση του NPAF λόγω της ύπαρξης της παρακάτω συμμετρικής σχέσης που συνδέει τη περιοδική με τη μη-περιοδική συνάρτηση αυτοσυσχέτισης μια ακολουθίας A,

$$PAF_A(s) = NPAF_A(s) + NPAF_A(n-s),\ s = 1, \ldots, n-1.$$

Συνεπώς, όταν μια ακολουθία έχει NPAF μηδέν, συνεπάγεται ότι έχει και PAF μηδέν. Παρόλα αυτά, το αντίστροφο δεν ισχύει και επιπλέον στην περίπτωση των συμβατών ακολουθιών ενδιαφερόμαστε για κλάσεις ακολουθιών συγκεκριμένης αυτοσυσχέτισης κάθε φορά.

Αρχικά δίνουμε τον Αλγόριθμο 4, ο οποίος υπολογίζει το διάνυσμα NPAF μιας ακολουθίας.

Algorithm 4 NPAFVector Algorithm

```
  procedure NPafVec(A)
Require: A is finite sequence of length n
    for s ← 1 to n − 1 do
      NPAF(A)[s] ← NPafS(A, s)
    end for
  return NPAF(A)
  end procedure

  procedure NPafS(A,s)                    ▷ NPafS computes the NPAF of A in s
Require: A is finite sequence of length n
    N_A ← 0
    n ← |A|
    for i ← 1 to n − s do
      N_A ← N_A + A[i] ∗ A[i + s]
    end for
  return N_A
  end procedure
```

Πρόταση 3 *Ο αλγόριθμος* NPAFVector *εκτελεί* $T_{NPAFVEC}(n) = 2n^2 + \mathcal{O}(n)$ *πράξεις και τρέχει σε* $\mathcal{O}(n^2)$ *χρόνο.*

Απόδειξη. Αρχικά, υπολογίζουμε το χρόνο εκτέλεσης $T_{N_A(s)}(n)$ του NPAF της A για δεδομένο s. Μετράμε ότι μπορούν να συμβούν 2 προσθέσεις, 1 πολλαπλασιασμός και 1 καταχώρηση μεταβλητής, συνολικά 4 πράξεις σε κάθε ένα από τα $n-s$ βήματα. Συνεπώς, ο χρόνος εκτέλεσης είναι $T_{N_A(s)}(n) = 4(n-s)+2$ και εξαρτάται από τη θέση s. Καθώς το $N_A(s)$ καλείται στο κυρίως σώμα του αλγορίθμου NPAFVector, χρειαζόμαστε $\mathcal{O}(n)$ μνήμη για να το διαβάσουμε ως είσοδο αφού το μήκος της ακολουθίας είναι n. Υπολογίζουμε το συνολικό χρόνο εκτέλεσης του αλγορίθμου ως $T_{NPAFVEC}(n) = \sum_{s=1}^{n-1} T_{N_A(s)}(n) + \mathcal{O}(n) = \sum_{s=1}^{n-1}(4(n-s)+2) + \mathcal{O}(n) = 2n^2 - 2 + \mathcal{O}(n) = 2n^2 + \mathcal{O}(1) + \mathcal{O}(n) = 2n^2 + \mathcal{O}(n)$.

□

Αντίστοιχα, δίνουμε τον Αλγόριθμο 5, ο οποίος υπολογίζει το διάνυσμα PAF μιας ακολουθίας.

Algorithm 5 PAFVector Algorithm

```
  procedure PafVec(A)
Require: A is finite sequence of length n
    for s ← 1 to n − 1 do
      PAF(A)[s] ← PafS(A, s)
    end for
  return PAF(A)
  end procedure

  procedure PafS(A,s)                          ▷ PafS computes the PAF of A in s
Require: A is finite sequence of length n
    P_A ← 0
    n ← |A|
    for i ← 1 to n do
      P_A ← P_A + A[i] ∗ A[((i + s − 1) mod n) + 1]
    end for
  return P_A
  end procedure
```

Πρόταση 4 *Ο αλγόριθμος* PAFVector *εκτελεί* $T_{PAFVEC}(n) = 7n^2 + \mathcal{O}(n)$ *πράξεις και τρέχει σε* $\mathcal{O}(n^2)$ *χρόνο.*

Απόδειξη. Αντίστοιχα, υπολογίζουμε το χρόνο εκτέλεσης $T_{P_A(s)}(n)$ του PAF της A για δεδομένο s. Μετράμε ότι μπορούν να συμβούν, 3 προσθέσεις, 1 αφαίρεση, 1 πολλαπλασιασμός, 1 modulo πράξη και 1 καταχώρηση μεταβλητής, συνολικά 7 πράξεις για καθένα από τα n βήματα. Συνεπώς, ο χρόνος εκτέλεσης είναι $T_{P_A(s)}(n) = 7n + 2$ και είναι ανεξάρτητος από τη θέση s. Καθώς το $P_A(s)$ καλείται στο κυρίως σώμα του αλγορίθμου PAFVector, χρειαζόμαστε $\mathcal{O}(n)$ μνήμη για να το διαβάσουμε ως είσοδο αφού το μήκος της ακολουθίας είναι n. Υπολογίζουμε το συνολικό χρόνο εκτέλεσης του αλγορίθμου ως $T_{PAFVEC}(n) = \sum_{s=1}^{n-1} T_{P_A(s)}(n) + \mathcal{O}(n) = T_{P_A(1)}(n) + \ldots + T_{P_A(n-1)}(n) + \mathcal{O}(n) = (n-1)(7n+2) + \mathcal{O}(n) = 7n^2 - 5n - 2 + \mathcal{O}(n) = 7n^2 - 5n + \mathcal{O}(1) + \mathcal{O}(n) = 7n^2 + \mathcal{O}(n)$. □

Στη συνέχεια, δίνουμε έναν αλγόριθμο για τη γενική περίπτωση του διανύσματος AF, εκφρασμένο μέσω των Αλγορίθμων 4 και 5.

Algorithm 6 AFVector Algorithm

```
  function AfVec(A, flag)
Require: A is finite sequence of length n
    if flag = NPAF then
      AF(A) ← NPAFVec(A)
  return AF(A)
    else if flag = PAF then
      AF(A) ← PAFVec(A)
  return AF(A)
    end if
  end function
```

Πόρισμα 2 *Ο αλγόριθμος* AFVector *τρέχει σε* $\mathcal{O}(n^2)$ *χρόνο.*

Απόδειξη. Σε αυτή την περίπτωση, ο χρόνος εκτέλεσης του αλγορίθμου AFVector είναι το μέγιστο των χρόνων εκτέλεσης των αλγορίθμων NPAFVector και PAFVector, δηλαδή εκφράζεται μέσω του $\max\{T_{NPAFVEC}(n), T_{PAFVEC}(n)\} = \max\{2n^2 + \mathcal{O}(n), 7n^2 + \mathcal{O}(n)\} \in \mathcal{O}(n^2)$. □

Όπως και στη φάση της αναπαράστασης, δίνουμε τον Αλγόριθμο 7 για να υπολογίσουμε το NPAF μιας ακολουθίας A που αναπαριστάται μέσω του στηρίγματος της, το οποίο ορίζεται μέσω των προσημασμένων διαφορών $D^{+}_{A,1}, D^{-}_{A,1}$ και των διασταυρούμενων διαφορών $C^{\rightrightarrows}_{A,1} = D^{\pm}_{A,1} \uplus D^{\mp}_{A,1}$.

Algorithm 7 NPAFSUPPORT ALGORITHM

function NPAFSUP($POS(A), NEG(A), n$)
Require: $(POS(A), NEG(A))$ are sets of positive values of length $\leq w$
  $w^+ \leftarrow \max|POS(A)|$
  $w^- \leftarrow \max|NEG(A)|$
  for $x \leftarrow 1$ **to** $w^+ - 1$ **do** ▷ Construction of the multiset $D^+_{A,1}$
    for $y \leftarrow x+1$ **to** w^+ **do**
      if $POS(A)[x] > POS(A)[y]$ **then**
        $D^+_{A,1} \leftarrow POS(A)[x] - POS(A)[y]$
      end if
    end for
  end for
  for $x \leftarrow 1$ **to** $w^- - 1$ **do** ▷ Construction of the multiset $D^-_{A,1}$
    for $y \leftarrow x+1$ **to** w^- **do**
      if $NEG(A)[x] > NEG(A)[y]$ **then**
        $D^-_{A,1} \leftarrow NEG(A)[x] - NEG(A)[y]$
      end if
    end for
  end for
  for $x \leftarrow 1$ **to** w^+ **do** ▷ Construction of the multiset $D^\pm_{A,1}$
    for $y \leftarrow 1$ **to** w^- **do**
      if $POS(A)[x] > NEG(A)[y]$ **then**
        $D^\pm_{A,1} \leftarrow POS(A)[x] - NEG(A)[y]$
      end if
    end for
  end for
  for $x \leftarrow 1$ **to** w^- **do** ▷ Construction of the multiset $D^\mp_{A,1}$
    for $y \leftarrow 1$ **to** w^+ **do**
      if $NEG(A)[x] > POS(A)[y]$ **then**
        $D^\mp_{A,1} \leftarrow NEG(A)[x] - POS(A)[y]$
      end if
    end for
  end for
  $C^\rightrightarrows_{A,1} \leftarrow$ JOIN$(D^\pm_{A,1}, D^\mp_{A,1})$ ▷ Construction of the multiset $C^\rightrightarrows_{A,1}$
return $(D^+_{A,1}, D^-_{A,1}, C^\rightrightarrows_{A,1})$
end function

Πρόταση 5 *Ο αλγόριθμος* NPAFSUPPORT *εκτελεί* $\mathsf{T}_{\mathsf{NPAFSUP}}(w) = \frac{9}{2}w^2 + \mathcal{O}(w)$ *πράξεις και τρέχει σε* $\mathcal{O}(w^2)$ *χρόνο.*

Απόδειξη. Σημειώνουμε ότι τα $w^+, w^- \leq w$, δηλαδή οι πληθικότητες των $\mathsf{POS}(A), \mathsf{NEG}(A)$ είναι φραγμένες από το βάρος w της ακολουθίας A, καθώς $w^+ + w^- = w$. Εφόσον ενδιαφερόμαστε για τη χείριστη περίπτωση θα θεωρήσουμε το μέγιστο αριθμό επαναλήψεων που λαμβάνουν μέρος στην κάθε κατασκευή των πολυσυνόλων. Στη συνέχεια υπολογίζουμε το χρόνο εκτέλεσης για καθένα από τα πολυσύνολα που κατασκευάζει ο αλγόριθμος NPAFSUPPORT ως ακολούθως:

- Για κάθε επανάληψη στην κατασκευή του πολυσυνόλου $\mathsf{D}^{+}_{A,1}$ έχουμε 1 σύγκριση, 1 αφαίρεση και 1 καταχώρηση μεταβλητής. Καθώς ο αριμός των επαναλήψεων είναι ίσος με $\frac{w^+(w^+-1)}{2}$, ο συνολικός αριθμός των πράξεων που εκτελούνται είναι $\frac{3w^+(w^+-1)}{2}$.

- Με παρόμοιο επιχείρημα για τις $\frac{w^-(w^--1)}{2}$ επαναλήψεις που εκτελούνται στην κατασκευή του πολυσυνόλου $\mathsf{D}^{-}_{A,1}$ έχουμε $\frac{3w^-(w^--1)}{2}$ επιπλέον πράξεις.

- Για τα πολυσύνολα $\mathsf{D}^{\pm}_{A,1}, \mathsf{D}^{\mp}_{A,1}$ έχουμε $3w^+w^-$ πράξεις για το καθενα, καθώς ο ίδιος τύπος πράξεων εκτελείται σε κάθε μια από τις w^+w^- επαναλήψεις.

Θεωρούμε ότι η παράθεση των στοιχείων στην κατασκευή των πολυσυνόλων $\mathsf{C}^{\rightleftarrows}_{A,1}$ καταλαμβάνει $\mathcal{O}(w)$ μνήμη. Συνεπώς, ο χρόνος εκτέλεσης του αλγορίθμου NPAFSUPPORT δίνεται από την σχέση, $\mathsf{T}_{\mathsf{NPAFSUP}}(w) = \frac{3}{2}(w^+(w^+-1)+w^-(w^--1))+6w^+w^-+\mathcal{O}(w) = \frac{3}{2}(w^2-w)+3w^+w^-+\mathcal{O}(w) = \frac{9}{2}w^2 - \frac{3w}{2} + \mathcal{O}(w) = \frac{9}{2}w^2 + \mathcal{O}(w)$. Σημείωνουμε ότι, όπως και στην περίπτωση του αλγορίθμου SUPPORT2SEQUENCE, ο αλγόριθμος NPAFSUPPORT εξαρτάται μόνο από το βάρος w της ακολουθίας. Συνεπώς, αποδεικνύουμε ότι αυτή η μέθοδος κωδικοποίησης της μη-περιοδικής συνάρτησης αυτοσυσχέτισης εξαρτάται μόνο από τα μη-μηδενικά στοιχεία της ακολουθίας, για την οποία υπολογίζεται.

□

Αντίστοιχα, δίνουμε τον Αλγόριθμο 8 για να υπολογίσουμε το PAF μιας ακολουθίας A που αναπαριστάται μέσω του στηρίγματος της, το οποίο ορίζεται μέσω των προσημασμένων διαφορών $\mathsf{D}^{+}_{A,2}, \mathsf{D}^{-}_{A,2}$ και των διασταυρούμενων διαφορών $\mathsf{C}^{\rightleftarrows}_{A,2} = \mathsf{D}^{\pm}_{A,2} \uplus \mathsf{D}^{\mp}_{A,2}$.

Algorithm 8 PAFSupport Algorithm

function PafSup($\mathrm{POS}(A), \mathrm{NEG}(A), n$)
Require: $(\mathrm{POS}(A), \mathrm{NEG}(A))$ are sets of positive values of length $\leq w$
  $w^+ \leftarrow \max|\mathrm{POS}(A)|$
  $w^- \leftarrow \max|\mathrm{NEG}(A)|$
  for $x \leftarrow 1$ **to** w^+ **do** ▷ Construction of the multiset $D^+_{A,2}$
    for $y \leftarrow 1$ **to** w^+ **do**
      if $\mathrm{POS}(A)[x] \neq \mathrm{POS}(A)[y]$ **then**
        $D^+_{A,2} \leftarrow (\mathrm{POS}(A)[x] - \mathrm{POS}(A)[y]) \pmod n$
      end if
    end for
  end for
  for $x \leftarrow 1$ **to** w^- **do** ▷ Construction of the multiset $D^-_{A,2}$
    for $y \leftarrow 1$ **to** w^- **do**
      if $\mathrm{NEG}(A)[x] \neq \mathrm{NEG}(A)[y]$ **then**
        $D^-_{A,2} \leftarrow (\mathrm{NEG}(A)[x] - \mathrm{NEG}(A)[y]) \pmod n$
      end if
    end for
  end for
  for $x \leftarrow 1$ **to** w^+ **do** ▷ Construction of the multiset $D^{\pm}_{A,2}$
    for $y \leftarrow 1$ **to** w^- **do**
      $D^{\pm}_{A,2} \leftarrow (\mathrm{POS}(A)[x] - \mathrm{NEG}(A)[y]) \pmod n$
    end for
  end for
  for $x \leftarrow 1$ **to** w^- **do** ▷ Construction of the multiset $D^{\mp}_{A,2}$
    for $y \leftarrow 1$ **to** w^+ **do**
      $D^{\mp}_{A,2} \leftarrow (\mathrm{NEG}(A)[x] - \mathrm{POS}(A)[y]) \pmod n$
    end for
  end for
  $C^{\rightleftarrows}_{A,2} \leftarrow$ Join$(D^{\pm}_{A,2}, D^{\mp}_{A,2})$ ▷ Construction of the multiset $C^{\rightleftarrows}_{A,2}$
return $(D^+_{A,2}, D^-_{A,2}, C^{\rightleftarrows}_{A,2})$
end function

Πρόταση 6 *Ο αλγόριθμος* PAFSUPPORT *εκτελεί* $\mathsf{T}_{\mathsf{PAFSUP}}(w) = 14w^2 + \mathcal{O}(w)$ *πράξεις και τρέχει σε* $\mathcal{O}(w^2)$ *χρόνο.*

Απόδειξη. Σημειώνουμε ότι τα $w^+, w^- \leq w$, δηλαδή οι πληθικότητες των $\mathsf{POS}(A), \mathsf{NEG}(A)$ είναι φραγμένες από το βάρος w της ακολουθίας A, καθώς $w^+ + w^- = w$. Εφόσον ενδιαφερόμαστε για τη χείριστη περίπτωση θα θεωρήσουμε ένα μέγιστο αριθμό επαναλήψεων, w^2, που λαμβάνουν μέρος στην κάθε κατασκευή των πολυσυνόλων. Στη συνέχεια υπολογίζουμε το χρόνο εκτέλεσης για καθένα από τα πολυσύνολα που κατασκευάζει ο αλγόριθμος PAFSUPPORT ως ακολούθως:

- Για κάθε επανάληψη στην κατασκευή του πολυσυνόλου $\mathsf{D}^+_{A,2}$ έχουμε 1 σύγκριση, 1 αφαίρεση, 1 modulo πράξη και 1 καταχώρηση μεταβλητής. Καθώς ο αριμός των επαναλήψεων είναι ίσος με $4w^2$, ο συνολικός αριθμός των πράξεων που εκτελούνται είναι $4w^2$.
- Με παρόμοιο επιχείρημα για τις $4w^2$ επαναλήψεις που εκτελούνται στην κατασκευή του πολυσυνόλου $\mathsf{D}^-_{A,2}$ έχουμε $4w^2$ επιπλέον πράξεις.
- Για τα πολυσύνολα $\mathsf{D}^{\pm}_{A,2}, \mathsf{D}^{\mp}_{A,2}$ έχουμε $3w^2$ πράξεις για το καθενα, καθώς ο ίδιος τύπος πράξεων εκτελείται σε κάθε μια από τις w^+w^- επαναλήψεις.

Θεωρούμε ότι η παράθεση των στοιχείων στην κατασκευή των πολυσυνόλων $\mathsf{C}^{\rightleftarrows}_{A,2}$ καταλαμβάνει $\mathcal{O}(w)$ μνήμη. Συνεπώς, ο χρόνος εκτέλεσης του αλγορίθμου PAFSUPPORT δίνεται από την σχέση, $\mathsf{T}_{\mathsf{PAFSUP}}(w) = 2 + (4+4+3+3)w^2 + \mathcal{O}(w) = 14w^2 + \mathcal{O}(w)$. Σημείωνουμε ότι, όπως και στην περίπτωση του αλγορίθμου SUPPORT2SEQUENCE, ο αλγόριθμος PAFSUPPORT εξαρτάται μόνο από το βάρος w της ακολουθίας. Συνεπώς, αποδεικνύουμε ότι άυτή η μέθοδος κωδικοποίησης της περιοδικής συνάρτησης αυτοσυσχέτισης εξαρτάται μόνο από τα μη-μηδενικά στοιχεία της ακολουθίας, για την οποία υπολογίζεται.

□

Στη συνέχεια, δίνουμε έναν αλγόριθμο για τη γενική περίπτωση των προσημασμένων $(\mathsf{D}^+_A, \mathsf{D}^-_A)$ και διασταυρούμενων διαφορών $(\mathsf{C}_A = \mathsf{D}^{\pm}_A \uplus \mathsf{D}^{\mp}_A)$ της AF, εκφρασμένο μέσω των Αλγορίθμων 7 και 8.

Algorithm 9 AFSupport Algorithm

function AfSup(POS(A), NEG(A), n, flag)
Require: (POS(A), NEG(A)) are sets of positive values of length $\leq w$
  if flag = NPAF **then**
    $(D^{+}_{A,1}, D^{-}_{A,1}, C^{\rightrightarrows}_{A,1}) \leftarrow$ NPAFSup(POS(A), NEG(A), n)
    $(D^{+}_{A}, D^{-}_{A}, C_{A}) \leftarrow (D^{+}_{A,1}, D^{-}_{A,1}, C^{\rightrightarrows}_{A,1})$
  return $D^{+}_{A}, D^{-}_{A}, C_{A}$
  else if flag = PAF **then**
    $(D^{+}_{A,2}, D^{-}_{A,2}, C^{\rightleftarrows}_{A,2}) \leftarrow$ PAFSup(POS(A), NEG(A), n)
    $(D^{+}_{A}, D^{-}_{A}, C_{A}) \leftarrow (D^{+}_{A,2}, D^{-}_{A,2}, C^{\rightleftarrows}_{A,2})$
  return $D^{+}_{A}, D^{-}_{A}, C_{A}$
  end if
end function

Πόρισμα 3 *Ο αλγόριθμος* AFSupport *τρέχει σε* $\mathcal{O}(w^2)$ *χρόνο.*

Απόδειξη. Σε αυτήν την περίπτωση, ο χρόνος εκτέλεσης του αλγορίθμου AFSupport είναι το μέγιστο των χρόνων εκτέλεσης των αλγορίθμων NPAFSupport και PAFSupport, δηλαδή εκφράζεται μέσω του $\max\{T_{\text{NPAFSUP}}(w), T_{\text{PAFSUP}}(w)\} = \max\{\frac{9}{2}w^2 + \mathcal{O}(w), 14w^2 + \mathcal{O}(w)\} \in \mathcal{O}(w^2)$. □

§1.3.3 Φάση Επαλήθευσης

Στην τελευταία φάση της επαλήθευσης, δηλαδή εκείνης κατά της οποίας δίνονται οι ακολουθίες ή τα στηρίγματα τους και ελέγχουμε για τη συμβατότητα αυτών. Αρχικά, δίνουμε τον Αλγόριθμο 10, ο οποίος ελέγχει αν οι ακολουθίες έχουν σταθερό NPAF ίσο με α. Σημειώνουμε ότι, ο αλγόριθμος αυτός χρειάζεται δύο ακολουθίες ως είσοδο και την τιμή της σταθεράς α. Οι επιτρεπτές τιμές για την σταθερά α είναι $0, 1, \ldots, 2n$, όπου n το μήκος των ακολουθιών.

Πρόταση 7 *Ο αλγόριθμος* NPAFVectorVerification *εκτελεί* $T_{\text{NPAFVECVER}}(n) = 2n + \mathcal{O}(1)$ *πράξεις και τρέχει σε* $\mathcal{O}(n)$ *χρόνο.*

Απόδειξη. Μπορούν να συμβούν το πολύ $n-1$ συγκρίσεις και $n-1$ δίτιμες (boolean) καταχωρήσεις μεταβλητών. Συνεπώς, ο συνολικός

Algorithm 10 NPAFVectorVerification Algorithm

```
procedure NPafVecVer(NPAF(A), NPAF(B), α)
Require: NPAF(A), NPAF(B) are integer arrays of length n − 1
Require: α ∈ {0, 1, ..., 2n}
    for i ← 1 to n − 1 do
        if NPAF(A)[i] + NPAF(B)[i] = α then
            bool ← true
        else
            bool ← false
                break
        end if
    end for
return (bool)
end procedure
```

χρόνος εκτέλεσης του αλγορίθμου είναι $T_{NPAFVECVER}(n) = 2n - 2 = 2n + \mathcal{O}(1)$. □

Αντίστοιχα, δίνουμε τον Αλγόριθμο 11 για να ελέγξουμε αν οι ακολουθίες έχουν σταθερό PAF ίσο με α, όπως και προηγουμένως.

Algorithm 11 PAFVectorVerification Algorithm

```
procedure PafVecVer(PAF(A), PAF(B), α)
Require: PAF(A), PAF(B) are integer arrays of length n − 1
Require: α ∈ {0, 1, ..., 2n}
    for i ← 1 to n − 1 do
        if PAF(A)[i] + PAF(B)[i] = α then
            bool ← true
        else
            bool ← false
                break
        end if
    end for
return (bool)
end procedure
```

Πρόταση 8 *Ο αλγόριθμος* PAFVectorVerification *εκτελεί* $T_{PAFVECVER}(n) = 2n + \mathcal{O}(1)$ *πράξεις και τρέχει σε* $\mathcal{O}(n)$ *χρόνο.*

Απόδειξη. Όμοιως, μπορούν να συμβούν το πολύ $n - 1$ συγκρίσεις και $n - 1$ δίτιμες (boolean) καταχωρήσεις μεταβλητών. Συνεπώς, όπως και στην περίπτωση του NPAF, ο συνολικός χρόνος εκτέλεσης του αλγορίθμου είναι $T_{PAFVECVER}(n) = 2n - 2 = 2n + O(1)$.

□

Στη συνέχεια, δίνουμε έναν αλγόριθμο για τη γενική περίπτωση όταν θέλουμε να ελέγξουμε αν οι ακολουθίες έχουν σταθερή PAF ίση με α, εκφρασμένο μέσω των Αλγορίθμων 10 και 11.

Algorithm 12 AFVectorVerification Algorithm

function AfSup(POS(A), NEG(A), α, flag)
Require: PAF(A), PAF(B) are integer arrays of length $n-1$
Require: $\alpha \in \{0, 1, \ldots, 2n\}$
  if flag = NPAF **then**
    bool $\leftarrow$ NPafVecVer(NPAF(A), NPAF(B), α)
return (bool)
  else if flag = PAF **then**
    bool $\leftarrow$ NPafVecVer(NPAF(A), NPAF(B), α)
return (bool)
  end if
end function

Πόρισμα 4 *Ο αλγόριθμος* AFVectorVerification *τρέχει σε* $\mathcal{O}(n)$ *χρόνο.*

Απόδειξη. Σε αυτή την περίπτωση, ο χρόνος εκτέλεσης του αλγορίθμου AFVectorVerification είναι το μέγιστο των χρόνων εκτέλεσης των αλγορίθμων NPAFVectorVerification και PAFVectorVerification, δηλαδή εκφράζεται μέσω του $\max\{T_{NPAFVECVER}(n), T_{PAFVECVER}(n)\} = \max\{2n + \mathcal{O}(1), 2n + \mathcal{O}(1)\} \in \mathcal{O}(n)$.

□

Τελικά, δίνουμε τον Αλγόριθμο 13, ο οποίος είναι μια άμεση υλοποίηση του Πορίσματος 1 για την περίπτωση της επαλήθευσης του NPAF για $\alpha = 0$. Όπως έχουμε ήδη δει από προηγούμενη ενότητα, το πρόβλημα επαλήθευσης συμβατών ακολουθιών έχει μετασχηματιστεί σε ένα συγκριτικό πρόβλημα ταξινόμησης. Παρόλο που υπάρχει μεγάλη ποικιλία αλγορίθμων ταξινόμησης, βλ. για παράδειγμα [129], θα θεωρήσουμε τον αλγόριθμο ταξινόμησης που χρησιμοποιήσαμε ως "μαύρο κουτί", και ότι εκτελεί $n \log n$ πράξεις, τρέχει σε $\mathcal{O}(n \log n)$ χρόνο και τέλος ότι απαιτείται $\mathcal{O}(n)$ μνήμη για την ταξινόμηση n εγγραφών, για παράδειγμα ταξινόμηση λίστας μήκους n, στη χείριστη περίπτωση. Αλγόριθμοι αυτής της κατηγορίας είναι n heapsort, introsort και διάφοροι άλλοι [129].

Algorithm 13 NPAFSupportVerification Algorithm

```
procedure NPafSupVer(D+_{A,1}, D-_{A,1}, C⇉_{A,1}, D+_{B,1}, D-_{B,1}, C⇉_{B,1}, α)
Require: D+_{A,1}, D-_{A,1}, C⇉_{A,1}, D+_{B,1}, D-_{B,1}, C⇉_{B,1} are arrays of length ≤ w^2
Require: α ∈ {0, 1, ..., 2n}
    maxlen ← max(|C⇉_{A,1}| + |C⇉_{B,1}|)
    lhs ← Sort([D+_{A,1}, D-_{A,1}, D+_{B,1}, D-_{B,1}])
    rhs ← Sort([C⇉_{A,1}, D⇉_{B,1}])
    for i ← 1 to maxlen do
        if lhs[i] − rhs[i] = α then
            bool ← true
        else
            bool ← false
                break
        end if
    end for
return (bool)
end procedure
```

Πρόταση 9 *Ο αλγόριθμος* NPAFSupportVerification *εκτελεί* $T_{\text{NPAFSUPVER}}(w) = 4w^2 \log w + \mathcal{O}(w^2)$ *πράξεις και τρέχει σε* $\mathcal{O}(w^2 \log w)$ *χρόνο.*

Απόδειξη. Η μέγιστη πληθικότητα των πολυσυνόλων είναι της τάξης $\mathcal{O}(w^2)$ όπου w είναι η πληθικότητα του στηρίγματος της ακολουθίας που αναπαριστάται, καθώς η πολλαπλότητα των διαφορών είναι φραγμένη από w^2. Υποθέτοντας ότι όλα τα πολυσύνολα μπορούν να έχουν πληθικότητα το πολύ $\mathcal{O}(w^2)$, απαιτείται $6 \cdot \mathcal{O}(w^2) = \mathcal{O}(w^2)$ μνήμη από τον αλγόριθμο για να παραθέσει τα στοιχεία στις λίστες που πρόκειται να ταξινομηθούν. Υποθέτουμε ότι αυτή η δέσμευση μνήμης επαρκεί και για την είσοδο στους αλγόριθμους ταξινόμησης. Για να ταξινομήσουμε λίστες μήκους w^2 δυο φορές εκτελούμε $2w^2 \log w^2 = 4w^2 \log w$ πράξεις. Τέλος πραγματοποιούμε το πολύ $2w^2$ συγκρίσεις και δίτιμες καταχωρήσεις μεταβλητών. Συνεπώς, ο συνολικός αριθμός των πράξεων που εκτελούνται από τον αλγόριθμο είναι $T_{\text{NPAFSUPVER}}(w) = \mathcal{O}(w^2) + 4w^2 \log w + 4w^2 = 4w^2 \log w + \mathcal{O}(w^2)$. Όπως και προηγουμένως, θα θέλαμε να αναφέρουμε ότι ο αλγόριθμος NPAFSupportVerification εξαρτάται μόνο από το βάρος w των υποψήφιων συμβατών ακολουθιών. □

Στη συνέχεια, δίνουμε τον Αλγόριθμο 14, ο οποίος είναι μια άμεση υλοποίηση του Πορίσματος 1 για την περίπτωση της επαλήθευσης

του PAF για $\alpha = 0$. Και σε αυτή τη περίπτωση, το πρόβλημα επαλήθευσης συμβατών ακολουθιών μετασχηματίζεται σε ένα συγκριτικό πρόβλημα ταξινόμησης και θα θεωρήσουμε τον αλγόριθμο ταξινόμησης που χρησιμοποιήσαμε πάλι ως "μαύρο κουτί", και ότι εκτελεί $n \log n$ πράξεις, τρέχει σε $\mathcal{O}(n \log n)$ χρόνο και τέλος ότι απαιτείται $\mathcal{O}(n)$ μνήμη για την ταξινόμηση n εγγραφών, για παράδειγμα ταξινόμηση λίστας μήκους n, στην χείριστη περίπτωση.

Algorithm 14 PAFSupportVerification Algorithm

```
procedure PafSupVer(D+_{A,2}, D-_{A,2}, C⇄_{A,2}, D+_{B,2}, D-_{B,2}, C⇄_{B,2}, α)
Require: D+_{A,2}, D-_{A,2}, C⇄_{A,2}, D+_{B,2}, D-_{B,2}, C⇄_{B,2} are arrays of length ≤ w^2
Require: α ∈ {0, 1, ..., 2n}
    maxlen ← max(|C⇄_{A,2}| + |C⇄_{B,2}|)
    lhs ← Sort([D+_{A,2}, D-_{A,2}, D+_{B,2}, D-_{B,2}])
    rhs ← Sort([C⇄_{A,2}, D⇄_{B,2}])
    for i ← 1 to maxlen do
        if lhs[i] − rhs[i] = α then
            bool ← true
        else
            bool ← false
                break
        end if
    end for
return (bool)
end procedure
```

Πρόταση 10 *Ο αλγόριθμος* PAFSupportVerification *εκτελεί* $T_{NPAFSUPVER}(w) = 4w^2 \log w + \mathcal{O}(w^2)$ *πράξεις και τρέχει σε* $\mathcal{O}(w^2 \log w)$ *χρόνο.*

Απόδειξη. Με παρόμοιο συλλογισμό, όπως στην περίπτωση του NPAF, ο συνολικός αριθμός των πράξεων που εκτελούνται από τον αλγόριθμο είναι $T_{PAFSUPVER}(w) = \mathcal{O}(w^2) + 4w^2 \log w + 4w^2 = 4w^2 \log w + \mathcal{O}(w^2)$. Επιπλέον, παρατήρουμε ότι προφανώς και ο αλγόριθμος PAFSupportVerification εξαρτάται μόνο από το βάρος w των υποψήφιων συμβατών ακολουθιών. □

Κλείνουμε αυτήν την ενότητα δίνοντας τον Αλγόριθμο 15, ο οποίος είναι μια άμεση υλοποίηση του Θεωρήματος 2 για την γενική περίπτωση της επαλήθευσης της AF για σταθερό α εκφρασμένο μέσω των Αλγορίθμων 13 και 14.

Algorithm 15 AFSupportVerification Algorithm

function AfSupVer($D^+_A, D^-_A, C_A, D^+_B, D^-_B, C_B, \alpha$, flag)
Require: $D^+_A, D^-_A, C_A, D^+_B, D^-_B, C_B$ are arrays of length $\leq w^2$
Require: $\alpha \in \{0, 1, \ldots, 2n\}$
  if flag = NPAF **then**
    $D^+_{A,1}, D^-_{A,1}, C^{\rightrightarrows}_{A,1}, D^+_{B,1}, D^-_{B,1}, C^{\rightrightarrows}_{B,1} \leftarrow D^+_A, D^-_A, C_A, D^+_B, D^-_B, C_B$
    bool $\leftarrow$ NPafSupVer($D^+_{A,1}, D^-_{A,1}, C^{\rightrightarrows}_{A,1}, D^+_{B,1}, D^-_{B,1}, C^{\rightrightarrows}_{B,1}, \alpha$)
  return (bool)
  else if flag = PAF **then**
    $D^+_{A,2}, D^-_{A,2}, C^{\rightleftarrows}_{A,2}, D^+_{B,2}, D^-_{B,2}, C^{\rightleftarrows}_{B,2} \leftarrow D^+_A, D^-_A, C_A, D^+_B, D^-_B, C_B$
    bool $\leftarrow$ PafSupVer($D^+_{A,2}, D^-_{A,2}, C^{\rightleftarrows}_{A,2}, D^+_{B,2}, D^-_{B,2}, C^{\rightleftarrows}_{B,2}, \alpha$)
  return (bool)
  end if
end function

Πόρισμα 5 *Ο αλγόριθμος* AFSupportVerification *τρέχει σε* $\mathcal{O}(w^2 \log w)$ *χρόνο.*

Απόδειξη. Σε αυτή την περίπτωση, ο χρόνος εκτέλεσης του αλγορίθμου AFSupportVerification είναι το μέγιστο των χρόνων εκτέλεσης των αλγορίθμων NPAFSupportVerification και PAFSupportVerification, δηλαδή εκφράζεται μέσω του $\max\{T_{\text{NPAFSUPVER}}(w), T_{\text{PAFSUPVER}}(w)\} = \max\{4w^2 \log w + \mathcal{O}(w^2), 4w^2 \log w + \mathcal{O}(w^2)\} \in \mathcal{O}(w^2 \log w)$.

□

§1.3.4 Μελέτη της Πολυπλοκότητας Χείριστης Περίπτωσης

Μια πρώτη εκτίμηση είναι ότι ο αλγόριθμος Support2Sequence εκτελεί λιγότερες πράξεις από τον (αντίστροφο) αλγόριθμο Sequence2Support, παρόλο που ο ασυμπτωτικός ρυθμός αύξησης των χρόνων εκτέλεσης τους είναι ίδιος καθώς $w < n$. Αυτή είναι και μια πρώτη ένδειξη ότι η κωδικοποίηση των ακολουθιών μέσω των στηριγμάτων τους είναι πιο αποδοτικός τρόπος για την επαλήθευση της συνάρτησης αυτοσυσχέτισης τους.

Μελέτη της Πολυπλοκότητας Χείριστης Περίπτωσης για Σταθερό NPAF Παραθέτουμε τις τρείς φάσεις που χρειάστηκαν για τον υπολογισμό του NPAF δυο ακολουθιών από αλγοριθμική σκοπιά:

- Αλγόριθμοι Sequence2Support και Support2Sequence
- Αλγόριθμοι NPAFVector και NPAFSupport
- Αλγόριθμοι NPAFVectorVerification και NPAFSupportVerification

Στη συνέχεια συγκρίνουμε την απόδοση των προηγούμενων αλγορίθμων για τις δύο περιπτώσεις, του προβλήματος ακολουθιών και στηρίγματος. Αρχικά, μελετάμε το πρόβλημα ακολουθιών, δηλαδή όταν έχουμε ως είσοδο υποψήφιες ακολουθίες. Σε αυτήν την περίπτωση, δεν χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή ακολουθιών.

Φάση	Αλγόριθμος	Πράξεις / Μνήμη	Χρόνος
Υπολογισμού	NPAFVector	$4n^2 + \mathcal{O}(n)$ / $\mathcal{O}(n)$	$\mathcal{O}(n^2)$
Επαλήθευσης	NPAFVectorVerification	$2n + \mathcal{O}(1)$ / $\mathcal{O}(n)$	$\mathcal{O}(n)$
Συνολικό Κόστος	-	$4n^2 + \mathcal{O}(n)$ / $\mathcal{O}(n)$	$\mathcal{O}(n^2)$

Συνεχίζουμε με το πρόβλημα στηρίγματος, όταν δηλαδή δίνονται τα στηρίγματα των υποψήφιων ακολουθιών. Όπως και προηγουμένως, δεν χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή στηριγμάτων.

Φάση	Αλγόριθμος	Πράξεις / Μνήμη	Χρόνος
Υπολογισμού	NPAFSupport	$9w^2 + \mathcal{O}(w)$ / $\mathcal{O}(w)$	$\mathcal{O}(w^2)$
Επαλήθευσης	NPAFSupportVerification	$4w^2 \log w + \mathcal{O}(w^2)$ / $\mathcal{O}(w^2)$	$\mathcal{O}(w^2 \log w)$
Συνολικό Κόστος	-	$4w^2 \log w + \mathcal{O}(w^2)$ / $\mathcal{O}(w^2)$	$\mathcal{O}(w^2 \log w)$

Συμπεραίνουμε ότι, για την πρώτη περίπτωση η πολυπλοκότητα, $T_{SEQ}(n)$, ειναι τετραγωνική ως πρός το μήκος n, ενώ στη δεύτερη περίπτωση η πολυπλοκότητα, $T_{SUP}(w)$, είναι λογαριθμικά τετραγωνική ως πρός το βάρος w. Συγκρίνουμε τη νέα μέθοδο κωδικοποίησης της μη-περιοδικής συνάρτησης αυτοσυσχέτισης με τη κλασική περιγραφή της, για το ίδιο στιγμιότυπο εισόδου χρησιμοποιώντας τους αλγορίθμους αναπαράστασης και δίνουμε τις χρονικές πολυπλοκότητες εκφρασμένες σε n και w για μια πιο λεπτομερής ασυμπτοτική ανάλυση [87].

1. Για το πρόβλημα ακολουθιών έχουμε $\mathsf{T}_{\mathsf{SEQ}}(n) = 4n^2 + \mathcal{O}(n)$ και $2 \cdot \mathsf{T}_{\mathsf{SEQ2SUP}}(n) + \mathsf{T}_{\mathsf{SUP}}(w) = 8n + 4w^2 \log w + \mathcal{O}(w^2)$. Συνεπώς, η νέα κωδικοποίηση του NPAF εκτελεί $\mathsf{T}(n, w) = 8n + 4w^2 \log w + \mathcal{O}(w^2)$ πράξεις και τρέχει σε $\mathcal{O}(n + w^2 \log w)$ χρόνο.

2. Για το πρόβλημα του στηρίγματος έχουμε $2 \cdot \mathsf{T}_{\mathsf{SUP2SEQ}}(w) + \mathsf{T}_{\mathsf{SEQ}}(n) = 6w + 4n^2 + \mathcal{O}(n)$ και $\mathsf{T}_{\mathsf{SUP}}(w) = 4w^2 \log w + \mathcal{O}(w^2)$. Καθώς το w μπορεί να είναι το πολύ $2n$ έχουμε ότι ο χρόνος εκτέλεσης $\mathsf{T}_{\mathsf{SUP2SEQ}}(w) + \mathsf{T}_{\mathsf{SEQ}}(n)$ είναι της τάξης $\mathcal{O}(n^2)$.

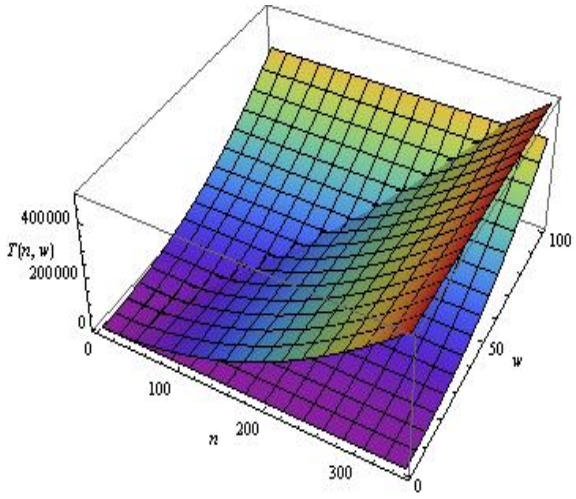
Όμως, σε πραγματικές εφαρμογές, η ασυμπτωτική ανάλυση παρέχει μια προσέγγιση του πόσο γρήγορα εκτελείται ένας αλγόριθμος. Πρακτικά είναι πιο χρήσιμο να γνωρίζουμε περισσότερα από τους μεγιστοβάθμιους όρους στις συναρτήσεις των χρόνων εκτέλεσης [87]. Συνεπώς, ξαναυπολογίζουμε το συνολικό αριθμό των πράξεων που εκτελούνται από τους Αλγορίθμους 4, 10 και τους Αλγορίθμους 2, 7, 13 χωρίς να λάβουμε υπόψιν $\mathcal{O}(1)$ πράξεις, καθώς αυτό είναι αποτέλεσμα της υλοποίησης σε μια υπολογιστική μηχανή και διαφέρει από περίπτωση σε περίπτωση.

Τελικά, έχουμε $\mathsf{T}_{\mathsf{SEQ}}(n) = 2 \cdot \mathsf{T}_{\mathsf{NPAFVEC}}(n) + \mathsf{T}_{\mathsf{NPAFVECVER}}(n) = 4n^2 + 2n$ πράξεις σε σύγκριση με $\mathsf{T}_{\mathsf{SUP}}(n, w) = 2 \cdot \mathsf{T}_{\mathsf{SEQ2SUP}}(n) + 2 \cdot \mathsf{T}_{\mathsf{NPAFSUP}}(w) + \mathsf{T}_{\mathsf{NPAFSUPVER}}(w) = 8n + 9w^2 - 3w + 4w^2 + 4w^2 \log w = 8n + 13w^2 - 3w + 4w^2 \log w$. Κατά συνέπεια, η νέα κωδικοποίηση του NPAF είναι αποδοτικότερη όταν,

$$\mathsf{T}_{\mathsf{SEQ}}(n) > \mathsf{T}_{\mathsf{SUP}}(n, w) \Leftrightarrow 4n^2 - 6n + w(4w \log w + 13w - 3) > 0 \quad (1.5)$$

Είναι προφανές ότι για σταθερό μικρό w καθώς το μήκος n αυξάνει, η κωδικοποίση του NPAF είναι αποδοτικότερη. Ιδιαίτερα, όταν $w \lesssim n/3$ η υλοποίηση αυτής της κωδικοποίησης είναι αποδοτικότερη, δηλαδή όταν η πληθικότητα των μηδενικών που εμφανίζονται στις δυο $\{0, \pm 1\}$ είναι τα $2/3$ του μήκους των ακολουθιών. Σημειώνουμε ότι, αυτό το αποτέλεσμα είναι σε συμφωνία με τη Θεωρία των TCP [36] (δηλαδή συμβατές ακολουθίες με NPAF ίσο με 0) που όταν ένα βάρος έχει καθοριστεί με κάποιο τρόπο για κάποιο μήκος, αυτό το μήκος μπορεί να αυξάνεται αυθαίρετα. Συνεπώς, το βάρος είναι θεμελιώδες και το μήκος αυθαίρετα μεγάλο.

Στο ακόλουθο γράφημα σχεδιάζουμε τις συναρτήσεις πολυπλοκότητας $\mathsf{T}_{\mathsf{SEQ}}(n)$ και $\mathsf{T}_{\mathsf{SUP}}(n, w)$. Το γράφημα, δικαιώνει τα προηγούμενα αποτελέσματα και προτείνουμε τη νέα κωδικοποίσης του NPAF για τριαδικές ακολουθίες όταν $w \lesssim n/3$.



Σχήμα 1.1: Σύγκριση των πολυπλοκοτήτων $T_{SEQ}(n)$ και $T_{SUP}(n, w)$ για την περίπτωση του NPAF

Μελέτη της Πολυπλοκότητας Χείριστης Περίπτωσης για Σταθερό PAF Παραθέτουμε τις τρείς φάσεις που χρειάστηκαν για τον υπολογισμό του PAF δυο ακολουθιών από αλγοριθμική σκοπιά:

- Αλγόριθμοι Sequence2Support και Support2Sequence
- Αλγόριθμοι PAFVector και PAFSupport
- Αλγόριθμοι PAFVectorVerification και PAFSupportVerification

Στη συνέχεια συγκρίνουμε την απόδοση των προηγούμενων αλγορίθμων για τις δυο περιπτώσεις, του προβλήματος ακολουθιών και στηρίγματος. Αρχικά, μελετάμε το πρόβλημα ακολουθιών, δηλαδή όταν έχουμε ως είσοδο υποψήφιες ακολουθίες. Σε αυτήν την περίπτωση, δε χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή ακολουθιών.

Φάση	Αλγόριθμος	Πράξεις / Μνήμη	Χρόνος
Υπολογισμού	PAFVector	$14n^2 + \mathcal{O}(n)$ / $\mathcal{O}(n)$	$\mathcal{O}(n^2)$
Επαλήθευσης	PAFVectorVerification	$2n + \mathcal{O}(1)$ / $\mathcal{O}(n)$	$\mathcal{O}(n)$
Συνολικό Κόστος	-	$14n^2 + \mathcal{O}(n)$ / $\mathcal{O}(n)$	$\mathcal{O}(n^2)$

Συνεχίζουμε με το πρόβλημα στηρίγματος, όταν δηλαδή δίνονται τα στηρίγματα των υποψήφιων ακολουθιών. Όπως και προηγουμένως,

δε χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή στηριγμάτων.

Φάση	Αλγόριθμος	Πράξεις / Μνήμη	Χρόνος
Υπολογισμού	PAFSupport	$28w^2 + \mathcal{O}(w)$ / $\mathcal{O}(w)$	$\mathcal{O}(w^2)$
Επαλήθευσης	PAFSupportVerification	$4w^2 \log w + \mathcal{O}(w^2)$ / $\mathcal{O}(w^2)$	$\mathcal{O}(w^2 \log w)$
Συνολικό Κόστος	-	$4w^2 \log w + \mathcal{O}(w^2)$ / $\mathcal{O}(w^2)$	$\mathcal{O}(w^2 \log w)$

Συμπεραίνουμε ότι, για την πρώτη περίπτωση η πολυπλοκότητα, $T_{SEQ}(n)$, ειναι τετραγωνική ως πρός το μήκος n, ενώ στη δεύτερη περίπτωση η πολυπλοκότητα, $T_{SUP}(w)$, είναι λογαριθμικά τετραγωνική ως πρός το βάρος w. Συγκρίνουμε τη νέα μέθοδο κωδικοποίησης της περιοδικής συνάρτησης αυτοσυσχέτισης με τη κλασική περιγραφή της, για το ίδιο στιγμιότυπο εισόδου χρησιμοποιώντας τους αλγορίθμους αναπαράστασης και δίνουμε τις χρονικές πολυπλοκότητες εκφρασμένες σε n και w για μια πιο λεπτομερής ασυμπτοτική ανάλυση [87].

1. Για το πρόβλημα ακολουθιών έχουμε $T_{SEQ}(n) = 14n^2 + \mathcal{O}(n)$ και $2 \cdot T_{SEQ2SUP}(n) + T_{SUP}(w) = 8n + 4w^2 \log w + \mathcal{O}(w^2)$. Συνεπώς, η νέα κωδικοποίηση του NPAF εκτελεί $T(n, w) = 8n + 4w^2 \log w + \mathcal{O}(w^2)$ πράξεις και τρέχει σε $\mathcal{O}(n + w^2 \log w)$ χρόνο.

2. Για το πρόβλημα του στηρίγματος έχουμε $2 \cdot T_{SUP2SEQ}(w) + T_{SEQ}(n) = 6w + 14n^2 + \mathcal{O}(n)$ και $T_{SUP}(w) = 4w^2 \log w + \mathcal{O}(w^2)$. Καθώς το w μπορεί να είναι το πολύ $2n$ έχουμε ότι ο χρόνος εκτέλεσης $T_{SUP2SEQ}(w) + T_{SEQ}(n)$ είναι της τάξης $\mathcal{O}(n^2)$.

Όμως, σε πραγματικές εφαρμογές, η ασυμπτωτική ανάλυση παρέχει μια προσέγγιση του πόσο γρήγορα εκτελείται ένας αλγόριθμος. Πρακτικά είναι πιο χρήσιμο να γνωρίζουμε περισσότερα από τους μεγιστοβάθμιους όρους στις συναρτήσεις των χρόνων εκτέλεσης [87]. Συνεπώς, ξαναυπολογίζουμε το συνολικό αριθμό των πράξεων που εκτελούνται από τους Αλγορίθμους 5, 11 και τους Αλγορίθμους 2, 8, 14 χωρίς να λάβουμε υπόψιν $\mathcal{O}(1)$ πράξεις, καθώς αυτό είναι αποτέλεσμα της υλοποίησης σε μια υπολογιστική μηχανή και διαφέρει από περίπτωση σε περίπτωση.

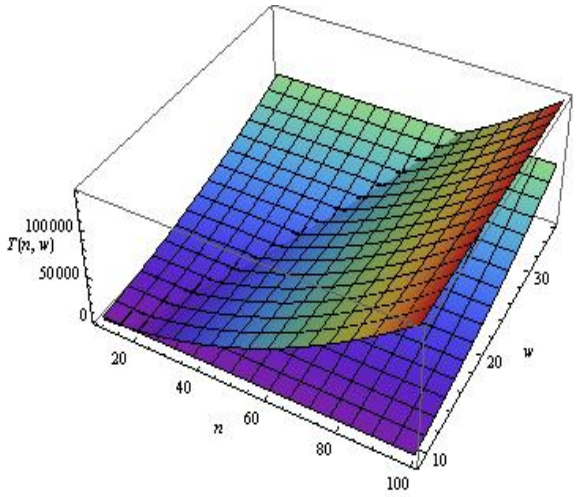
Τελικά, έχουμε $T_{SEQ}(n) = 2 \cdot T_{PAFVEC}(n) + T_{PAFVECVER}(n) = 14n^2 - 10n + 2n = 14n^2 - 8n$ πράξεις σε σύγκριση με $T_{SUP}(n, w) = 2 \cdot T_{SEQ2SUP}(n) + 2 \cdot T_{PAFSUP}(w) + T_{NAFSUPVER}(w) = 8n + 28w^2 + 4w^2 + 4w^2 \log w = 8n +$

$32w^2 + 4w^2 \log w$. Κατά συνέπεια, η νέα κωδικοποίηση του PAF είναι αποδοτικότερη όταν,

$$T_{SEQ}(n) > T_{SUP}(n, w) \Leftrightarrow 14n^2 - 16n - 4w^2(\log w + 8) > 0 \qquad (1.6)$$

Είναι προφανές ότι για σταθερό μικρό w καθώς το μήκος n αυξάνει, η κωδικοποίση του PAF είναι αποδοτικότερη. Ιδιαίτερα, όταν $w \lesssim n/2$ η υλοποίηση αυτής της κωδικοποίησης είναι αποδοτικότερη, δηλαδή όταν η πληθικότητα των μηδενικών που εμφανίζονται στις δυο $\{0, \pm 1\}$ είναι το $1/2$ του μήκους των ακολουθιών.

Στο ακόλουθο γράφημα σχεδιάζουμε τις συναρτήσεις πολυπλοκότητας $T_{SEQ}(n)$ και $T_{SUP}(n, w)$. Το γράφημα, δικαιώνει τα προηγούμενα αποτελέσματα και προτείνουμε τη νέα κωδικοποίσης του PAF για τριαδικές ακολουθίες όταν $w \lesssim n/2$.



Σχήμα 1.2: Σύγκριση των πολυπλοκοτήτων $T_{SEQ}(n)$ και $T_{SUP}(n, w)$ για την περίπτωση του PAF

Μελέτη της Πολυπλοκότητας Χείριστης Περίπτωσης για Σταθερή AF Παραθέτουμε τις τρείς φάσεις που χρειάστηκαν για τον υπολογισμό της AF δυο ακολουθιών από αλγοριθμική σκοπιά:

- Αλγόριθμοι Sequence2Support και Support2Sequence
- Αλγόριθμοι AFVector και AFSupport
- Αλγόριθμοι AFVectorVerification και AFSupportVerification

Στη συνέχεια συγκρίνουμε την απόδοση των προηγούμενων αλγορίθμων για τις δυο περιπτώσεις, του προβλήματος ακολουθιών και στηρίγματος. Αρχικά, μελετάμε το πρόβλημα ακολουθιών, δηλαδή όταν έχουμε ως είσοδο υποψήφιες ακολουθίες. Σε αυτήν την περίπτωση, δε χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή ακολουθιών.

Φάση	Αλγόριθμος	Χρόνος
Υπολογισμού	AFVector	$\mathcal{O}(n^2)$
Επαλήθευσης	AFVectorVerification	$\mathcal{O}(n)$
Συνολικό Κόστος	-	$\mathcal{O}(n^2)$

Συνεχίζουμε με το πρόβλημα στηρίγματος, όταν δηλαδή δίνονται τα στηρίγματα των υποψήφιων ακολουθιών. Όπως και προηγουμένως, δε χρειάζεται να μετασχηματίσουμε την είσοδο καθώς αυτή είναι ήδη εκφρασμένη με τη μορφή στηριγμάτων.

Φάση	Αλγόριθμος	Χρόνος
Υπολογισμού	AFSupport	$\mathcal{O}(w^2)$
Επαλήθευσης	AFSupportVerification	$\mathcal{O}(w^2 \log w)$
Συνολικό Κόστος	-	$\mathcal{O}(w^2 \log w)$

Συμπεραίνουμε ότι, για την πρώτη περίπτωση η πολυπλοκότητα, $\mathsf{T}_{\mathsf{SEQ}}(n)$, ειναι τετραγωνική ως πρός το μήκος n, ενώ στη δεύτερη περίπτωση η πολυπλοκότητα, $\mathsf{T}_{\mathsf{SUP}}(w)$, είναι λογαριθμικά τετραγωνική ως πρός το βάρος w. Συγκρίνουμε τη νέα μέθοδο κωδικοποίησης της συνάρτησης αυτοσυσχέτισης με τη κλασική περιγραφή της, για το ίδιο στιγμιότυπο εισόδου χρησιμοποιώντας τους αλγορίθμους αναπαράστασης και δίνουμε τις χρονικές πολυπλοκότητες εκφρασμένες σε n και w για μια πιο λεπτομερής ασυμπτοτική ανάλυση [87].

Θεώρημα 3 *Αν $n > w^2 \log w$ ο αλγόριθμος για το πρόβλημα του στηρίγματος τρέχει σε $\mathcal{O}(n)$ χρόνο, και κατά συνέπεια είναι βέλτιστος, υπό την έννοια ότι δεν αναμένουμε ασυμπτωτικά καλύτερους άλγοριθμους.*

Απόδειξη. Για το πρόβλημα του στηρίγματος έχουμε $\mathsf{T}_{\mathsf{SEQ}}(n) = \mathcal{O}(n^2)$ και το κόστος μετατροπής υποψηφίων συμβατών ακολουθιών στα στηρίγματα τους είναι $\mathsf{T}_{\mathsf{SEQ2SUP}}(n) = \mathcal{O}(n)$. Συνεπώς, το συνολικό κόστος είναι $2 \cdot \mathsf{T}_{\mathsf{SEQ2SUP}}(n) + \mathsf{T}_{\mathsf{SUP}}(w) = \mathcal{O}(n + w^2 \log w)$ και κατά συνέπεια n

νέα κωδικοποίηση για την AF τρέχει σε $\mathcal{O}(n + w^2 \log w)$. Αν επιπλέον ισχύει ότι $n > w^2 \log w$ αυτή n τάξη μεγέθους μειώνεται σε $\mathcal{O}(n)$. Καθώς για ένα πρόβλημα μεγέθους n πάντα χρειαζόμαστε $\mathcal{O}(n)$ πράξεις για να διαβάσουμε την είσοδο, αυτή n τελική πολυπλοκότητα είναι βέλτιστη υπό την έννοια ότι δεν αναμένουμε ασυμπτωτικά καλύτερους άλγοριθμους για την κωδικοποίηση της AF. □

Πόρισμα 6 *Για το πρόβλημα του στηρίγματος και υποψήφιες συμβατές ακολουθίες οι ακόλουθες περιπτώσεις είναι αποδοτικές για τη κωδικοποίηση της AF (όταν συγκρίνονται με το χρόνο του προβλήματος ακολουθιών* $T_{SEQ}(n) = \mathcal{O}(n^2)$*):*

1. *Αν* $n > w^2$*, τότε η κωδικοποίηση της AF μπορεί να υλοποιηθεί σε* $\mathcal{O}(n \log w)$ *χρόνο.*
2. *Αν* $n > w \log w$*, τότε η κωδικοποίηση της AF μπορεί να υλοποιηθεί σε* $\mathcal{O}(nw)$ *χρόνο.*

Απόδειξη. Άμεση από την απόδειξη του Θεωρήματος 3.

□

§1.4 Πίνακες Στάθμισης Μικρού Βάρους

Κατασκευάσαμε χιλιάδες $DC(n, w)$ ζεύγη ακολουθιών για να παράγουμε $W(2n, w)$ πίνακες στάθμισης, για βάρη $w = 9, 18, 36$ και μήκη n στο διάστημα 10 εώς 50000 σε αρκετά μικρό υπολογιστικό χρόνο, για τα επιτρεπτά μήκη n. Τα $DC(n, w)$ ζεύγη ακολουθιών που αναπαριστώνται μέσω των ακολουθιών μπορούν να βρεθούν στην ιστοσελίδα `www.math.ntua.gr/~ckoukouv`. Ιδιαίτερα, έχουμε τις ακόλουθες περιπτώσεις:

(i) Αν $w = 9$, τότε για $n \gtrsim 18$ και από την σχέση (1.6), $T_{SUP}(n, 9) < T_{SEQ}(n)$ και κατασκευάσαμε 25344 $DC(n, 9) \to W(2n, 9)$ για $10 \leq n \leq 50000$.

(ii) Αν $w = 18$, τότε για $n \gtrsim 36$ και από την σχέση (1.6), $T_{SUP}(n, 18) < T_{SEQ}(n)$ και κατασκευάσαμε 33500 $DC(n, 18) \to W(2n, 18)$ για $11 \leq n \leq 49500$.

(iii) Αν $w = 36$, τότε για $n \gtrsim 72$ και από την σχέση (1.6), $T_{SUP}(n, 36) < T_{SEQ}(n)$ και κατασκευάσαμε 29500 $DC(n, 36) \rightarrow W(2n, 36)$ για $19 \leq n \leq 49500$.

First, solve the problem. Then, write the code.

John Jonhson (1977)

2 Πίνακες Hadamard

Στο δεύτερο αυτό κεφάλαιο, κατασκευάζουμε νέους μη-ισοδύναμους πίνακες Hadamard βασιζόμενοι στις πολλαπλασιαστικές μεθόδους του Yang για βασικές ακολουθίες που προκύπτουν από σχεδόν-κανονικές ακολουθίες. Αυτό επετεύχθη κάνοντας χρήση διαφόρων εργαλείων του Unix *και προχωρημένων υπολογιστικών τεχνικών, όπως είναι το meta-programming. Επιπλέον, παρουσιάζεται μια πλήρης ταξινόμηση σχεδόν-κανονικών ακολουθιών, για πρώτη φορά, για μήκη* $4n+1$*, όπου* $n \leq 11$ *και ορισμένες από αυτές για* $n = 12, 13, 14$ *και* 15*, λαμβάνοντας υπόψιν και προηγουμένως γνωστά αποτελέσματα.*

Στη συνέχεια, κατασκευάζουμε νέους μη-ισοδύναμους πίνακες Hadamard οι οποίοι παράγονται από αρκετούς νέους αλλά και γνωστούς πλήρεις ορθογώνιους σχεδιασμούς, χρησιμοποιώντας κυκλικούς και συμμετρικούς block πίνακες. Οι ορθογώνιοι σχεδιασμοί προκύπτουν από ορισμένες νέες θεωρητικές και αλγοριθμικές κατασκευές για ακολουθίες με μηδενική αυτοσυσχέτιση. Για την εύρεση των μη-ισοδύναμων πινάκων Hadamard από ορθογώνιους σχεδιασμούς αναπτύχθηκε κατάλληλο λογισμικό, το οποίο διέπεται από διάφορες αυτοματοποιήσεις κάνοντας χρήση των υπολογιστικών πακέτων Magma, Maple *και της γλώσσας προγραμματισμού* C*. Εν κατακλείδι, βελτιώνουμε αρκετά κατασκευαστικά φράγματα για μη-ισοδύναμους πίνακες Hadamard μεγάλων τάξεων.*

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στις επιστημονικές εργασίες [142] και [156].

§2.1 Βασικοί Ορισμοί και Ιδιότητες

Ένας *πίνακας Hadamard* τάξης n, που θα συμβολίζεται με $H(n)$ ή H_n, είναι ένας $n \times n$ πίνακας με στοιχεία $\{1, -1\}$, που έχει την ακόλουθη ιδιότητα,

$$HH^T = nI_n$$

όπου με H^T συμβολίζουμε τον ανάστροφο πίνακα του H και με I_n τον ταυτοτικό πίνακα τάξης n. Η ιδιότητα αυτή συνεπάγεται ότι οι γραμμές (και οι στήλες) ενός πίνακα Hadamard είναι ορθογώνιες. Είναι γνωστό ότι αν n είναι n τάξη ενός πίνακα Hadamard τότε το n είναι απαραίτητα $1, 2$ ή ένα πολλαπλάσιο του 4, βλ. [208]. Ένας πίνακας Hadamard θα καλείται *ημικανονικοποιημένος* αν όλα τα στοιχεία της πρώτης του γραμμής είναι ίσα με 1, ενώ θα καλείται αντίστοιχα *κανονικοποιημένος* αν όλα τα στοιχεία της πρώτης του γραμμής αλλά και στήλης είναι ίσα με 1. Δυο πίνακες Hadamard θα καλούνται *ισοδύναμοι* αν ο ένας μπορεί να μετασχηματιστεί στον άλλον εφραμόζοντας διαδοχικά μεταθέσεις γραμμών ή στηλών και πολλαπλασιασμούς με -1. Η εικασία του Hadamard δηλώνει ότι υπάρχει ένας πίνακας Hadamard τάξης $4m$, για κάθε θετικό ακέραιο m. Η εικασία του Hadamard είναι ένα από τα βασικά άλυτα προβλήματα στα Διακριτά Μαθηματικά [113]. Η μικρότερη τάξη n για την οποία ένας πίνακας Hadamard δεν είναι γνωστός, είναι $n = 668$.

Οι πίνακες Hadamard έχουν σημαντικές εφαρμογές στην Στατιστική, στη Θεωρία κωδίκων και τη Κρυπτογραφία, σε συστήματα τηλεπικοινωνιών και σε πολλές άλλες περιοχές όπως θα δούμε σε επόμενη ενότητα. Το πακέτο υπολογιστικής άλγεβρας, Magma, διατηρεί μια βάση δεδομένων για μη-ισοδύναμους πίνακες Hadamard μικρών τάξεων [15], ενώ κάτω φράγματα στον αριθμό των μη-ισοδύναμων πινάκων Hadamard μπορούν να βρεθούν στην [144]. Για περισσότερες πληροφορίες στους πίνακες Hadamard και των εφαρμογών τους παραπέμπουμε στις [70, 113, 208, 231].

Ερευνητικό Πρόβλημα 2 *Η κατασκευή νέων μη-ισοδύναμων πινάκων Hadamard που παράγονται απο ακολουθίες με μηδενική συνάρτηση αυτοσυσχέτισης και ορθογώνιους σχεδιασμούς, καθώς και η ανάπτυξη κατάλληλου λογισμικού για την εύρεση αυτών.*

§2.1.1 Εφαρμογές των Πινάκων Hadamard

Σε αυτήν την ενότητα δίνουμε μερικές αναφορές σε εργασίες που περιγράφουν τις εφαρμογές των πινάκων Hadamard. Δεν αποσκοπούμε στο να παρέχουμε μια ολοκληρωμένη, ή με κάθε τρόπο πλήρη, αντιμετώπιση του θέματος, καθώς αυτό δεν είναι ο σκοπός της παρούσας διατριβής. Απλά ενδιαφερόμαστε να δώσουμε μια εικόνα των πολλών εφαρμογών που συναντά κάποιος στους πίνακες Hadamard, προκειμένου να εκθέσουμε οτι παρόλο που οι πίνακες Hadamard είναι ειδική περίπτωση των ορθογώνιων σχεδιασμών (όπως θα δούμε σε επόμενη ενότητα), οι εφαρμογές τους είναι ευρύτερου ενδιαφέροντος.

Όπως πρώτα παρατηρήθηκε στην [192], οι πίνακες Hadamard χρησιμοποιούνται στην Στατιστική όπου παράγουν βέλτιστους στατιστικούς σχεδιασμούς για χρήση σε πειράματα στάθμισης. Οι πίνακες Hadamard διαδραματίζουν σημαντικό ρόλο στη Θεωρία κωδίκων όπου παράγουν τους λεγόμενους κώδικες Hadamard ([176]), οι οποίοι είναι κώδικες διόρθωσης σφαλμάτων που διορθώνουν το μέγιστο αριθμό λαθών στη μετάδοση ενός μηνύματος. Αξίζει να αναφερθεί ότι, ένας κώδικας Hadamard χρησιμοποιήθηκε κατά την διαστημική αποστολή Mariner 9 από τη NASA το 1971 για να διορθώσει το λάθος κατα την μετάδοση εικόνων. Η αποστολή Mariner 9 και η σχέση της με τη Θεωρία κωδίκων είναι το κύριο θέμα των [197] και [172].

Οι πίνακες Hadamard χρησιμοποιούνται στις τηλεπικοινωνίες όπου παράγουν ακολουθίες που βρίσκουν εφαρμογή σε ψηφιακά συστήματα και στην Οπτική για τη βελτίωση της ποιότητας και ανάλυσης των σαρωτών εικόνας (image scanners). Περισσότερες πληροφορίες, σχετικά με τις εφαρμογές τους στις τηλεπικοινωνίες και στην επεξεργασία σήματος μπορούν να βρεθούν στην [241]. Επιπλέον, οι πίνακες Hadamard πάιζουν σημαντικό ρόλο στην Αριθμητική Ανάλυση και συγκεκριμένα στην μελέτη του συντελεστή μεγέθυνσης (growth factor) της μεθόδου απαλοιφής του Gauss με πλήρη οδήγηση ([41]). Οι πίνακες Hadamard, είναι οι μόνοι γνωστοί πίνακες εώς σήμερα που πετυχαίνουν ένα συντελεστή μεγέθυνσης ίσο με τη διάσταση τους.

§2.2 Πίνακες Hadamard από Σχεδόν-Κανονίκες Ακολουθίες

Σε αυτήν την ενότητα, παρουσίαζουμε την ταξινόμηση των σχεδόν-κανονικών ακολουθιών που χρησιμοποιήσαμε για την εύρεση των μη-ισοδύναμων πινάκων Hadamard μέσω των πολλαπλασιαστικών μεθόδων του Yang.

§2.2.1 Ταξινόμηση Σχεδόν-Κανονικών Ακολουθιών

Για τις ανάγκες αυτής της ενότητας θα χρειαστούμε τις έννοιες της περιοδικής (PAF) και μη-περιοδικής (NPAF) συνάρτησης αυτοσυσχέτισης που δίνονται στο πρώτο κεφάλαιο της διατριβής και στην [143]. Η αντίστροφη ακολουθία A^* της $A = [a_1, \ldots, a_n]$ ορίζεται ως $[a_n, \ldots, a_1]$. Για δοθείσες ακολουθίες $A = [a_1, a_2, \ldots, a_{m+1}]$ και $C = [c_1, c_2, \ldots, c_m]$, η παρεμβάλλουσα ακολουθία (interleaved sequence) A/C των A και C ορίζεται ως $A/C = [a_1, c_1, a_2, c_2, \ldots, a_m, c_m, a_{m+1}]$.

Ορισμός 8 *Μια τετράδα* $(E, F; G, H)$ *από* $(0, \pm 1)$ *ακολουθίες είναι ένα σύνολο από σχεδόν κανονικές ακολουθίες (near-normal sequences) μήκους* $n = 4m + 1$ *(και θα συμβολίζονται με* $\mathrm{NNS}(n)$*) αν ικανοποιούνται οι ακόλουθες συνθήκες.*

1. $E = [1, X/O_{m-1}]$, $F = [Y/O_{m-1}]$ *όπου* X *και* Y *είναι* $(1, -1)$ *ακολουθίες μήκους* m *και* O_{m-1} *είναι η ακολουθία μηδενικών μήκους* $m - 1$*, δηλαδή, οι* E *και* F *είναι αντίστοιχα μήκους* $2m$ *και* $2m - 1$*, ενώ οι* G *και* H *είναι* $(0, \pm 1)$ *ακολουθίες μήκους* $2m$*, τέτοιες ώστε η* $G + H$ *να είναι μια* $(1, -1)$ *ακολουθία μήκους* $2m$*.*

2. $N_E(s) + N_F(s) + N_G(s) + N_H(s) = 0$, $s = 1, \ldots, 2m - 1$*.*

Παρατήρηση 3 *Οι ακολουθίες* G *και* H *του προηγούμενου ορισμού είναι πολυσυμμετρικές (quasi-symmetric), δηλαδή, αν* $g_k = 0$*, τότε* $g_{2m+1-k} = 0$ *και επίσης αν* $h_k = 0$*, τότε* $h_{2m+1-k} = 0$*.*

Ορισμός 9 *Δυο σύνολα από σχεδόν-κανονικές ακολουθίες* $\mathrm{NNS}(n)$, $(E, F; G, H)$ *και* $(E', F'; G', H')$, *θα καλούνται ισοδύναμα αν το ένα μπορεί να μετασχηματιστεί στο άλλο εφαρμόζοντας τους ακόλουθους ισομορφικούς μετασχηματισμούς:*

(i) $E' = E$ *ή* $-E$, $S' = S, S^*$ *ή* $-S$ *για* $S = F, G$ *και* H.

(ii) $S' = S$ *για* $S = E$ *και* F, $G' = G_s + H_k$ *και* $H' = H_s + G_k$, *όπου* G_s, H_s *και* G_k, H_k *είναι τα συμμετρικά και skew μέρη των* G *και* H *αντίστοιχα.*

(iii) $S' = S^e$ *για* $S = E, F, G$ *και* H, *όπου με* S^e *δηλώνουμε ότι η* S^e *προκύπτει από την* S *με αλλάγή των προσήμων των άρτιων θέσεων της ακολουθίας.*

(iv) Οι E', F', G' *και* H' *προκύπτουν από οποιοδήποτε συνδυασμό των μετασχηματισμών (i), (ii) και (iii).*

Ορισμένα μήκη από σχεδόν-κανονικές ακολουθίες δίονται στις [147] και [240]. Στη συνέχεια, παρουσιάζουμε μια πλήρη ταξινόμηση για σχεδόν-κανονικές ακολουθίες $\mathrm{NNS}(n)$, $n = 4m + 1$. Ο πίνακας 2.2.1, απαριθμεί τον αριθμό $I(n)$ των μη-ισοδύναμων $\mathrm{NNS}(n)$ για $1 \leq m \leq 11$, δηλαδή $5 \leq n \leq 45$.

m	1	2	3	4	5	6	7	8	9	10	11
n	5	9	13	17	21	25	29	33	37	41	45
$I(n)$	1	2	2	3	8	14	11	23	20	18	31

Πίνακας 2.1: Μη-ισοδύναμες $\mathrm{NNS}(n)$ για $5 \leq n \leq 45$

Δίνουμε επίσης σύνολα από σχεδόν-κανονικές ακολουθίες $\mathrm{NNS}(n)$, $n = 4m + 1$ για $m = 12, 13, 14$ και 15, δηλαδή $n = 49, 53, 57$ και 61.

m	12	13	14	15
n	49	53	57	61
$S(n)$	12	2	3	1

Πίνακας 2.2: Σύνολα από $\mathrm{NNS}(n)$ για $49 \leq n \leq 61$.

Οι μη-ισοδύναμες NNS(n) για $5 \leq n \leq 45$ μπορούν να βρεθούν στην ιστοσελίδα, `http://www.math.ntua.gr/~ckoukouv/nnseq.htm`.

Μήκος n	Άθροισμα Τετραγώνων $a^2+b^2+c^2+d^2$	Σχεδόν-Κανονικές Ακολουθίες
5	$2^2+1^2+0^2+0^2$	$E=[++]$ $F=[+]$ $G=[+-]$ $H=[00]$
9	$3^2+0^2+0^2+0^2$	$E=[++0+]$ $F=[+0-]$ $G=[+00-]$ $H=[0-+0]$
9	$1^2+2^2+2^2+0^2$	$E=[++0-]$ $F=[+0+]$ $G=[+00+]$ $H=[0-+0]$
13	$2^2+3^2+0^2+0^2$	$E=[+-0+0+]$ $F=[+0+0+]$ $G=[+0000-]$ $H=[0++--0]$
13	$2^2+3^2+0^2+0^2$	$E=[++0-0+]$ $F=[+0+0+]$ $G=[++-+--]$ $H=[000000]$

Πίνακας 2.3: Σχεδόν-κανονικές ακολουθίες NNS(n) για $5 \leq n \leq 13$

§2.2.2 Πολλαπλασιαστικές μέθοδοι του Yang

Μια αρκετά παραγωγική μέθοδος για την κατασκευή πινάκων Hadamard χρησιμοποίει T-πίνακες ή T-ακολουθίες. Αυτή η μέθοδος βασίζεται σε βασικές ακολουθίες και αριθμούς Yang (Yang number) ως τα κύρια χαρακτηριστικά της. Τα πολλαπλασιαστικά θεωρήματα του Yang σε T-ακολουθίες χρησιμοποιούν κατάλληλες ακολουθίες, οι οποίες κατασκευάζονται από βασικές ακολουθίες μικρότερου μήκους, για να παράγουν T-ακολουθίες μεγαλύτερου μήκους. Έτσι είναι εφικτό να κατασκευάσουμε T-πίνακες μεγαλύτερων τάξεων και με την βοήθεια του

σχηματισμού Goethals-Seidel, που είναι ένας πολύ χρήσιμος ορθογώνιος σχεδιασμός, να παράγουμε πίνακες Hadamard για διάφορες τάξεις. Η δομή και τα βήματα που διεκπαιραιώσαμε για την μεταφορά αυτών των μεθόδων σε μια αλγοριθμική υλοποίηση δείχνουν ότι είναι μια ιδανική περίπτωση για την χρήση προχωρημένων προγραμματιστικών τεχνικών όπως είναι το metaprogramming.

Δίνουμε τους απαραίτητους ορισμούς που χρειάζοντα για να σχηματίσουμε το απαραίτητο θεωρητικό υπόβαθρο στα πολλαπλασιαστικά θεωρήματα του Yang σε T-ακολουθίες. Για περαιτέρω λεπτομέρειες σε ακολουθίες με μηδενική αυτοσυσχέτιση και πολλαπλασιαστικές μεθόδους σε T-ακολουθίες παραπέμπουμε τον αναγνώστη στα [122, 143] και [148, 147, 237, 238, 239].

Ορισμός 10 *Τεσσερις* $(-1,1)$ *ακολουθίες* A,B,C,D *μήκους* $n+p, n+p, n, n$ *θα καλούνται βασικές ακολουθίες, (και θα συμβολίζονται ως* $BS(n+p,n)$*) αν:*

1. $N_A(s)+N_B(s)+N_C(s)+N_D(s) = \begin{cases} 0, & s=1,\ldots,n-1 \\ 4n+2p, & s=0 \end{cases}$
2. $N_A(s)+N_B(s)=0, s=n,\ldots,n+p-1$

όπου με N_X *συμβολίζουμε τη μη-περιοδική συνάρτηση αυτοσυσχέτισης μιας ακολουθίας* X*.*

Ορισμός 11 *Αν* A,B,C,D *είναι βασικές ακολουθίες μήκους* $n+1, n+1, n, n$ *τότε οι ακολουθίες* $[\frac{1}{2}(A+B)]$, $[\frac{1}{2}(A-B)]$, $[\frac{1}{2}(C+D)]$, $[\frac{1}{2}(C-D)]$ *θα καλούνται κατάλληλες ή Yang ακολουθίες.*

Ορισμός 12 *Τέσσερις ακολουθίες* X,Y,Z,W *μήκους* n *με στοιχεία* $(-1,0,1)$ *θα καλούνται* T*-ακολουθίες, (και θα συμβολίζονται ως* $TS(n)$*) αν:*

1. $|x_i|+|y_i|+|z_i|+|w_i|=1,\ i=1,\ldots,n.$
2. $N_X(s)+N_Y(s)+N_Z(s)+N_W(s) = \begin{cases} 0, & s=1,\ldots,n-1 \\ n, & s=0 \end{cases}$

Ορισμός 13 *Τέσσερις κυκλικοί πίνακες* T_1, T_2, T_3, T_4 *τάξεως* t *με στοιχεία* $(-1,0,1)$ *θα καλούνται* T*-πίνακες αν:*

1. $T_i * T_j = 0, i \neq j$ *(* $*$ *συμβολίζει το γινόμενο Hadamard)*
2. $T_1T_1^T + T_2T_2^T + T_3T_3^T + T_4T_4^T = tI_t.$

Είναι γνωστό ότι, T-ακολουθίες παράγουν πάντα T-πίνακες εφόσον μια T-ακολουθία μήκους n μπορεί να χρησιμοποιηθεί ως n πρώτη γραμμή ενός κυκλικού πίνακα που δίνει έναν T-πίνακα τάξης n, αλλά το αντίστροφο δεν ισχύει.

Σε μια σειρά εργασιών το 1982 και 1983, ο Yang [237, 238, 239] βρήκε οτι οι βασικές ακολουθίες μπορούν να πολλαπλασιαστούν με $3, 7, 13$ και $2g+1$, όπου g έιναι ένας αριθμός Golay: $g = 2^a 10^b 26^c$, $a, b, c \geq 0$. Αυτές οι τιμές είναι παραδείγματα αυτών που καλούνται σήμερα αριθμοί Yang. Τα αποτελέσματα αυτών των εργασιών σε πολλαπλασιαστικές μεθόδους μπορούν να συνοψιστούν ως ακολούθως: Εάν υπάρχει μια πολλαπλασιαστική μέθοδος που χρησιμοποιεί κατάλληλες ακολουθίες μήκους $n+p, n+p, n, n$ για να παράγει T-ακολουθίες μήκους $y(2n+p)$, τότε το y θα καλείται αριθμός Yang. Η ύπαρξη των αριθμών Yang δίνεται στην ακόλουθη πρόταση.

Πρόταση 11 (Koukouvinos [143]) *Οι αριθμοί Yang είναι γνωστοί για* $y \epsilon \{3, 5, 7, \ldots, 33, 37, 39, 41, 45, 49, 51, 53, 57, 59, 61, 65, 81\}$ *και για όλα τα* $y = 2g+1 > 81$, *όπου* g *είναι ένας αριθμός Golay [148, 208, 240].*

Δίνουμε τις πολλαπλασιαστικές μεθόδους του Yang για $y = 3, 5, 7, 9, 11$ και $p = 1$ στη μορφή που τις συμπεριλάβαμε στην υλοποίηση μας στο υπολογιστικό πακέτο Maple στα ακόλουθα θεωρήματα.

Θεώρημα 4 (Yang [237]) *Υποθέτουμε οτι* A, B, C, D *είναι κατάλληλες (Yang) ακολουθίες μήκους* $n+1, n+1, n, n$ *και με* S^* *συμβολίζουμε την αντίστροφη ακολουθία της* S. *Τότε οι ακόλουθες ακολουθίες,*
$X = [A, C; 0_{n+1}, 0_n; -B^*, 0_n]$
$Y = [B, D; 0_{n+1}, 0_n; A^*, 0_n]$
$Z = [0_{n+1}, 0_n; A, -C; 0_{n+1}, -D^*]$
$W = [0_{n+1}, 0_n; B, -D; 0_{n+1}, C^*]$
είναι T-*ακολουθίες μήκους* $3(2n+1)$.

Θεώρημα 5 (Yang [238]) *Υποθέτουμε οτι* A, B, C, D *είναι κατάλληλες (Yang) ακολουθίες μήκους* $n+1, n+1, n, n$ *και με* S^* *συμβολίζουμε την αντίστροφη ακολουθία της* S. *Τότε οι ακόλουθες ακολουθίες,*
$X = [A, C; 0_{n+1}, 0_n; -A, C; 0_{n+1}, 0_n; -B^*, 0_n]$
$Y = [B, D; 0_{n+1}, 0_n; -B, D; 0_{n+1}, 0_n; A^*, 0_n]$
$Z = [0_{n+1}, 0_n; A, C; 0_{n+1}, 0_n; A, -C; 0_{n+1}, -D^*]$
$W = [0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; B, -D; 0_{n+1}, C^*]$
είναι T-*ακολουθίες μήκους* $5(2n+1)$.

Θεώρημα 6 (Yang [239]) *Υποθέτουμε οτι* A, B, C, D *είναι κατάλληλες (Yang) ακολουθίες μήκους* $n+1, n+1, n, n$ *και με* S^* *συμβολίζουμε την αντίστροφη ακολουθία της* S*. Τότε οι ακόλουθες ακολουθίες,*
$X = [-A, C; 0_{n+1}, 0_n; A, D; 0_{n+1}, 0_n; A, C; 0_{n+1}, 0_n; -B^*, 0_n]$
$Y = [-B, D; 0_{n+1}, 0_n; B, -C; 0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; A^*, 0_n]$
$Z = [0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; -B, -C; 0_{n+1}, 0_n; A, C; 0_{n+1}, -D^*]$
$W = [0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; A, -D; 0_{n+1}, 0_n; B, D; 0_{n+1}, C^*]$
είναι T*-ακολουθίες μήκους* $7(2n+1)$*.*

Θεώρημα 7 (Yang [240]) *Υποθέτουμε οτι* A, B, C, D *είναι κατάλληλες (Yang) ακολουθίες μήκους* $n+1, n+1, n, n$ *και με* S^* *συμβολίζουμε την αντίστροφη ακολουθία της* S*. Τότε οι ακόλουθες ακολουθίες,*
$X = [-A, C; 0_{n+1}, 0_n; A, C; 0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; A, C; 0_{n+1}, 0_n; -B^*, 0_n]$
$Y = [-B, D; 0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; A^*, 0_n]$
$Z = [0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; -A, -C; 0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; A, C; 0_{n+1}, -D^*]$
$W = [0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; -B, -D; 0_{n+1}, 0_n; B, D; 0_{n+1}, C^*]$
είναι T*-ακολουθίες μήκους* $9(2n+1)$*.*

Θεώρημα 8 (Yang [240]) *Υποθέτουμε οτι* A, B, C, D *είναι κατάλληλες (Yang) ακολουθίες μήκους* $n+1, n+1, n, n$ *και με* S^* *συμβολίζουμε την αντίστροφη ακολουθία της* S*. Τότε οι ακόλουθες ακολουθίες,*
$X = [A, C; 0_{n+1}, 0_n; -A, D; 0_{n+1}, 0_n; A, C; 0_{n+1}, 0_n; A, -D; 0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; -B^*, 0_n]$
$Y = [B, -D; 0_{n+1}, 0_n; -B, C; 0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; B, -C; 0_{n+1}, 0_n; B, D; 0_{n+1}, 0_n; A^*, 0_n]$
$Z = [0_{n+1}, 0_n; -A, -C; 0_{n+1}, 0_n; -B, -C; 0_{n+1}, 0_n; A, -C; 0_{n+1}, 0_n; B, C; 0_{n+1}, 0_n; A, -C; 0_{n+1}, -D^*]$
$W = [0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; -A, -D; 0_{n+1}, 0_n; B, -D; 0_{n+1}, 0_n; A, D; 0_{n+1}, 0_n; -B, -D; 0_{n+1}, C^*]$
είναι T*-ακολουθίες μήκους* $11(2n+1)$*.*

Είναι αρκετά γνωστό ότι, αν υπάρχουν T-ακολουθίες μήκους t τότε υπάρχει ένας πίνακας Hadamard τάξεως 4t. Δίνουμε το ακόλουθο θεώρημα κατασκευής πινάκων Hadamard τάξεως 4t (από T-ακολουθίες μήκους t), στη μορφή που το χρησιμοποιήσαμε στο λογισμικό που αναπτύξαμε για την εύρεση νέων μη-ισοδύναμων πινάκων Hadamard.

Θεώρημα 9 (Cooper και Wallis [29]) *Υποθέτουμε ότι υπάρχουν κυκλικοί* T*-πίνακες (ή ισοδύναμα* T*-ακολουθίες)* T_i, $i = 1, \ldots, 4$ *τάξεως* n. *Τότε οι πίνακες,*

$$\begin{aligned} A &= T_1 + T_2 + T_3 + T_4 \\ B &= -T_1 + T_2 + T_3 - T_4 \\ C &= -T_1 - T_2 + T_3 + T_4 \\ D &= -T_1 + T_2 - T_3 + T_4 \end{aligned}$$

μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel (βλ. [70, σελ. 107]), για να παράγουν έναν πίνακα Hadamard τάξεως $4n$.

§2.2.3 Λογισμικό για Σχεδόν-Κανονικές Ακολουθίες

Υλοποιήσαμε ένα metaprogram το οποίο δέχεται ως είσοδο ένα αρχείο HTML με σχεδόν-κανονικές ακολουθίες και παράγει τα ανεξάρτητα αρχεια σχεδόν-κανονικών ακολουθιών τα οποία παράγουν ένα πρόγραμμα MAPLE το οποίο εκτελείται και παράγει τους αντίστοιχους πίνακες Hadamard για συγκεκριμένους αριθμούς Yang. Το metaprogram χρησιμοποιεί το BASH SHELL ως metalanguage ενώ η object-language στην οποία κάθε πρόγραμμα εισάγεται είναι το πακέτο συμβολικών υπολογισμών, MAPLE. Σχεδιάσαμε και υλοποιήσαμε το πακέτο `YangMultiplications` στο MAPLE για τους σκοπούς του metaprogram μας. Επιπρόσθετα, κάναμε εκτεταμένη χρήση του UNIX `sed` streaming editor, για να μετατρέψουμε κάθε πίνακα Hadamard σε μια μορφή κατάλληλη να την δεχθεί ως είσοδο το Magma καθώς και της UNIX `awk` pattern-matching γλώσσας προγραμματισμού, για να αναγνωρίσουμε δυναμικά τα μήκη κάθε σχεδόν κανονικής ακολουθίας. Ορισμένες από τις κυριότερες δυσκολίες στον σχεδιασμό ενός τέτοιου προγράμματος εντοπίζονται στην δυναμική παραγωγή των τιμών των μεταβλητών που τους έχουν ανατεθεί τα χαρακτηριστικά των σχεδόν κανονικών ακολουθιών από το αρχείο εισόδου, π.χ. το μήκος κάθε $NNS(n)$, ο αριθμός των διαθέσιμων συνόλων $NNS(n)$ για μια συγκεκριμένη τιμή του n και n λίστα διάφορων μεταβλητών.

Το BASH SHELL μας παρέχει έναν ευέλικτο τρόπο να εκτελούμε εντόλες σε περιβάλλον UNIX και άλλα προγράμματα χρησιμοποιώντας τα ονόματα των αρχείων ως ορίσματα. Το metaprogram το οποίο παράγει τους

πίνακες Hadamard έχει ως μόνη είσοδο ένα αρχείο με σχεδόν-κανονικές ακολουθίες και υλοποιείται ως ένα BASH SHELL αλγόριθμος το οποίο εκτελεί τα ακόλουθα βήματα:

Algorithm 16 NEARNORMALSEQS2HADAMARDMATRIX ALGORITHM

function NEARNORMALSEQS2HADAMARDMATRIX(N1, N2, N3, N4)
Require: NNS(n) exist

Step 1 Initialize variables, such as the number of lines, L, which are going to be processed from the input file and the Yang numbers, YangNumberLimit, that are going to be computed.

Step 2 (bash loop) Begin iterative loop until condition L is met.

Step 2a do `sed` to isolate a set of NNS(n) from the input html file.

Step 2b do `awk` to identify the length n of each NNS(n).

Step 2c Create suitable indices for filenames targeting the individual sets of NNS(n).

Step 2d do `sed` and `awk` to transform the individual file containing one set of NNS(n) into Maple format.

Step 3 (Maple loop) Begin iterative loop for automated Maple code generation until condition YangNumberLimit is met.

Step 3a Create input files in Maple format from the processed files of NNS(n).

Step 3b Append to each file a Maple command that reads the `YangMultiplications` package.

Step 3c Append to each file a Maple command that calls the `YangMultiplication2HM` procedure from the Maple package.

Step 3d Append to each file a Maple command that writes the generated Hadamard matrix into a result file.

Step 3e Execute the Maple program with the implementation of the Yang multiplication method for a specific Yang number.

Step 3f do `sed` to the result file to transform the generated Hadamard matrix into Magma format.

Step 4 (Magma session) Begin Magma session to validate the generated Hadamard matrix.

Step 4a Create input files in Magma format from the generated Hadamard matrices.

Step 4b Append to each file the `IsHadamard` Magma command to check the validity of the Hadamard matrix.

Step 4c Execute the Magma program.

end Magma session

end Maple loop

Step 5 Remove any intermediate files produced.

end bash loop

end function

Το υπολογιστικό πακέτο, MAPLE μας παρέχει έναν έξοχο τρόπο για την εκτέλεση συμβολικών και αριθμητικών υπολογισμών, ειδικά όταν υλοποιούμε μεθόδους που είναι βασισμένες στα διακριτά μαθηματικά.

Υλοποιήσαμε τις πολλαπλασιαστικές μεθόδους του Yang για βασικές και σχεδόν-κανονικές ακολουθίες στο MAPLE, έτσι ώστε να έχουμε την μέγιστη δυνατή ευελιξία και φορησιμότητα με άλλα πακέτα Υπολογιστικής Άλγεβρας, όπως είναι το MAGMA. Υλοποιήσαμε ένα πακέτο MAPLE το οποίο περιέχει όλες τις απαραίτητες ρουτίνες για την παραγωγή των πινάκων Hadamard από σχεδόν-κανονικές ακολουθίες. Μια

περιγραφή των κυριότερων ρουτινών δίνεται παρακάτω.

Οι ρουτίνες Maple

NearNormalSeqs2BaseSeqs Αυτή η ρουτίνα δέχεται ως είσοδο ένα αρχείο με σχεδόν κανονικές ακολουθίες μηκους $2n+1$ και επιστρέφει βασικές ακολουθίες μήκους $n+1, n+1, n, n$.

BaseSeqs2YangSeqs Αυτή η ρουτίνα δέχεται ως είσοδο ένα αρχείο βασικών ακολουθίων μήκους $n+1, n+1, n, n$ και δίνει ως έξοδο κατάλληλες (Yang) ακολουθίες μήκους $n+1, n+1, n, n$.

YangSeqs2TSeqs Αυτή η ρουτίνα δέχεται ως είσοδο κατάλληλες (Yang) ακολουθίες μήκους $n+1, n+1, n, n$ και τον αριθμό Yang y και δίνει ως έξοδο T-ακολουθίες μήκους $y(2n+1)$. Η παρούσα υλοποίηση περιλαμβάνει τις πολλαπλασιαστικές μεθόδους για $y = 3, 5, 7, 9, 11$.

TSeqs2Hadamard Αυτή η ρουτίνα δέχεται ως είσοδο T-ακολουθίες μήκους n και δίνει ως έξοδο έναν πίνακα Hadamard τάξεως $4n$.

Επιπλέον, δίνουμε τον πρωτότυπο κώδικα Maple της ρουτίνας που καλείται από τον Αλγόριθμο 16 και είναι υπεύθυνη για την παραγωγή πινάκων Hadamard από σχεδόν κανονικές ακολουθίες.

```
YangMultiplications[YangMultiplication2HM] := proc(nn1,nn2,nn3,nn4,y)

local HM, b1, b2, b3, b4, bsy1, bsy2, bsy3, bsy4, X1, Y1, Z1, W1, ot;

b1, b2, b3, b4 := NearNormalSeqs2BaseSeqs(nn1,nn2,nn3,nn4);
bsy1, bsy2, bsy3, bsy4 := BaseSeqs2YangSeqs(b1,b2,b3,b4);
X1, Y1, Z1, W1 := YangSeqs2TSeqs(bsy1,bsy2,bsy3,bsy4,y);
ot := nops(X1);
HM := Matrix(TSeqs2Hadamard(X1,Y1,Z1,W1,ot));

RETURN(HM);

end proc;
```

§2.2.4 Νέοι Mn-Ισοδύναμοι Πίνακες Hadamard από Σχεδόν-Κανονικές Ακολουθίες

Εκτελέσαμε το metaprogram για όλες τις διαθέσιμες σχεδόν-κανονικές ακολουθίες, $NNS(n)$, και παράγαμε τους αντίστοιχους πίνακες Hadamard τάξης $4yn$, για κάθε $y = 3, 5, 7, 9, 11$ όπου y είναι ένας αριθμός Yang. Ο μικρότερος πίνακας Hadamard που κατασκευάσαμε είναι τάξης 60, ενώ ο μεγαλύτερος πίνακας Hadamard που κατασκευάστηκε είναι τάξης 2684. Ολόκληρη η βάση δεδομένων των παραγόμενων πινάκων Hadamard είναι διαθέσιμη σε μορφή Magma εφόσον ζητηθεί.

Επιπλέον, εκτελέσαμε έναν έλεγχο στη βάση δεδομένων που παράγαμε για μη-ισοδύναμους πίνακες Hadamard για τάξεις από 60 σε 1140, χρησιμοποιώντας το 4-profile κριτήριο όπως αυτό έχει υλοποιηθεί στο Magma, για να μελετήσουμε αν αυτοί οι πίνακες Hadamard είναι ισοδύναμοι. Τα αποτελέσματα αυτού του ελέγχου δίνονται στον παρακάτω πίνακα. Συμβολίζουμε με N_n τον αριθμό των πινάκων Hadamard που κατασκευάστηκαν από σχεδόν-κανονικές ακολουθίες, ενώ με IN_n συμβολίζουμε τον αριθμό των μη-ισοδύναμων πινάκων Hadamard που βρήκαμε. Επίσης, συμβολίζουμε με n την τάξη των αντίστοιχων πινάκων Hadamard.

n	N_n	IN_n	n	N_n	IN_n	n	N_n	IN_n	n	N_n	IN_n
60	1	1	100	1	1	108	2	2	140	1	1
156	2	2	180	3	3	204	3	3	220	1	1
252	10	10	260	2	2	300	14	14	324	2	2
340	3	3	348	11	11	364	2	2	396	25	25
420	8	8	444	20	20	468	2	2	476	3	3
492	18	18	500	14	14	540	31	31	572	2	2
580	11	11	588	20	20	612	3	3	636	2	2
660	23	23	684	3	3	700	14	14	732	1	1
740	20	20	748	3	3	756	8	8	812	11	11
820	18	18	900	45	45	924	31	31	980	12	12
1036	20	20	1044	11	11	1060	2	2	1100	14	14
1140	3	3									

Πίνακας 2.4: Νέοι μη-ισοδύναμοι πίνακες Hadamard από σχεδόν-κανονικές ακολουθίες, τάξεων $60 \leq n \leq 1140$

Από τα υπολογιστικά αποτελέσματα που παρουσιάστηκαν στον προηγούμενο πίνακα μπορούμε να εξάγουμε την ακόλουθη παρατήρηση.

Παρατήρηση 4 *Σημειώνουμε ότι, όλοι οι πίνακες Hadamard που κατασκευάζονται από τις πολλαπλασιαστικές μεθόδους του Yang για σχεδόν-κανονικές ακολουθίες είναι μη-ισοδύναμοι, καθώς για κάθε τάξη βρήκαμε ότι τα αντίστοιχα 4-profiles είναι διαφορετικά.*

Επιπλέον, κάποιος θα μπορούσε να ελέγξει τους πίνακες Hadamard για ισοδυναμία, χρησιμοποιώντας το graph isomorphism κριτήριο, το οποίο είναι πολυ πιο χρονοβόρο υπολογιστικά [15, 183].

Η πλήρης ταξινόμηση των μη-ισοδύναμων πινάκων Hadamard τάξεων n είναι γνωστή για $n \equiv 0 \pmod 4$, $n \leq 28$. Για $n = 32, 36$ υπάρχουν τουλάχιστον $3,578,006$ και $4,745,357$ μη-ισοδύναμοι πίνακες Hadamard αντίστοιχα, βλ. [190]. Επιπλέον, υπάρχουν κάποια θεωρητικά αποτελέσματα που παρέχουν τεράστια κάτω φράγματα, βλ. [168, 169, 185] αλλά αυτοί οι πίνακες δεν είναι διαθέσιμοι. Από αυτήν τη σκοπιά, πιστεύουμε ότι τα δικά μας κάτω φράγματα στον αριθμό των μη-ισοδύναμων πινάκων Hadamard, που παρουσιάστηκαν σε αυτήν την ενότητα, έχουν ιδιαίτερη αξία για πρακτικές εφαρμογές στα πεδία της Συνδυαστικής και της Στατιστικής (βλ. και Ενότητα 2.1.1) καθώς είναι κατασκευαστικά. Τέλος, θεωρούμε σκόπιμο να αναφέρουμε οτι η βάση δεδομένων των πινάκων Hadamard που παράγαμε ταχυδρομήθηκε ηλεκτρονικά στον καθ. J. Cannon, επικεφαλή του Computational Algebra Group του School of Mathematics and Statistics του University of Sydney, το οποίο είναι υπεύθυνο για την ομαλή λειτουργία και περαιτέρω ανάπτυξη του πακέτου υπολογιστικής άλγεβρας Magma.

§2.3 Πίνακες Hadamard από Ορθογώνιους Σχεδιασμούς

Σε αυτήν την ενότητα, παρουσιάζουμε διάφορες θεωρητικές και αλγοριθμικές κατασκευές ορθογώνιων σχεδιασμών, μέσω των οποίων παράγονται αντίστοιχοι πίνακες Hadamard διαφόρων τάξεων. Αρχικά δίνουμε τους απαραίτητους ορισμούς που χρειάζονται από τη Θεωρία σχεδιασμών για να σχηματίσουμε το απαραίτητο θεωρητικό υπόβαθρο για τις μεθόδους κατασκευής που θα παρουσιαστούν.

§2.3.1 Στοιχεία Θεωρίας Ορθογώνιων Σχεδιασμών

Ένας *ορθογώνιος σχεδιασμός (orthogonal design)* τάξης n και τύπου (type) $(s_1, s_2, \ldots, s_k)$ συμβολίζόμενος με $OD(n; s_1, s_2, \ldots, s_k)$ στις μεταθετικές μεταβλητές $x_1, x_2, \ldots, x_k$, είναι ένας τετραγωνικός πίνακας D τάξης n με στοιχεία από το σύνολο $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ που ικανοποιεί τη σχέση

$$DD^T = \sum_{i=1}^{k} (s_i x_i^2) I_n,$$

όπου I_n είναι ο μοναδιαίος πίνακας τάξης n. Με βάση αυτό τον ορισμό, ένας πίνακας Hadamard τάξης n είναι ένας $OD(n; n)$. Οι ορθογώνιοι σχεδιασμοί χρησιμοποιούνται στη Συνδυαστική, στη Στατιστική, στη Θεωρία κωδίκων, τις τηλεπικοινωνίες καθώς και σε διάφορες άλλες περιοχές. Για περισσότερες λεπτομέρειες στους ορθογώνιους σχεδιασμούς παραπέμπουμε στις [70, 206].
Είναι γνωστό ότι, ο μέγιστος αριθμός των μεταβλητών που μπορεί να εμφανιστεί σε έναν ορθογώνιο σχεδιασμό δίνεται από τη συνάρτηση του Radon $\rho(n)$ που ορίζεται ως $\rho(n) = 8c + 2^d$, όπου $n = 2^a b$, b περιττό, $a = 4c + d$, $0 \leq d < 4$, (βλ. [70]). Ένας $OD(m; a_1, \ldots, a_k)$ θα καλείται πλήρης ορθογώνιος σχεδιασμός (full orthogonal design), αν $a_1 + \cdots + a_k = m$.

Θα χρειαστούμε επίσης τους ακόλουθους ορισμούς από τις ακολουθίες με μηδενική συνάρτηση αυτοσυσχετίσης.

Ορισμός 14 *Δυο ακολουθίες,* $A = [a_1, \cdots, a_n]$ *και* $B = [b_1, \cdots, b_n]$*, μήκους* n *θα λέμε ότι έχουν PAF μηδέν ή μηδενική περιοδική συνάρτηση αυτοσυσχέτισης (αντίστοιχα NPAF μηδέν ή μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης), αν* $P_A(s) + P_B(s) = 0$ *(αντίστοιχα αν* $N_A(s) + N_B(s) = 0$*) για* $s = 1, \ldots, n-1$*.*

Ορισμός 15 *Δυο ακολουθίες,* $A = [a_1, \cdots, a_n]$ *και* $B = [b_1, \cdots, b_n]$*, μήκους* n *με στοιχεία* $\{-1, +1\}$ *καλούνται* ακολουθίες Golay *αν έχουν NPAF μηδέν, δηλαδή αν* $N_A(s) + N_B(s) = 0$ *για* $s = 1, \ldots, n-1$*.*

Επίσης χρειαζόμαστε τον ακόλουθο ορισμό από την [153]:

Ορισμός 16 *Δύο ακολουθίες μήκους* n*, που έχουν PAF ή NPAF μηδέν, θα λέμε ότι έχουν τύπο* (u, v) *αν οι ακολουθίες συνθέτονται από δυο μεταβλητές, έστω* a *και* b*, έτσι ώστε οι* a *και* $-a$ *να εμφανίζονται συνολικά* u *φορές και οι* b *και* $-b$ *να εμφανίζονται συνολικά* v *φορές.*

Έστω B_i, $i = 1, 2, 3, 4$ κυκλικοί πίνακες τάξης n με στοιχεία από το σύνολο $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ που ικανοποιούν την σχέση

$$\sum_{i=1}^{4} B_i B_i^T = \sum_{i=1}^{k} (s_i x_i^2) I_n.$$

Τότε, ο σχηματισμός Goethals-Seidel

$$G = \begin{pmatrix} B_1 & B_2R & B_3R & B_4R \\ -B_2R & B_1 & B_4^TR & -B_3^TR \\ -B_3R & -B_4^TR & B_1 & B_2^TR \\ -B_4R & B_3^TR & -B_2^TR & B_1 \end{pmatrix}, \tag{2.1}$$

όπου R είναι ο πίσω-διαγώνιος ταυτοτικός πίνακας, είναι ένας $OD(4n; s_1, s_2, \ldots, s_k)$ (βλ. [70, σελ. 107]).

Παρατήρηση 5 *Σημειώνουμε ότι, αν υπάρχουν τέσσερις ακολουθίες* A_1*,* A_2*,* A_3*,* A_4 *μήκους* n *με στοιχεία από το σύνολο* $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ *με μηδενική περιοδική ή μη-περιοδική συνάρτηση αυτοσυσχέτισης, τότε αυτές οι ακολουθίες μπορούν να χρησιμοποιηθούν ως οι πρώτες γραμμές των αντίστοιχων κυκλικών πινάκων* $B_i = \mathrm{circ}(A_i)$*,* $i = 1, 2, 3, 4$*, στο σχηματισμό Goethals-Seidel για να σχηματίσουν έναν* $OD(4n; s_1, s_2, s_3, s_4)$*.*

Ένα ζεύγος πινάκων A, B θα λέμε ότι είναι amicable (anti-amicable) αν $AB^T - BA^T = 0$ ($AB^T + BA^T = 0$). Από την εργασία του Kharaghani [121] ένα σύνολο $\{A_1, A_2, \ldots, A_{2n}\}$ από τετραγωνικούς πραγματικούς πίνακας θα λέμε ότι είναι *amicable* αν ισχύει

$$\sum_{i=1}^{n} \left(A_{\sigma(2i-1)} A_{\sigma(2i)}^T - A_{\sigma(2i)} A_{\sigma(2i-1)}^T \right) = 0$$

για κάποια μετάθεση σ του συνόλου $\{1, 2, \ldots, 2n\}$. Για απλότητα, θα θεωρούμε πάντα $\sigma(i) = i$ εκτός αν δηλωθεί διαφορετικά. Συνεπώς,

$$\sum_{i=1}^{n} \left(A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0. \tag{2.2}$$

Προφανώς, ένα σύνολο από αμοιβαίους amicable πίνακες είναι amicable αλλά το αντίστροφο δεν είναι αληθές γενικά. Κατά τη διάρκεια αυτής της ενότητας με R_k θα συμβολίζουμε τον πίσω-διαγώνιο ταυτοτικό πίνακα τάξης k.

Ένα σύνολο από πίνακες $\{A_1, A_2, \ldots, A_n\}$ τάξης m με στοιχεία από το σύνολο $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ ικανοποιεί μια προσθετική ιδιότητα αν

$$\sum_{i=1}^{n} A_i A_i^T = \sum_{i=1}^{k} (s_i x_i^2) I_m. \tag{2.3}$$

Για τα αποτελέσματα αυτής της ενότητας, χρειαζόμαστε τον ακόλουθο σχηματισμό από την [121]. Έστω $\{A_i\}_{i=1}^{8}$ ένα amicable σύνολο από οκτώ κυκλικούς πίνακες τάξεως t, που ικανοποιούν την προσθετική ιδιότητα για $(s_1, s_2, \ldots, s_k)$. Τότε ο σχηματισμός Kharaghani

$$H = \begin{pmatrix}
A_1 & A_2 & A_4R_n & A_3R_n & A_6R_n & A_5R_n & A_8R_n & A_7R_n \\
-A_2 & A_1 & A_3R_n & -A_4R_n & A_5R_n & -A_6R_n & A_7R_n & -A_8R_n \\
-A_4R_n & -A_3R_n & A_1 & A_2 & -A_8^TR_n & A_7^TR_n & A_6^TR_n & -A_5^TR_n \\
-A_3R_n & A_4R_n & -A_2 & A_1 & A_7^TR_n & A_8^TR_n & -A_5^TR_n & -A_6^TR_n \\
-A_6R_n & -A_5R_n & A_8^TR_n & -A_7^TR_n & A_1 & A_2 & -A_4^TR_n & A_3^TR_n \\
-A_5R_n & A_6R_n & -A_7^TR_n & -A_8^TR_n & -A_2 & A_1 & A_3^TR_n & A_4^TR_n \\
-A_8R_n & -A_7R_n & -A_6^TR_n & A_5^TR_n & A_4^TR_n & -A_3^TR_n & A_1 & A_2 \\
-A_7R_n & A_8R_n & A_5^TR_n & A_6^TR_n & -A_3^TR_n & -A_4^TR_n & -A_2 & A_1
\end{pmatrix} \tag{2.4}$$

είναι ένας $OD(8t; s_1, s_2, \ldots, s_k)$.

§2.3.2 Νέες Μέθοδοι Κατασκευής Πλήρων Ορθογώνιων Σχεδιασμών

Σε αυτήν την ενότητα, δίνουμε ορισμένες νέες κατασκευές για πλήρεις ορθογώνιους σχεδιασμούς από ακολουθίες με μηδενική συνάρτηση αυτοσυσχέτισης. Πλήρεις ορθογώνιοι σχεδιασμοί μπορούν να χρησιμοποιηθούν για να παράγουν πίνακες Hadamard όπως θα δούμε σε επόμενες ενότητες.

Θεώρημα 10 *Έστω ότι υπάρχουν δύο ακολουθίες μήκους* n *με NPAF μηδέν και τύπου* (u, v) *όπου* $u + v = 2n$. *Επιπλέον, υποθέτουμε ότι υπάρχουν δύο ακολουθίες Golay μήκους* g. *Τότε, υπάρχει ένας πλήρης ορθογώνιος σχεδιασμός σε τέσσερις μεταβλητές,* $\mathrm{OD}(4 \cdot (n + 2g); 2u, 2v, 4g, 4g)$.

Απόδειξη. Ας συμβολίσουμε τις δυο ακολούθίες μήκους n, με NPAF μηδέν και τύπο (u, v) όπου $u + v = 2n$ με $A = [a_1, \cdots, a_n]$ και $B = [b_1, \cdots, b_n]$ όπου $a_k, b_k \in \{\pm\alpha, \pm\beta\}$, $k = 1, \ldots, n$ και $a_k \neq 0$, $b_k \neq 0$.
Στη συνέχεια, θεωρούμε τις δυο ακολουθίες Golay μήκους g, έστω G και H. Συμβολίζουμε με $G^\star$ και $H^\star$ τις αντίστροφες ακολουθίες των G και H αντίστοιχα. Το σύμβολο $|$ δηλώνει την παράθεση των ακολουθιών. Έστω x και y να είναι μεταθετικές μεταβλητές. Τότε ο $\mathrm{OD}(4 \cdot (n + 2g); 2u, 2v, 4g, 4g)$ μπορεί να κατασκευαστεί σχηματίζοντας τους τέσσερις κυκλικούς πίνακες με δοθείσες πρώτες γραμμές P, Q, R, S όπως παρακάτω, που στη συνέχεια χρησιμοποιούνται στο σχηματισμό Goethals-Seidel.

$$\begin{array}{lcccccc} P = [& a_1, & \cdots, & a_n \mid & Gx \mid & Hy &] \\ Q = [& a_1, & \cdots, & a_n \mid & -Gx \mid & -Hy &] \\ R = [& b_1, & \cdots, & b_n \mid & H^\star x \mid & -G^\star y &] \\ S = [& b_1, & \cdots, & b_n \mid & -H^\star x \mid & G^\star y &] \end{array} \tag{2.5}$$

Οι ακολουθίες P, Q, R, S έχουν NPAF μηδέν. Πράγματι, αν συμβολίσουμε με $P' = [Gx \mid Hy]$ και $Q' = [H^\star x \mid -G^\star y]$, τότε οι ακολουθίες P' και Q' είναι μήκους $2g$ και τύπου $(2g, 2g)$ με NPAF μηδέν. Οποιοδήποτε γινόμενα τα οποία προκύπτουν στο NPAF του P από τα στοιχεία της P' με τα στοιχεία της ακολουθίας $[a_1, \cdots, a_n]$ διαγράφονται στο NPAF της Q από τα γινόμενα των στοιχείων της $-P'$ με τα στοιχεία της ακολουθίας $[a_1, \cdots, a_n]$. Ομοίως για την Q' και την ακολουθία $[b_1, \cdots, b_n]$ στις R και S. Το άθροισμα των γινομένων των στοιχείων της ακολουθίας $[a_1, \cdots, a_n]$ με τα γινόμενα των στοιχείων της ακολουθίας $[b_1, \cdots, b_n]$ είναι ίσο με μηδέν στο NPAF των P, Q, R, S, καθώς οι ακολουθίες A και B έχουν NPAF μηδέν. Ομοίως για το άθροισμα των γινομένων των στοιχείων της ακολουθίας P' με τα γινόμενα των στοιχείων της Q' στο NPAF των P, Q, R, S, καθώς αυτές οι ακολουθίες έχουν NPAF μηδέν. Αυτό δίνει και τον ζητούμενο $\mathrm{OD}(4 \cdot (n + 2g); 2u, 2v, 4g, 4g)$. □

Δείχνουμε την εφαρμογή του Θεωρήματος 10 με το παρακάτω παράδειγμα.

Παράδειγμα 9 Θεωρούμε τις ακολουθίες μήκους $n = 4$, με NPAF μηδέν και τύπο $(u, v) = (4, 4)$ από την [153]:

```
A = [ a,  a, b, -b]
B = [ a, -a, b,  b]
```

Θεωρούμε τις ακολουθίες Golay μήκους $g = 2$, με NPAF μηδέν:

$$G = [1, 1] \quad \text{και} \quad H = [1, -1].$$

Τότε οι αντίστροφες ακολουθίες $G^\star$ και $H^\star$ των G και H είναι:

$$G^\star = [1, 1] \quad \text{και} \quad H^\star = [-1, 1].$$

Οι ακολουθίες $P' = [Gx \mid Hy]$ και $Q' = [H^\star x \mid -G^\star y]$ που έχουν NPAF μηδέν και τύπο $(2g, 2g) = (4, 4)$ είναι:

$$P' = [x, x, y, -y] \quad \text{και} \quad Q' = [-x, x, -y, -y].$$

Τότε οι ζητούμενες ακολουθίες P, Q, R, S που θα έχουν NPAF μηδέν είναι οι:

$$\begin{array}{lcccccccc} P & = [& a, & a, & b, & -b, & x, & x, & y, & -y &] \\ Q & = [& a, & a, & b, & -b, & -x, & -x, & -y, & y &] \\ R & = [& a, & -a, & b, & b, & -x, & x, & -y, & -y &] \\ S & = [& a, & -a, & b, & b, & x, & -x, & y, & y &] \end{array}$$

και μπορούν να χρησιμοποιηθούν στον σχηματισμό Goethals-Seidel για να παράγουν έναν πλήρη ορθογώνιο σχεδιασμό $\mathrm{OD}(4 \cdot (n + 2g); 2u, 2v, 4g, 4g)$, δηλαδή έναν $\mathrm{OD}(32; 8, 8, 8, 8)$.

Θεώρημα 11 *Έστω ότι υπαρχουν δυο ακολουθίες Golay μήκους* g_1. *Επιπλέον, υποθέτουμε ότι υπάρχει άλλο ένα σύνολο από δυο ακολουθίες Golay μήκους* g_2. *Τότε, υπάρχει ένας πλήρης ορθογώνιος σχεδιασμός σε τρεις μεταβλητές,* $OD(4 \cdot (g_1 + 2g_2); 4g_1, 4g_2, 4g_2)$.

Απόδειξη. Έστω A και B οι δυο ακολουθίες Golay μήκους g_1 με στοιχεία $\{-1, +1\}$. Πολλαπλασιάζουμε τις A και B με την μεταβλητή α:

$$\begin{array}{l} A = [\ a_1,\ a_2,\ \cdots,\ a_{g_1}\ ] \\ B = [\ b_1,\ b_2,\ \cdots,\ b_{g_1}\ ] \end{array} \tag{2.6}$$

όπου $a_k, b_k \in \{\pm\alpha\}, k = 1, \ldots, n$ και $a_k \neq 0,\ b_k \neq 0$.
Στη συνέχεια θεωρούμε τις δυ ακολουθίες Golay μήκους g_2, έστω G και H. Συμβολίζουμε με $G^\star$ και $H^\star$ τις αντίστροφες ακολουθίες των G και H, αντίστοιχα. Το σύμβολο | υποδηλώνει την παράθεση των ακολουθιών. Έστω x και y μεταθετικές μεταβλητές. Τότε ο $OD(4 \cdot (g_1 + 2g_2); 4g_1, 4g_2, 4g_2)$ μπορεί να κατασκευαστεί σχηματίζοντας τους τέσσερις κυκλικούς πίνακες με δοθέισες πρώτες γραμμές P, Q, R, S όπως παρακάτω, που στην συνέχεια χρησιμοποιούνται στο σχηματισμό Goethals-Seidel.

$$\begin{array}{l} P = [\ a_1,\ \cdots,\ a_{g_1} \mid\ Gx \mid\ Hy\ ] \\ Q = [\ a_1,\ \cdots,\ a_{g_1} \mid\ -Gx \mid\ -Hy\ ] \\ R = [\ b_1,\ \cdots,\ b_{g_1} \mid\ H^\star x \mid\ -G^\star y\ ] \\ S = [\ b_1,\ \cdots,\ b_{g_1} \mid\ -H^\star x \mid\ G^\star y\ ] \end{array} \tag{2.7}$$

Οι ακολουθίες P, Q, R, S έχουν NPAF μηδέν. Πράγματι, αν συμβολίσουμε με $P' = [Gx \mid Hy]$ και $Q' = [H^\star x \mid -G^\star y]$, τότε οι ακολουθίες P' και Q' είναι μήκους $2g_2$ και τύπου $(2g_2, 2g_2)$ με NPAF μηδέν. Οποιοδήποτε γινόμενα τα οποία προκύπτουν στο NPAF του P από τα στοιχεία της P' με τα στοιχεία της ακολουθίας $[a_1, \cdots, a_{g_1}]$ διαγράφονται στο NPAF της Q από τα γινόμενα των στοιχείων της $-P'$ με τα στοιχεία της ακολουθίας $[a_1, \cdots, a_{g_1}]$. Ομοίως για την Q' και την ακολουθία $[b_1, \cdots, b_{g_1}]$ στις R και S. Το άθροισμα των γινομένων των στοιχείων της ακολουθίας $[a_1, \cdots, a_{g_1}]$ με τα γινόμενα των στοιχείων της ακολουθίας $[b_1, \cdots, b_{g_1}]$ είναι ίσο με μηδέν στο NPAF των P, Q, R, S, καθώς οι ακολουθίες A και B έχουν NPAF μηδέν. Ομοίως για το άθροισμα των γινομένων των στοιχείων της ακολουθίας P' με τα γινόμενα των στοιχείων της Q' στο NPAF των P, Q, R, S, καθώς αυτές οι ακολουθίες έχουν NPAF μηδέν. Αυτό δίνει και τον ζητούμενο $OD(4 \cdot (g_1 + 2g_2); 4g_1, 4g_2, 4g_2)$. □

Δείχνουμε την εφαρμογή του Θεωρήματος 11 με το παρακάτω παράδειγμα.

Παράδειγμα 10 Θεωρούμε τις ακολουθίες Golay μήκους $g_1 = 10$

```
A = [ 1, -1, -1,  1, -1,  1, -1, -1, -1,  1]
B = [ 1, -1, -1, -1, -1, -1, -1,  1,  1, -1]
```

Πολλαπλασιάζουμε τις A και B με την μεταβλητή α:

$$\begin{aligned} A &= [\ \alpha,\ -\alpha,\ -\alpha,\ \alpha,\ -\alpha,\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha\ ] \\ B &= [\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha,\ \alpha,\ -\alpha\ ] \end{aligned}$$

Θεωρούμε τις ακολουθίες Golay μήκους $g_2 = 2$, με NPAF μηδέν:

$$G = [1, 1] \quad \text{και} \quad H = [1, -1].$$

Τότε οι αντίστροφες ακολουθίες $G^\star$ και $H^\star$ των G και H είναι:

$$G^\star = [1, 1] \quad \text{και} \quad H^\star = [-1, 1].$$

Οι ακολουθίες $P' = [Gx \mid Hy]$ και $Q' = [H^\star x \mid -G^\star y]$ που έχουν NPAF μηδέν και τύπο $(2g_2, 2g_2) = (4, 4)$ είναι:

$$P' = [x, x, y, -y] \quad \text{και} \quad Q' = [-x, x, -y, -y].$$

Τότε οι ζητούμενες ακολουθίες P, Q, R, S που θα έχουν NPAF μηδέν είναι οι:

$$\begin{aligned} P &= [\ \alpha,\ -\alpha,\ -\alpha,\ \alpha,\ -\alpha,\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha,\ x,\ x,\ y,\ -y\ ] \\ Q &= [\ \alpha,\ -\alpha,\ -\alpha,\ \alpha,\ -\alpha,\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha,\ -x,\ -x,\ -y,\ y\ ] \\ R &= [\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha,\ \alpha,\ -\alpha,\ -x,\ x,\ -y,\ -y\ ] \\ S &= [\ \alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ -\alpha,\ \alpha,\ \alpha,\ -\alpha,\ x,\ -x,\ y,\ y\ ] \end{aligned}$$

και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για να παράγουν έναν πλήρη ορθογώνιο σχεδιασμό $OD(4 \cdot (g_1 + 2g_2); 4g_2, 4g_2, 4g_1)$, δηλαδή έναν $OD(56; 8, 8, 40)$.

§2.3.3 Αλγόριθμοι Κατασκευής Πλήρων Ορθογώνιων Σχεδιασμών

Σε αυτήν την ενότητα, δίνουμε μια σύντομη περιγραφή της διαδικασίας που χρησιμοποιήσαμε για να παράγουμε πλήρεις ορθογώνιους σχεδιασμούς σε έξι και οκτώ μεταβλητές. Όλα τα amicable σύνολα των οκτώ πινάκων που παράγουν ορθογώνιους σχεδιασμούς κατασκευάστηκανε με αυτή τη διαδικασία. Μια παρόμοια εκδοχή αυτής μπορεί να βρεθεί στην [112]. Έστω A, B, C, D ένα σύνολο απο κυκλικούς πίνακες τάξης m και τύπου (s_1, s_2, s_3, s_4), με στοιχεία από το σύνολο $\{0, \pm a, \pm b, \pm c, \pm d\}$, όπου a, b, c, d είναι μεταθετικές μεταβλητές, οι οποίοι ικανοποιούν την προσθετική ιδιότητα

$$AA^T + BB^T + CC^T + DD^T = (s_1a^2 + s_2b^2 + s_3c^2 + s_4d^2)I_m.$$

Επιπλέον, έστω E, F, G, H ένα ακόμη σύνολο από κυκλικούς πίνακες τάξης m και τύπου (s_5, s_6, s_7, s_8), με στοιχεία από το σύνολο $\{0, \pm e, \pm f, \pm g, \pm h\}$, όπου e, f, g, h είναι μεταθετικές μεταβλητές, οι οποίοι ικανοποιούν την προσθετική ιδιότητα

$$EE^T + FF^T + GG^T + HH^T = (s_5e^2 + s_6f^2 + s_7g^2 + s_8h^2)I_m.$$

Αν υπάρχει ένα matching (ταίριασμα) μεταξύ των συνόλων $\{A, B, C, D\}$ και $\{E, F, G, H\}$ τέτοιο ώστε το σύνολο $\{A, B, C, D, E, F, G, H\}$ να γίνεται amicable, τότε το σύνολο $\{A, B, C, D, E, F, G, H\}$ μπορεί να χρησιμοποιηθεί στο σχηματισμό Kharaghani για να παράγει έναν ορθογώνιο σχεδιασμό $OD(8m; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8)$. Αυτά τα σύνολα καλούνται ειδικά (special) amicable σύνολα πινάκων, βλ. Holzmann και Kharaghani [112].

Ο αλγόριθμος που δίνεται σε αυτήν την ενότητα εφαρμόστηκε στις τετράδες κυκλικών πινάκων που παράγονται από τις θεωρητικές κατασκευές για πλήρεις ορθογώνιους σχεδιασμούς που δώσαμε προηγουμένως. Όλα τα amicable σύνολα των οκτώ κυκλικών πινάκων που παράγουν πλήρεις ορθογώνιους σχεδιασμούς (βλ. Πίνακα 2.3.5), κατασκευάζονται με αυτό το τρόπο. Το matching περιγράφεται από τη σχέση (2.2).

Τροποποιήσαμε έναν αλγόριθμο που δόθηκε στην [139], που χρησιμοποιεί τα γνωστά σύνολα τεσσάρων κυκλικών πινάκων για να κατασκευάσουμε ένα amicable σύνολο από οκτώ πίνακες κατάλληλους για τον σχηματισμό που δίνεται στη σχέση (2.4).

Algorithm 17 EXTENDEDMATCHING ALGORITHM

function EXTENDEDMATCHING(A, B, C, D)

Require: A, B, C, D exist

Step 1 Find four circulants matrices A, B, C, D of order n with variables a, b, c, d satisfying

$$AA^T + BB^T + CC^T + DD^T = (r_1a^2 + r_2b^2 + r_3c^2 + r_4d^2)I_n$$

for some integers r_i.

Step 2 Form four new circulant matrices E, F, G, H from A, B, C, D just by replacing a, b, c, d with e, f, g, h respectively. Obviously the new matrices satisfy the previous conditions but on variables e, f, g, h.

Step 3 Search the set $\{A, B, C, D, E, F, G, H\}$ for a combination suitable to form an amicable set of eight matrices.

Step 4 If we find such a set, we replace the matrices in the array given by (2.4).

end function

Εφαρμόσαμε αυτόν τον αλγόριθμο στους κυκλικούς πίνακες που κατασκευάζονται από τις αντίστοιχες ή ισοδύναμες ακολουθίες με NPAF μηδέν (για παράδειγμα τις αντίθετες ακολουθίες) που δόθηκαν στην προηγούμενη ενότητα και παράγουμε τα αποτελέσματα που δίνονται στον Πίνακα 2.3.5.

Πολυπλοκότητα Ένας υπολογιστικός έλεγχος για ένα amicable σύνολο από $\{A_1, A_2, \ldots, A_n\}$ τετραγωνικούς πραγματικούς πίνακες, απαιτεί να εξετάσουμε $n!$ διακριτές περιπτώσεις. Συνεπώς ο εξαντλητικός έλεγχος για ένα amicable σύνολο οκτώ πινάκων απαιτεί 40320 περιπτώσεις. Είναι γνωστό ότι χρησιμοποιώντας τον τύπο του Stirling, ο ρυθμός αύξησης της παραγοντικής συνάρτησης $n!$ σε όρους εκθετικών συναρτήσεων είναι $\Theta(n^{n+1/2}e^{-n})$, βλ. [30].

Δείχνουμε την εφαρμογή του αλγορίθμου σε ένα γνωστό σύνολο από τέσσερις ακολουθίες με NPAF μηδέν στο ακόλουθο παράδειγμα.

Παράδειγμα 11 Θεωρούμε τις ακολουθίες P, Q, R, S που έχουν NPAF μηδέν, κατασκευαζόμενες από το Θεώρημα 10 και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για να παράγουν έναν $OD(32; 8, 8, 8, 8)$:

$$\begin{array}{rcl} P & = [& a, \quad a, \quad b, \quad -b, \quad c, \quad c, \quad d, \quad -d \ ] \\ Q & = [& a, \quad a, \quad b, \quad -b, \quad -c, \quad -c, \quad -d, \quad d \ ] \\ R & = [& a, \quad -a, \quad b, \quad b, \quad -c, \quad c, \quad -d, \quad -d \ ] \\ S & = [& a, \quad -a, \quad b, \quad b, \quad c, \quad -c, \quad d, \quad d \ ] \end{array}$$

Σχηματίζουμε τους κυκλικούς πίνακες A, B, C, και D που έχουν ως πρώτες γραμμές τις ακολουθίες P, Q, R και S, αντίστοιχα. Αυτοί οι πίνακες ικανοποιούν την ακόλουθη προσθετική ιδιότητα:

$$AA^T + BB^T + CC^T + DD^T = (8 \cdot a^2 + 8 \cdot b^2 + 8 \cdot c^2 + 8 \cdot d^2) I_8$$

Στη συνέχεια, αντικαθιστούμε τις μεταβλητέσε a με e, b με f, c με g και d με h και σχηματίζουμε τις παρακάτω ακολουθίες:

$$\begin{array}{rcl} P' & = [& e, \quad e, \quad f, \quad -f, \quad g, \quad g, \quad h, \quad -h \ ] \\ Q' & = [& e, \quad e, \quad f, \quad -f, \quad -g, \quad -g, \quad -h, \quad h \ ] \\ R' & = [& e, \quad -e, \quad f, \quad f, \quad -g, \quad g, \quad -h, \quad -h \ ] \\ S' & = [& e, \quad -e, \quad f, \quad f, \quad g, \quad -g, \quad h, \quad h \ ] \end{array}$$

Σχηματίζοντας τους κυκλικούς πίνακες E, F, G, και H που έχουν ως πρώτες γραμμές τις ακολουθίες P', Q', R' και S', είναι προφανές ότι αυτοί οι πίνακες ικανοποιούν την προηγούμενη σχέση αλλά πλέον στις μεταβλητές e, f, g, και h:

$$EE^T + FF^T + GG^T + HH^T = (8 \cdot e^2 + 8 \cdot f^2 + 8 \cdot g^2 + 8 \cdot h^2) I_8$$

Μπορεί εύκολα να πιστοποιηθεί με έναν υπολογιστικό έλεγχο ότι η παρακάτω συνθήκη ισχύει:

$$(AE^T - EA^T) + (BF^T - FB^T) + (CG^T - GC^T) + (DH^T - HD^T) = 0$$

Συνεπώς, το ειδικό amicable σύνολο $\{A, E, B, F, C, G, D, H\}$ οκτώ πινάκων μπορεί να χρησιμοποιηθεί στο σχηματισμό Kharaghani για να σχηματίσει έναν $OD(64; 8, 8, 8, 8, 8, 8, 8, 8)$.

§2.3.4 Λογισμικό για Πλήρεις Ορθογώνιους Σχεδιασμούς

Σε αυτήν την ενότητα, δίνουμε το απαραίτητο θεωρητικό υπόβαθρο κατασκευής πινάκων Hadamard από ορθογώνιους σχεδιασμούς και αναπτύσουμε ένα λογισμικό για την εύρεση μη-ισοδύναμων πινάκων Hadamard που κάνει χρήση διαφόρων αυτοματοποιήσεων.

Πίνακες Hadamard από Κυκλικούς Πίνακες Ο σχηματισμός Williamson

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

έχει χρησιμοποιηθεί για την κατασκευή μη-ισοδύναμων πινάκων Hadamard [99]. Συγκεριμένα, έστω U ο πίνακας τάξης n

$$U = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

που έχει την ιδιότητα $U^n = I_n$. Ο πίνακας U χρησιμοποιείται για να ορίσει τους block πίνακες τάξης n στο σχηματισμό Williamson, ως πολυώνυμα του U με συντελεστές ± 1. Τότε οι block πίνακες θα είναι μεταθετικοί. Επιπλέον, θεωρώντας συνθήκες συμμετρίας στους συντελεστές, οι block πίνακες θα είναι επίσης συμμετρικοί, γνωρίζοντας ότι $U^T = U^{-1}$. Οι τέσσερις πίνακες A, B, C, D ορίζονται από τα πολυώνυμα του U ως ακολούθως:

$$\begin{array}{rcccccccc} A & = & a_0 I_n & + & a_1 U & + & \cdots & + & a_{n-1} U^{n-1} \\ B & = & b_0 I_n & + & b_1 U & + & \cdots & + & b_{n-1} U^{n-1} \\ C & = & c_0 I_n & + & c_1 U & + & \cdots & + & c_{n-1} U^{n-1} \\ D & = & d_0 I_n & + & d_1 U & + & \cdots & + & d_{n-1} U^{n-1} \end{array} \quad (2.8)$$

όπου οι $4n$ συντελεστές $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}, c_0, \ldots, c_{n-1}, d_0, \ldots, d_{n-1}$ ικανοποιούν τις επιπλέον συνθήκες συμμετρίας

$$a_{n-i} = a_i, b_{n-i} = b_i, c_{n-i} = c_i, d_{n-i} = d_i, \ i = 1, \ldots, n-1. \qquad (2.9)$$

Τότε η απαίτηση $HH^T = (4n)I_{4n}$ παράγει ένα σύστημα πολυωνυμικών εξισώσεων σε $2n+2$ αγνώστους (θεωρώντας το n να είναι περιττό).

Είναι κατανοητό να χρησιμοποιήσουμε την ίδια διαδικασία με πιο γενικούς σχηματισμούς από τον σχηματισμό Williamson, για παράδειγμα με πλήρεις ορθογώνιους σχεδιασμούς, για να ψάξουμε για μη-ισοδύναμους πίνακες Hadamard.

Έστω m ένα πολλαπλάσιο του 4 και $OD(m; a_1, \ldots, a_k)$ ένας πλήρης ορθογώνιος σχεδιασμός ($a_1 + \cdots + a_k = m$) τάξης m σε k μεταβλητές ($k \leq \rho(m)$ όπου με $\rho(m)$ συμβολίζουμε τη συνάρτηση του Radon [70]). Τότε μπορούμε να αντικαθιστήσουμε κάθε μεταβλητή που εμφανίζεται στον πλήρη ορθογώνιο σχεδιασμό με έναν πίνακα τάξης n που παράγουμε από τον πίνακα U και τον απαραίτητο αριθμό αγνώστων μεταβλητών. Σχεδιάσαμε ένα λογισμικό (που περιγράφεται στην επόμενη ενότητα) για να υλοποιήσουμε αυτήν την ιδέα πιο συστηματικά. Αφού χρησιμοποιήσαμε το λογισμικό μας με διάφορους ορθογώνιους σχεδιασμούς, δίνουμε το παρακάτω κριτήριο που επιτρέπει να κάνουμε χρήση της έννοιας του PAF [143] για να παρέχουμε μια ακριβής περιγραφή του συστήματος των πολυωνυμικών εξισώσεων που προκύπτουν κατά την διαδικασία εύρεσης μη-ισοδύναμων πινάκων Hadamard από ορθογώνιους σχεδιασμούς. Αυτό το κριτήριο μας επιτρέπει να καθορίσουμε πότε συγκεκριμένα block πινάκων είναι κατάλληλα για την κατασκευή ενός πίνακα Hadamard από έναν ορθογώνιο σχεδιασμό, ως ένα σύστημα γραμμικών εξισώσεων.

Ιδιαίτερα, θεωρούμε το n να είναι ένας περιττός ακέραιος τέτοιος ώστε $n \geq 3$ και θέτουμε $p = \frac{n-1}{2}$. Για όλες τις τιμές του i από 1 εώς k, υποθέτουμε ότι κάθεμια από τις a_i μεταβλητές στις γραμμές και στήλες του ορθογώνιου σχεδιασμού αντικαθιστάται από έναν $n \times n$ κυκλικό και συμμετρικό πίνακα με αγνώστους A_i. Όταν τα A_i κατασκευάζονται ως πολυώνυμα μέσω του πίνακα U, τότε μια ακολουθία $p+1$ αγνώστων $A_i^p = [a_i^0, \ldots, a_i^p]$ επαρκεί για την πλήρη περιγραφή των A_i. Ας συμβολίσουμε με O τον παραγόμενο $mn \times mn$ πίνακα. Τότε η σχέση $OO^T = (mn)I_{mn}$ παράγει το ακόλουθο σύστημα από p πολυωνυμικές

εξισώσεις σε $k(p+1)$ δυαδικούς αγνώστους:

$$\begin{array}{ccccc} a_1 PAF_{A_1^p}(1) & +\cdots+ & a_k PAF_{A_k^p}(1) & + & \frac{m}{2} = 0 \\ \vdots & & \vdots & & \vdots \\ a_1 PAF_{A_1^p}(p) & +\cdots+ & a_k PAF_{A_k^p}(p) & + & \frac{m}{2} = 0 \end{array} \qquad (2.10)$$

Επιπρόσθετα, όταν $g = \gcd\left(a_1, \ldots, a_k, \frac{m}{2}\right) > 1$, αυτές οι εξισώσεις μπορούν να απλοποιηθούν διαιρώντας κατά μέλη με g.

Δείχνουμε την εφαρμογή του προηγούμενου κριτηρίου, υποθέτοντας ότι μας δίνεται ο πλήρης ορθογώνιος σχεδιασμός τάξης 16, $OD(16;1,2,2,2,2,2,2,3)$ σε 8 μεταβλητές a, b, c, d, e, f, g, h:

$$\begin{bmatrix} a & b & b & b & c & c & d & d & e & e & f & f & g & g & h & h \\ -b & a & b & -b & c & -c & d & -d & e & -e & f & -f & g & -g & h & -h \\ b & b & -a & -b & -d & -d & c & c & -f & -f & e & e & -h & -h & g & g \\ b-b & b & -a & -d & d & c & -c & -f & f & e & -e & -h & h & g & -g & \\ -c & -c & -d & -d & a & b & b & b & g & g & -h & -h & -e & -e & f & f \\ -c & c & -d & d & -b & a & b & -b & g & -g & -h & h & -e & e & f & -f \\ d & d & -c & -c & b & b & -a & -b & h & h & g & g & -f & -f & -e & -e \\ d & -d & -c & c & b & -b & b & -a & h & -h & g & -g & -f & f & -e & e \\ -e & -e & -f & -f & -g & -g & h & h & a & b & b & b & c & c & -d & -d \\ -e & e & -f & f & -g & g & h & -h & -b & a & b & -b & c & -c & -d & d \\ f & f & -e & -e & -h & -h & -g & -g & b & b & -a & -b & d & d & c & c \\ f & -f & -e & e & -h & h & -g & g & b & -b & b & -a & d & -d & c & -c \\ -g & -g & -h & -h & e & e & -f & -f & -c & -c & d & d & a & b & b & b \\ -g & g & -h & h & e & -e & -f & f & -c & c & d & -d & -b & a & b & -b \\ h & h & -g & -g & f & f & e & e & -d & -d & -c & -c & b & b & -a & -b \\ h & -h & -g & g & f & -f & e & -e & -d & d & -c & c & b & -b & b & -a \end{bmatrix}$$

και αντικαθιστούμε κάθε μεταβλητή με ένα συμμετρικό κυκλικό πίνακα τάξης n. Τότε μπορουμε να παράγουμε το σύστημα των πολυωνυμικών εξισώσεων που προκύπτουν με αποτελεσματικό τρόπο, για πιθανή χρήση σε έναν υπολογιστή.

- $n = 3, m = 16, p = 1$

  $a_0a_1 + 3b_0b_1 + 2c_0c_1 + 2d_0d_1 + 2e_0e_1 + 2f_0f_1 + 2g_0g_1 + 2h_0h_1 + 8 = 0$

  Η παραπάνω εξίσωση έχει 4096 λύσεις, όταν όλες οι μεταβλητές παίρνουν τιμές ± 1. Μια λύση (στη μορφή $[a_0a_1b_0b_1c_0c_1d_0d_1e_0e_1f_0f_1 g_0g_1h_0h_1]$) δίνεται από:

  ```
  [-1, -1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1]
  ```

Αυτές οι λύσεις παράγουν 4096 πίνακες Hadamard τάξεως $16 \cdot 3 = 48$. Στη συνέχεια, αναζητούμε μη-ισοδύναμους πίνακες Hadamard τάξης 48 με το Magma, στο σύνολο των 4096 πινάκων Hadamard.

- $n = 5, m = 16, p = 2$

$$a_0a_2 + a_1a_2 + 3b_0b_2 + 3b_1b_2 + 2c_0c_2 + 2c_1c_2 + 2d_0d_2 + 2d_1d_2 +$$
$$2e_0e_2 + 2e_1e_2 + 2f_0f_2 + 2f_1f_2 + 2g_0g_2 + 2g_1g_2 + 2h_0h_2 + 2h_1h_2 + 8 = 0$$
$$a_0a_1 + a_1a2 + 3b_0b_1 + 3b_1b_2 + 2c_0c_1 + 2c_1c_2 + 2d_0d_1 + 2d_1d_2 +$$
$$2e_0e_1 + 2e_1e_2 + 2f_0f_1 + 2f_1f_2 + 2g_0g_1 + 2g_1g_2 + 2h_0h_1 + 2h_1h_2 + 8 = 0$$

Οι παραπάνω εξισώσεις έχουν 92160 λύσεις, όταν όλες οι μεταβλητές παίρνουν τιμές ± 1. Μια λύση (στη μορφή $[a_0a_1a_2b_0b_1b_2c_0c_1c_2$ $d_0d_1d_2e_0e_1e_2f_0f_1f_2g_0g_1g_2h_0h_1h_2]$) δίνεται από:

```
[-1, -1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1,
 1, -1, -1, 1, 1, -1, 1, -1]
```

Αυτές οι λύσεις παράγουν 92160 πίνακες Hadamard τάξεως $16 \cdot 5 = 80$. Στη συνέχεια, αναζητούμε μη-ισοδύναμους πίνακες Hadamard τάξης 80 με το Magma, στο σύνολο των 92160 πινάκων Hadamard.

- $n = 7, m = 16, p = 3$

$a_0a_2 + a_1a_3 + a_2a_3 + 3b_0b_2 + 3b_1b_3 + 3b_2b_3 + 2c_0c_2 + 2c_1c_3 + 2c_2c_3 +$
$2d_0d_2 + 2d_1d_3 + 2d_2d_3 + 2e_0e_2 + 2e_1e_3 + 2e_2e_3 + 2f_0f_2 + 2f_1f_3 + 2f_2f_3 +$
$2g_0g_2 + 2g_1g_3 + 2g_2g_3 + 2h_0h_2 + 2h_1h_3 + 2h_2h_3 + 8 = 0$

$a_2a_3 + a_0a_1 + a_1a_2 + 3b_2b_3 + 2c_2c_3 + 2d_2d_3 + 2e_2e_3 + 2f_2f_3 + 2g_2g_3 +$
$2h_2h_3 + 3b_0b_1 + 3b_1b_2 + 2c_0c_1 + 2c_1c_2 + 2d_0d_1 + 2d_1d_2 + 2e_0e_1 + 2e_1e_2 +$
$2f_0f_1 + 2f_1f_2 + 2g_0g_1 + 2g_1g_2 + 2h_0h_1 + 2h_1h_2 + 8 = 0$

$a_1a_3 + a_1a_2 + a_0a_3 + 3b_1b_3 + 2c_1c_3 + 2d_1d_3 + 2e_1e_3 + 2f_1f_3 + 2g_1g_3 +$
$2h_1h_3 + 3b_1b_2 + 2c_1c_2 + 2d_1d_2 + 2e_1e_2 + 2f_1f_2 + 2g_1g_2 + 2h_1h_2 + 3b_0b_3 +$
$2c_0c_3 + 2d_0d_3 + 2e_0e_3 + 2f_0f_3 + 2g_0g_3 + 2h_0h_3 + 8 = 0$

Οι παραπάνω εξισώσεις έχουν 1105920 λύσεις, όταν όλες οι μεταβλητές παίρνουν τιμές ± 1. Μια λύση στην (μορφή $[a_0a_1a_2a_3b_0b_1b_2$ $b_3c_0c_1c_2c_3d_0d_1d_2d_3e_0e_1e_2e_3f_0f_1f_2f_3g_0g_1g_2g_3h_0h_1h_2h_3]$) δίνεται από:

```
[-1, -1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1,
 -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1]
```

Αυτές οι λύσεις παράγουν 1105920 πίνακες Hadamard τάξεως $16 \cdot 7 = 112$. Στη συνέχεια, αναζητούμε μη-ισοδύναμους πίνακες Hadamard τάξης 112 με το Magma, στο σύνολο των 1105920 πινάκων Hadamard.

Ανάπτυξη του Λογισμικού Το metaprogramming δεν είναι καινούργια έννοια, και έχει χρησιμοποιηθεί με επιτυχία στις περιπτώσεις όπου χρειάστηκε η επαναχρησιμοποίηση ενός λογισμικού, δηλαδή η διαδικασία ανάπτυξης λογισμικού από ύπάρχουσα συστήματα λογισμικού πάρα η δημιουργία τους από μηδενική βάση [167]. Παραθέτουμε ορισμένες βασικές χρήσεις του metaprogramming:

- Παραγωγή (Generation) - μετακώδικας που παράγει κώδικα
- Μεταλλαγή (Transformation) - μετακώδικας που τροποποιέι κώδικα (παρόμοια με την παραγωγή)
- Μετάφραση (Translation) - μεταλλαγή σε άλλη γλώσσα (προγραμματισμού)
- Ανάλυση (Analysis) - μετακώδικας που αναλύει (υπάρχον) κώδικα

Το μεταλογισμικό που αναπτύξαμε για ορθογώνιους σχεδιασμούς για την εύρεση μη-ισοδύναμων πινάκων Hadamard κάνει αποτελεσματική χρησή όλων των προηγούμενων μεθόδων του metaprogramming. Ιδιαίτερα, το metaprogram χρησιμοποιεί το BASH SHELL ως metalanguage ενώ η object-language του κάθε προγράμματος είναι τα πακέτα Υπολογιστικής Άλγεβρας, MAPLE και MAGMA. Το MAPLE παρέχει έναν άριστο τρόπο εκτέλεσης συμβολικών και αριθμητικών υπολογισμών, ιδιαίτερα όταν έχουμε να υλοποιήσουμε μέθοδους που βασίζονται στα Διακριτά Μαθηματικά. Υλοποιήσαμε ένα πακέτο MAPLE το οποίο περιέχει όλες τις απαραίτητες κατασκευές για την παραγωγή των πινάκων Hadamard από ορθογώνιους σχεδιασμούς στο MAPLE, έτσι ώστε να πετύχουμε τη μέγιστη δυνατή φορησιμότητα με άλλα πακέτα Υπολογιστικής Άλγεβρας, όπως είναι το MAGMA. Στη συνέχεια, χρησιμοποιήσαμε το MAGMA για να αυτοματοποιήσουμε την εύρεση μη-ισοδύναμων πινάκων Hadamard. Προηγούμενες προσπάθειες υλοποίησης λογισμικών ικανών για την εύρεση μη-ισοδύναμων πινάκων Hadamard μπορούν να βρεθούν στις [57], [133], [134], [136], [140] και [142]. Μια πρόσφατη εφαρμογή του παρόντος μεταλογισμικού μπορεί να βρεθεί στην [156]. Το μεταλογισμικό που δίνεται παρακάτω, μπορεί να θεωρηθεί ως η ενοποίηση και περαιτέρω επέκταση των προηγουμένων (λογισμικών), το οποίο και οδήγησε στην παραγωγή μεγάλων βάσεων δεδομένων από νέους μη-ισοδύναμους πίνακες Hadamard. Οι λεπτομέρειες του μεταλογισμικού αυτής της ενότητας παρουσιάζονται στον Αλγόριθμο 18.

Υλοποιήσαμε ένα meta-metaprogram το οποίο δέχεται ως είσοδο ένα αρχείο με έναν ορθογώνιο σχεδιασμό σε ASCII και παράγει ένα αρ-

χειο Maple, το οποίο παράγει κώδικα σε C, ο οποίος μπορεί να μεταγλωτιστεί και να εκτελεστεί για να λύσει εξαντλητικά τα συστήματα εξισώσεων που αντιστοιχούν σε αυτόν τον ορθογώνιο σχεδιασμό. Το meta-metaprogram χρησιμοποιεί το bash shell, και το `CodeGeneration` πακέτο του Maple. Ορισμένες από τις κύριες δυσκολίες που αντιμετωπίσαμε κατά την ανάπτυξη αυτού του λογισμικού βρίσκονται στην δυναμική παραγωγή των τιμών των μεταβλητών που αντιπροσωπεύουν τις ιδιότητες του ορθγώνιου σχεδιασμού στο αρχείο εισόδου. Για παράδειγμα, ο αριθμός των μεταβλητών και η λίστα των διαφορετικών μεταβλητών. Δίνουμε παρακάτω σε ψευδοκώδικα το meta-metaprogram που χρησιμοποιήσαμε.

Ιδιαίτρα, το σύστημα των εξισώσεων που προκύπτουν κατά την εύρεση μη-ισοδύναμων πινάκων Hadamard από πλήρεις ορθογώνιους σχεδιασμούς χρησιμοποιώντας κυκλικούς και συμμετρικούς block πίνακες, μπορεί να λύθει κάνοντας χρήση υπερυπολογιστών. Χρησιμοποιήσαμε το Maple για να αυτοματοποιήσουμε την παραγωγή των προγραμμάτων σε C, τα οποία στη συνέχεια παραλληλοποιήσαμε με ένα bash/sed/awk πρόγραμμα. Η χρήση του metaprogramming με τις δυνατότητες του Maple για αυτόματη παραγωγή κώδικα, διασφαλίζει την αποτελεσματική και σωστή προτυποποίηση του κώδικα. Στη συνέχεια, το λογισμικό κάνει χρήση του Magma για να κατασκευάσει τον πίνακα Hadamard που αντιστοιχεί σε κάθε λύση και μετέπειτα χρησιμοποιεί τον αλγόριθμο που δόθηκε στην [132], για να εντοπίσει μη-ισοδύναμους πίνακες Hadamard.

§2.3.5 Νέοι Μη-Ισοδύναμοι Πίνακες Hadamard από Ορθογώνιους Σχεδιασμούς

Αναζητήσαμε μη-ισοδύναμους πίνακες Hadamard χρησιμοποιώντας το μεταλογισμικό που αναπτύξαμε προηγουμένως και το 4-profile κριτήριο όπως αυτό είναι υλοποιημένο στο Magma [15], με τους 25 πλήρεις ορθογώνιους σχεδιασμούς που απαριθμούνται παρακάτω. Οι πλήρεις ορθογώνιοι σχεδιασμοί κατασκευάστηκαν μέσω των θεωρημάτων 10 και 11 χρησιμοποιώντας ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης από την [153] και ακολουθίες Golay, και μέσω του Αλγορίθμου 17.

Algorithm 18 HMOD ALGORITHM

procedure HMOD(OD, n) ▷ n is the size of block matrices
Require: n odd
Ensure: Generation of binary vectors corresponding to Hadamard matrices
validate that given OD is an orthogonal design
do awk to detect the order and the variables of the OD
assign variable names to the variables of the OD
calculate the order of Hadamard matrices
assign a list to the k variables of the OD
set p equal to $(n-1)/2$
transform in Maple format given inputs
create Maple input file from OD and the variables of the OD ▷ Begin Maple phase
  begin for loop from 1 to k
    create the sequence of $p+1$ indeterminates
    replace the OD variables with symmetric circulant matrices
  end for loop
  begin for loop from 1 to p
    compute PAF equations from relation (2.10)
  end for loop
do sed to create a Maple file containing the polynomial equations
call procedure `Maple2C` to convert the equations in C format ▷ End Maple phase
compile the C file ▷ Begin C phase
execute the C executable ▷ End C phase
do sed/awk to convert the output into solutions in Magma format
return solutions as binary vectors representing the Hadamard matrices
end procedure

procedure MAPLE2C(PolEqs) ▷ PolEqs are the polynomial equations in Maple format
Require: Polynomial equations in Maple format
Ensure: Conversion to C format
call `CodeGeneration` Maple package
declare types of variables in C and procedures to be converted
execute C conversion of polynomial equations
return the polynomial equations in C format
end procedure

Α/Α	Σχεδιασμός	Κατασκευή
1	$\mathrm{OD}(20;2,2,8,8)$	Θεώρημα 10
2	$\mathrm{OD}(24;8,8,8)$	Θεώρημα 11
3	$\mathrm{OD}(24;4,4,8,8)$	Θεώρημα 10
4	$\mathrm{OD}(32;8,8,8,8)$	Θεώρημα 10
5	$\mathrm{OD}(32;8,8,16)$	Θεώρημα 11
6	$\mathrm{OD}(40;2,2,2,2,8,8,8,8)$	Αλγόριθμος 17
7	$\mathrm{OD}(40;4,4,16,16)$	Θεώρημα 10
8	$\mathrm{OD}(48;4,4,4,4,8,8,8,8)$	Αλγόριθμος 17
9	$\mathrm{OD}(48;8,8,8,8,8,8)$	Αλγόριθμος 17
10	$\mathrm{OD}(48;8,8,16,16)$	Θεώρημα 10
11	$\mathrm{OD}(48;16,16,16)$	Θεώρημα 11
12	$\mathrm{OD}(56;8,8,8,32)$	Θεώρημα 10
13	$\mathrm{OD}(56;8,8,20,20)$	Θεώρημα 10
14	$\mathrm{OD}(56;8,8,40)$	Θεώρημα 11
15	$\mathrm{OD}(64;8,8,8,8,8,8,8,8)$	Αλγόριθμος 17
16	$\mathrm{OD}(64;8,8,8,8,16,16)$	Αλγόριθμος 17
17	$\mathrm{OD}(64;16,16,16,16)$	Θεώρημα 10
18	$\mathrm{OD}(72;16,16,20,20)$	Θεώρημα 10
19	$\mathrm{OD}(80;4,4,4,4,16,16,16,16)$	Αλγόριθμος 17
20	$\mathrm{OD}(96;8,8,8,8,16,16,16,16)$	Αλγόριθμος 17
21	$\mathrm{OD}(96;16,16,16,16,16,16)$	Αλγόριθμος 17
22	$\mathrm{OD}(112;8,8,8,8,40,40)$	Αλγόριθμος 17
23	$\mathrm{OD}(112;8,8,8,8,20,20,20,20)$	Αλγόριθμος 17
24	$\mathrm{OD}(128;16,16,16,16,16,16,16,16)$	Αλγόριθμος 17
25	$\mathrm{OD}(144;16,16,16,16,20,20,20,20)$	Αλγόριθμος 17

Πίνακας 2.5: Πλήρεις ορθογώνιοι σχεδιασμοί μεγάλων τάξεων

Οι υπολογισμοί πραγματοποιήθηκαν με το MAGMA V 2.13. Με N_n στους ακόλουθους πίνακες συμβολίζουμε τον αριθμό των μη-ισοδύναμων πινάκων Hadamard που βρήκαμε.

n	96	120	144	160	192	200
N_n	4	64	160	8	121	360

Πίνακας 2.6: Νέοι μη-ισοδύναμοι πίνακες Hadamard τάξεων n, $96 \leq n \leq 200$

n	224	240	288	320	336	384	432	448
N_n	20	2816	80	176	128	240	128	40

Πίνακας 2.7: Νέοι μη-ισοδύναμοι πίνακες Hadamard τάξεων n, $224 \leq n \leq 448$

Παρατήρηση 6 *Σημειώνουμε ότι, οι πίνακες Hadamard που παρουσιάζονται στους Πίνακες της Ενότητας 2.3.5, που κατασκευάστηκαν μέσω ορθογώνιων σχεδιασμών, είναι μη-ισοδύναμοι κάθως για κάθε τάξη (πινάκων) βρήκαμε ότι τα αντίστοιχα 4-profiles είναι διαφορετικά.*

Επιπλέον, κάποιος θα μπορούσε να ελέγξει τους πίνακες Hadamard για ισοδυναμία, χρησιμοποιώντας το graph isomorphism κριτήριο, το οποίο είναι πολύ πιο χρονοβόρο υπολογιστικά [15, 183].

Logic merely
sanctions the conquests
of the intuition.

Jacques Hadamard
(1865-1963)

3

Πίνακες Στάθμισης και Ορθογώνιοι Σχεδιασμοί

Στο τέταρτο αυτό κεφάλαιο, παρουσιάζονται νέες άπειρες οικογένειες ορθογώνιων σχεδιασμών σε τρείς και τέσσερις μεταβλητές που παράγονται μέσω συμπληρωματικών ακολουθιών. Ένα συνολο ακολουθιών θα καλείται συμπληρωματικό (complementary), αν το άθροισμα της συνάρτησης αυτοσυσχέτισης του είναι μηδέν. Επιπλέον, γίνεται χρήση κατευθυνόμενων ακολουθιών (directed sequences) για την κατασκευή νέων ορθογώνιων σχεδιασμών. Οι κατασκευές αυτές, πραγματοποιούνται πολλαπλασιάζοντας το μήκος και τον τύπο κατάλληλων συμβατών ακολουθιών. Ιδιαίτερα, αποδεικνύεται ότι σχεδόν-κανονικές ακολουθίες μήκους $n = 4m + 1$ *μπορούν να χρησιμοποιηθούν για την κατασκευή τεσσάρων κατευθυνόμενων ακολουθιών με μήκη* $2m + 1$, $2m + 1$, $2m$, $2m$ *τύπου* $(4m + 1, 4m + 1) = (n, n)$ *που έχουν NPAF μηδέν. Αυτές οι μέθοδοι οδηγούν στην κατασκευή πολλών νέων κλάσεων ορθογώνιων σχεδιασμών. Επιπρόσθετα, παράγουμε νέες άπειρες οικογένειες πινάκων στάθμισης από συμπληρωματικές ακολουθίες, όπως είναι για παράδειγμα οι* $W(156 + 4k, 125)$, $W(144 + 4k, 144)$, $W(160 + 4k, 144)$, $W(200 + 4k, 196)$, $W(224 + 4k, 196)$ *και* $W(276 + 4k, 225)$ *για κάθε* $k \geq 0$. *Αυτές οι οικογένειες δίνουν πάνω από 35 νέους πίνακες στάθμισης που η ύπαρξη τους ήταν καταχωρημένη ως άγνωστη στη δεύτερη έκδοση του Εγχειριδίου Συνδυαστικών Σχεδιασμών (*Handbook of Combinatorial Designs*).*

Στο δεύτερο μέρος του κεφαλαίου, κατασκευάζονται άπειρες οικογένειες ορθογώνιων σχεδιασμών μέσω πινάκων στάθμισης τάξεως $2n$, *βάρους* $2n-k$ *και διάδοσης ή εξάπλωσης (spread)* σ, *και συμπληρωματικών ακολουθιών με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης. Επιπλέον, εισάγεται ένα νέο κριτήριο για τριαδικά συμπληρωματικά ζεύγη ακολουθιών (ternary complementary pairs), η ζ-αποδοτικότητα (ζ-*

efficiency), και μελετώνται διάφορες ιδιότητες της. Στη συνέχεια, με την εφαρμοφή της ζ-αποδικότητας αποδεικνύεται ένα νέο πολλαπλασιαστικό θεώρημα για ακολουθίες με μηδενική περιοδική αυτοσυσχέτιση και εξετάζονται οι συνέπειες του στη Θεωρία Σχεδιασμών.

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στις επιστημονικές εργασίες [157, 158] και [159].

§3.1 Απεικονίσεις για Ορθογώνιους Σχεδιασμούς

Για τις απαραίτητες έννοιες από τη Θεωρία Πινάκων Στάθμισης και Ορθογώνιων Σχεδιασμών που θα χρησιμοποιήσουμε σε αυτό το κεφάλαιο, παραπέμπουμε στις Ενότητες 1.1.1 και 2.3.1 της διατριβής, αντίστοιχα. Οι πίνακες στάθμισης και οι ορθογώνιοι σχεδιασμοί έχουν πολλές εφαρμογές στη Συνδυαστική, τη Στατιστική, τη Θεωρία Κωδίκων και στις τηλεπικοινωνίες, καθώς και σε δίαφορες άλλες συγγενείς περιοχές. Για περαιτέρω λεπτομέρειες, σε πίνακες στάθμισης, ορθογώνιους σχεδιασμούς και εφαρμογές αυτών, παραπέμπουμε αντίστοιχα στις [33, 152, 153] και [70, 206, 208].

Για τα αποτελέσματα αυτού του κεφαλαίου υιοθετούμε και τροποποιούμε κατάλληλα τους ακόλουθους ορισμούς από τις [70, 143].

Ορισμός 17 *Το βάρος μιας ακολουθίας A, είναι ο αριθμός των μη-μηδενικών στοιχείων της A. Μια οικογένεια από m ακολουθίες $A_1, A_2, \ldots, A_m$ μήκους n και στοιχεία $\{0, \pm 1\}$ θα καλούνται m-συμπληρωματικές ακολουθίες (m-complementary sequences), εν συντομία CS, βάρους w, και θα συμβολίζονται με $m - \mathrm{CS}(n, w)$ αν $\mathrm{N}_{A_1}(s) + \mathrm{N}_{A_2}(s) + \ldots + \mathrm{N}_{A_m}(s) = 0$, για $s = 1, \ldots, n-1$. Αυτές οι ακολουθίες θα λεμε ότι έχουν NPAF μηδέν.*

Ορισμός 18 *Μια οικογένεια από m ακολουθίες μήκους n στις μεταθετικές μεταβλητές $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ με NPAF μηδέν όπου οι $\pm x_i$ εμφανίζονται s_i φορές, καλούνται $m - \mathrm{NPAF}(n; s_1, s_2, \ldots, s_k)$ ακολουθίες τύπου $(s_1, s_2, \ldots, s_k)$.*

Παρατήρηση 7 *Μια οικογένεια από $2 - \mathrm{CS}(n, 2n)$ είναι ακολουθίες Golay, εν συντομία GS, μήκους n που συμβολίζονται με $\mathrm{GS}(n)$.*

Είναι γνωστές οι ακόλουθες απεικονίσεις (maps) ή κατασκευές για συμπληρωματικές ακολουθίες (CS) και ορθογώνιους σχεδιασμούς:

$$2 - \mathrm{CS}(n, w) \to W(2n, w) \tag{3.1}$$

$$2 - \mathrm{NPAF}(n; u, v) \to \mathrm{OD}(2n; u, v) \tag{3.2}$$

$$4 - \mathrm{CS}(n, w) \to W(4n, w) \tag{3.3}$$

$$4 - \mathrm{NPAF}(n; s_1, s_2, \ldots, s_k) \to \mathrm{OD}(4n; s_1, s_2, \ldots, s_k) \quad (3.4)$$

$$m - \mathrm{NPAF}(n; s_1, s_2, \ldots, s_k) \to m - \mathrm{CS}(n, \sum_{i=1}^{k} s_i) \quad (3.5)$$

$$m - \mathrm{CS}(n, w) \to m - \mathrm{CS}(n + s, w), \ \forall\ s \in \mathbb{N} \quad (3.6)$$

$$m - \mathrm{NPAF}(n; s_1, s_2, \ldots, s_k) \to m - \mathrm{NPAF}(n + s; s_1, s_2, \ldots, s_k), \ \forall\ s \in \mathbb{N} \quad (3.7)$$

$$\mathrm{GS}(g) \to 2 - \mathrm{NPAF}(g; 2g) \quad (3.8)$$

$$\mathrm{GS}(g) \to 2 - \mathrm{NPAF}(2g; 2g, 2g) \quad (3.9)$$

$$\mathrm{GS}(g_1) \times \mathrm{GS}(g_2) \to \mathrm{GS}(g_1 g_2) \quad (3.10)$$

Για τις κατασκευές (3.1) και (3.2) χρησιμοποιούμε τις δύο ακολουθίες στην κατασκευή με δύο κυκλικούς πίνακες (the two circulant construction) των [153] και [70]. Για τις κατασκευές (3.3) και (3.4) χρησιμοποιούμε τις τέσσερις ακολουθίες ως τις πρώτες γραμμές των κυκλικών πινάκων για να παράγουμε το σχηματισμό Goethals-Seidel (βλ. Geramita και Seberry [70, σελ. 107]). Για τις κατασκευές (3.6) και (3.7), παραθέτουμε στο τέλος των ακολουθιών s μηδενικά για να παράγουμε μεγαλύτερες ακολουθίες με NPAF μηδέν, ενώ για την κατασκευή (3.5) αντικαθιστούμε τις μεταθετικές μεταβλητές με ± 1. Πολλαπλασιάζουμε τις GS με τη μεταθετική μεταβλητή α για να παράγουμε την κατασκευή (3.8). Στην κατασκευή (3.9) υποθέτουμε ότι οι δύο $\mathrm{GS}(g)$ είναι οι G και H και συμβολίζουμε με $G^\star$ και $H^\star$ τις αντίστροφες ακολουθίες των G και H αντίστοιχα (όπου $A^\star = [a_n, \cdots, a_2, a_1]$ είναι n αντίστροφη ακολουθία της $A = [a_1, a_2, \cdots, a_n]$). Ο συμβολισμός $|$ απεικονίζει την παράθεση των ακολουθιών. Έστω x και y να είναι μεταθετικές μεταβλητές. Τότε οι ακολουθίες $P' = [Gx \mid Hy]$ και $Q' = [H^\star x \mid -G^\star y]$ είναι $2-\mathrm{NPAF}(2g; 2g, 2g)$. Οι ακολουθίες Golay είναι γνωστές για μήκη $n = 2$ και 10 ([71]), και για μήκος 26 ([72]). Η σύνθετη κατασκευή (3.10) οφείλεται στον Turyn [229]. Συνεπώς, οι $\mathrm{GS}(n)$ υπάρχουν για $n = 2^a \cdot 10^b \cdot 26^c$ όπου a, b, c μη-αρνητικοί ακέραιοι.

Ερευνητικό Πρόβλημα 3 *Η κατασκευή νέων πινάκων στάθμισης και ορθογώνιων σχεδιασμών, καθώς και η ανάπτυξη πολλαπλασιαστικών μεθόδων για συμπληρωματικές ακολουθίες με μηδενική συνάρτηση αυτοσυσχέτισης.*

§3.2 Ορθογώνιοι Σχεδιασμοί από Συμπληρωματικές Ακολουθίες

Σε αυτήν την ενότητα, δίνουμε ορισμένες κατασκευές νέων άπειρων οικογενειών ορθογώνιων σχεδιασμών από συμπληρωματικές ακολουθίες. Για περαιτέρω λεπτομέρειες που αφορούν συμπληρωματικές ακολουθίες παραπέμπουμε στην [143]. Σημειώνουμε ότι, για κάθε μέθοδο κατασκευής που ακολουθεί, υποθέτοντας ότι υπάρχουν συμπληρωματικές ακολουθίες χωρίς μηδενικά, η ειδική περίπτωση $s = 0$ παράγει πλήρεις ορθογώνιους σχεδιασμούς.

§3.2.1 Ορθογώνιοι Σχεδιασμοί από NPAF ακολουθίες

Θεώρημα 12 *Υποθέτουμε ότι υπάρχουν* $2-\mathrm{NPAF}(n;u,v)$ *και* $\mathrm{GS}(g)$. *Τότε υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για CS και ορθογώνιους σχεδιασμούς:*

(i) $2-\mathrm{NPAF}(n;u,v)\times\mathrm{GS}(g)\to 4-\mathrm{NPAF}(n+2g+s;2u,2v,4g,4g)\ \forall\, s\in\mathbb{N}$.

(ii) $2-\mathrm{NPAF}(n;u,v)\times\mathrm{GS}(g)\to \mathrm{OD}(4\cdot(n+2g+s);2u,2v,4g,4g)\ \forall\, s\in\mathbb{N}$.

Απόδειξη.

(i) Έστω $A=[a_1,\cdots,a_n]$ και $B=[b_1,\cdots,b_n]$ όπου $a_k,b_k\in\{0,\pm\alpha,\pm\beta\}$, $k=1,\ldots,n$, να είναι $2-\mathrm{NPAF}(n;u,v)\to\mathrm{OD}(2n;u,v)$ (εφαρμόζουμε την κατασκευή (3.2)).

Στη συνέχεια υποθέτουμε ότι οι δύο ακολουθίες $\mathrm{GS}(g)$ είναι οι G και H. Εφαρμόζοντας την απεικόνιση (3.9), οι $P'=[Gx\mid Hy]$ και $Q'=[H^{\star}x\mid -G^{\star}y]$ είναι $2-\mathrm{NPAF}(2g;2g,2g)$.

Αυτά τα δύο ζεύγη ακολουθιών διπλασίαζονται και σχηματίζουμε τις ακόλουθες τέσσερις ακολουθίες,

$$\begin{array}{llllll} P = [& a_1, & \cdots, & a_n \mid & Gx \mid & Hy \quad] \\ Q = [& a_1, & \cdots, & a_n \mid & -Gx \mid & -Hy \quad] \\ R = [& b_1, & \cdots, & b_n \mid & H^\star x \mid & -G^\star y \quad] \\ S = [& b_1, & \cdots, & b_n \mid & -H^\star x \mid & G^\star y \quad] \end{array} \qquad (3.11)$$

Οι ακολουθίες P, Q, R, S έχουν NPAF μηδέν με έναν ευθύ υπολογισμό της συνάρτησης αυτοσυσχέτισης τους και συνεπως είναι μια οικογένεια από $4-\text{NPAF}(n+2g; 2u, 2v, 4g, 4g)$ ακολουθίες. Στη συνέχεια, εφαρμόζουμε την απεικόνιση (3.7) στις P, Q, R, S για να παράγουμε μια άπειρη οικογένεια από $4-\text{NPAF}(n+2g+s; 2u, 2v, 4g, 4g)\ \forall\ s \in \mathbb{IN}$.

(ii) Εφαρμόζουμε την κατασκευή (3.4) στα αποτελέσματα του (i) ερωτήματος.

□

Σημειώνουμε ότι, η περίπτωση του Θεωρήματος 12, η οποία παράγει πλήρεις ορθογώνιους σχεδιασμούς, μελετήθηκε στην [156]. Η εφαρμογή του Θεωρήματος 12 περιγράφεται από το ακόλουθο παράδειγμα.

Παράδειγμα 12 Θεώρουμε τις $2-\text{NPAF}(3;1,4)$ ακολουθίες από την [153]:

```
A = [a,  b, -a]
B = [a,  0,  a]
```

Από την κατασκευή (3.9) υπάρχουν $GS(2) \to 2-\text{NPAF}(4;4,4)$, ως ακολούθως:

$$P' = [x, x, y, -y] \quad \text{and} \quad Q' = [-x, x, -y, -y].$$

Τότε από το Θεώρημα 12 οι ακολουθίες P, Q, R, S είναι $2-\text{NPAF}(3;1,4) \times GS(2) \to 4-\text{NPAF}(7;2,8,8,8)$:

$$\begin{array}{llllllll} P & = [& a, & b, & -a, & x, & x, & y, & -y \quad] \\ Q & = [& a, & b, & -a, & -x, & -x, & -y, & y \quad] \\ R & = [& a, & 0, & a, & -x, & x, & -y, & -y \quad] \\ S & = [& a, & 0, & a, & x, & -x, & y, & y \quad] \end{array}$$

Εφαρμόζοντας τις απεικονίσεις (3.7) και (3.4) παίρνουμε:
$4-\text{NPAF}(7;2,8,8,8) \to 4-\text{NPAF}(7+s;2,8,8,8) \to \text{OD}(28+4s;2,8,8,8)\ \forall\ s \in \mathbb{IN}$.

§3.2.2 Ορθογώνιοι Σχεδιασμοί από Κατευθυνόμενες Ακολουθίες

Το Θεώρημα 12, έχει ορισμένες συνέπειες που αφορούν κατευθυνόμενες ακολουθίες (directed sequences), εν συντομία DS. Θα λέμε ότι κάποιες ακολουθίες μεταβλητών είναι *κατευθυνόμενες* αν οι ακολουθίες έχουν μηδενική συνάρτηση αυτοσυσχέτισης ανεξάρτητα από τις ιδιότητες των μεταβλητών, όπως είναι η μεταθετικότητα, για να διασφαλίσουν NPAF μηδέν. Προφανώς, δύο κατευθυνόμενες ακολουθίες είναι $2-\mathrm{NPAF}(n;u,u)$ ακολουθίες και θα συμβολίζονται με $\mathrm{DS}(n;u,u)$. Οι κατευθυνόμενες ακολουθίες εισήχθησαν στην [153] και έχουν χρησιμοποιηθεί εκτεταμένα στην κατασκευή ορθογώνιων σχεδιασμών. Επιπλέον, ορθογώνιοι σχεδιασμοί που κατασκευάζονται μέσω κατευθυνόμενων ακολουθιών θα καλούνται κατευθυνόμενοι ορθογώνιοι σχεδιασμοί (directed orthogonal designs).

Για παράδειγμα, οι $[a,b]$ και $[a,-b]$ είναι δύο κατευθυνόμενες ακολουθίες ενώ οι $[a,b]$ και $[b,-a]$ δεν είναι κατευθυνόμενες. Επίσης, οι $[a,b]$, $[a,-b]$,$[c,d]$ και $[c,-d]$ είναι τέσσερις κατευθυνόμενες ακολουθίες ενώ οι $[a,b]$, $[b,-a]$,$[c,d]$ και $[c,-d]$ δεν είναι κατευθυνόμενες.

Πόρισμα 7 *Υποθέτουμε ότι υπάρχουν* $\mathrm{DS}(m;n,n)$ *και* $\mathrm{GS}(g)$. *Τότε υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για DS και ορθογώνιους σχεδιασμούς:*

(i) $\mathrm{DS}(m;n,n)\times\mathrm{GS}(g)\rightarrow 4-\mathrm{NPAF}(m+2g+s;2n,2n,4g,4g)\ \forall\ s\in\mathbb{N}$.

(ii) $\mathrm{DS}(m;n,n)\times\mathrm{GS}(g)\rightarrow \mathrm{OD}(4\cdot(m+2g+s);2n,2n,4g,4g)\ \forall\ s\in\mathbb{N}$.

Απόδειξη.

(i) Οι $\mathrm{DS}(m;n,n)$ είναι $2-\mathrm{NPAF}(m;n,n)$ ακολουθίες και από το Θεώρημα 12 παίρνουμε την ακόλουθη απεικόνιση: $2-\mathrm{NPAF}(m;n,n)\times \mathrm{GS}(g)\rightarrow 4-\mathrm{NPAF}(m+2g+s;2n,2n,4g,4g)\ \forall\ s\in\mathbb{N}$. Επιπλέον, πρέπει να αποδείξουμε ότι οι $4-\mathrm{NPAF}(m+2g+s;2n,2n,4g,4g)$ ακολουθίες είναι κατευθυνόμενες. Καθώς οι αρχικές ακολουθίες είναι κατευθυνόμενες έχουμε ότι στην κατασκευή του Θεωρήματος 12 οι όροι που προκύπτουν στο NPAF της P από την P' θα διαγραφούν στο NPAF της Q από την $-P'$ χωρίς να εξαρτώνται από τη μεταθετικότητα των μεταβλητών. Το ίδιο ισχύει για την Q' στις

ακολουθίες R και S. Συνεπώς, οι ακολουθίες P, Q, R, S με NPAF μηδέν, είναι κατευθυνόμενες.

(ii) Εφαρμόζουμε την κατασκευή (3.4) στα αποτελέσματα του (i) ερωτήματος.

□

Παρατήρηση 8 *Το αντίστροφο του Πορίσματος 7 (το οποίο μπορεί να θεωρηθεί ειδική περίπτωση του Θεωρήματος 12) δεν είναι αληθές. Στο Παράδειγμα 12 οι ακολουθίες* P, Q, R, S *με NPAF μηδέν, δεν είναι κατευθυνόμενες (*$P_P(1)+P_Q(1)+P_R(1)+P_S(1) = 2(ab-ba) = 0$ *αν και μόνον αν οι* a *και* b *είναι μεταθετικές μεταβλητές). Αυτό συμβαίνει διότι οι ακολουθίες* $A = [a, b, -a]$ *και* $B = [a, 0, a]$ *με NPAF μηδέν, δεν είναι κατευθυνόμενες (*$N_A(1) + N_B(1) = ab - ba = 0$ *αν και μόνον αν οι* a *και* b *είναι μεταθετικές μεταβλητές).*

Το βασικό πλεονέκτημα των κατευθυνόμενων ακολουθιών, είναι η πολλαπλασιαστική τους ιδιότητα. Δηλαδή ότι οι μεταβλητές τους μπορούν να αντικατασταθούν από ακολουθίες με NPAF μηδέν για να παράγουν μεγαλύτερες ακολουθίες διαφορετικού τύπου με NPAF μηδέν, κατάλληλες για την κατασκευή μεγάλων ορθογώνιων σχεδιασμών. Αυτή ακριβώς η ιδιότητα, περιγράφεται στο ακόλουθο παράδειγμα.

Παράδειγμα 13 Υπάρχουν $2 - \mathrm{NPAF}(4; 4, 4)$ και $\mathrm{GS}(2)$ ακολουθίες. Τότε από το Θεώρημα 12, υπάρχουν $2 - \mathrm{NPAF}(4; 4, 4) \times \mathrm{GS}(2) \rightarrow 4 - \mathrm{NPAF}(8; 8, 8, 8, 8)$ ακολουθίες:

$$\begin{array}{rl} P & = [\ a,\ a,\ b,\ -b,\ c,\ c,\ d,\ -d\ ] \\ Q & = [\ a,\ a,\ b,\ -b,\ -c,\ -c,\ -d,\ d\ ] \\ R & = [\ a,\ -a,\ b,\ b,\ -c,\ c,\ -d,\ -d\ ] \\ S & = [\ a,\ -a,\ b,\ b,\ c,\ -c,\ d,\ d\ ] \end{array}$$

Οι ακολουθίες A και B είναι $\mathrm{DS}(4; 4, 4)$:

$$A = [a, a, b, -b] \quad \text{και} \quad B = [a, -a, b, b].$$

Επομένως, μπορούμε να αντικαθιστήσουμε τις μεταβλητές των ακολουθιών A και B με τις ακόλουθες $2-\mathrm{NPAF}(2; 2, 2)$ ακολουθίες F και G από την [153] για να παράγουμε μεγαλύτερες ακολουθίες με NPAF μηδέν.

$$F = [e, f] \quad \text{και} \quad G = [e, -f].$$

Παράδειγμα 14 (Συνέχεια του Παραδείγματος 13) Ιδιαίτερα, αντικαθιστώντας τις μεταβλητές a, b στις ακολουθίες A, B με τις ακολουθίες F, G αντίστοιχα παράγουμε την απεικόνιση $DS(4;4,4) \times 2 - NPAF(2;2,2) \to DS(8;8,8)$:

$$A' = [e, f, e, f, e, -f, -e, f] \quad \text{και} \quad B' = [e, f, -e, -f, e, -f, e, -f].$$

Οι ακολουθίες A',B', τότε εφαρμόζονται στις ακολουθίες P, Q, R, S για να παράγουν μια νέα οικογένεια από $4-NPAF(12;8,8,16,16)$ ακολουθίες P', Q', R', S':

$$\begin{array}{lcccccccccccc} P' & = [& e, & f, & e, & f, & e, & -f, & -e, & f, & c, & c, & d, & -d &] \\ Q' & = [& e, & f, & e, & f, & e, & -f, & -e, & f, & -c, & -c, & -d, & d &] \\ R' & = [& e, & f, & -e, & -f, & e, & -f, & e, & -f, & -c, & c, & -d, & -d &] \\ S' & = [& e, & f, & -e, & -f, & e, & -f, & e, & -f, & c, & -c, & d, & d &] \end{array}$$

και εφαρμόζοντας τις κατασκευές (3.7) και (3.4) παίρνουμε:
$4 - NPAF(12;8,8,16,16) \to 4 - NPAF(12+s;8,8,16,16) \to OD(48+4s;8,8,16,16)\ \forall\ s \in \mathbb{IN}$.

Πόρισμα 8 *Υποθέτουμε ότι υπάρχουν* $DS(m;n,n)$, $GS(g)$ *και* $2 - NPAF(k;u,v)$ *ακολουθίες. Τότε υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για DS και ορθογώνιους σχεδιασμούς:*

(i) $DS(m;n,n) \times 2 - NPAF(k;u,v) \times GS(g) \to 4 - NPAF(mk+2g+s;2nu,2nv,4g,4g)\ \forall\ s \in \mathbb{IN}$.

(ii) $DS(m;n,n) \times 2 - NPAF(k;u,v) \times GS(g) \to OD(4\cdot(mk+2g+s);2nu,2nv,4g,4g)\ \forall\ s \in \mathbb{IN}$.

Απόδειξη.

(i) Με παρόμοιο τρόπο, όπως στην απόδειξη του Πορίσματος 7, παίρνουμε την απεικόνιση:
$DS(m;n,n) \times 2 - NPAF(k;u,v) \to DS(mk;nu,nv)$. Οι παραγόμενες ακολουθίες είναι $2 - NPAF(mk;nu,nv)$, και μπορούν να χρησιμοποιηθούν στο Θεώρημα 12 για να παράγουν το επιθυμητό αποτέλεσμα.

(ii) Εφαρμόζουμε την κατασκευή (3.4) στα αποτελέσματα του (i) ερωτήματος.

□

Θέτουμε $M = \{(2,2,2),\ (6,5,5),\ (10,10,10),\ (14,13,13),\ (24,17,17),\ (26,26,26),\ (30,25,25),\ (40,34,34)\}$ και $N = \{(3,1,4),\ (6,2,8),\ (6,5,5),\ (10,10,10),\ (10,4,16),\ (14,13,13),\ (18,5,20),\ (20,8,32),\ (24,17,17),\ (26,26,26),\ (30,10,40),\ (30,25,25),\ (40,34,34),\ (42,13,52)\}$.

Πόρισμα 9 *Έστω* $x_1 \geq 0, x_2 \geq 0, \ldots, x_8 \geq 0, s \geq 0$ *να είναι ακέραιοι αριθμοί. Τότε υπάρχει ένας ορθογώνιος σχεδιασμός* $OD(4(\cdot k \cdot 2^{x_1} \cdot 6^{x_2} \cdot 10^{x_3} \cdot 14^{x_4} \cdot 24^{x_5} \cdot 26^{x_6} \cdot 30^{x_7} \cdot 40^{x_8} + 2g + s); u \cdot 2^{x_1+1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8}, \nu \cdot 2^{x_1+1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8}, 4g, 4g)$ *για κάθε* $(k, u, \nu) \in N$.

Απόδειξη. Υπάρχουν $DS(s;t,t)$ για κάθε $(s,t,t) \in M$ (βλ. [153]). Για κάθε ακέραιο $x_1 \geq 0, x_2 \geq 0, \ldots, x_8 \geq 0$ μπορούμε να κατασκευάσουμε $DS(2^{x_1} \cdot 6^{x_2} \cdot 10^{x_3} \cdot 14^{x_4} \cdot 24^{x_5} \cdot 26^{x_6} \cdot 30^{x_7} \cdot 40^{x_8}; 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8}, 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8})$. Αυτές οι ακολουθίες στη συνέχεια εφαρμόζονται στις τέσσερις ακολουθίες του Θεωρήματος 12 για να παράγουν τις επιθυμητές ακολουθίες με NPAF μηδέν. Τότε, για κάθε $(k, u, \nu) \in N$, χρησιμοποιούμε τις $2-NPAF(k; u, \nu)$ ακολουθίες από την [153] και εφαρμόζοντας την κατασκευή (3.7) έπεται το ζητούμενο αποτέλεσμα.

□

Παράδειγμα 15 Για $x_2 = 1$ και $x_5 = 1$, όπου $x_i = 0, i = 1,3,4,6,7,8$ παίρνουμε $DS(144; 85, 85)$ ακολουθίες. Ύπάρχουν $2-NPAF(6;2,8)$ και $GS(10)$. Από το Πόρισμα 8 παράγουμε μια άπειρη οικογένεια ορθογώνιων σχεδιασμών: $DS(144;85,85) \times 2-NPAF(6;2,8) \times GS(10) \rightarrow 4-NPAF(20776+s; 40, 40, 170, 680) \rightarrow OD(20776+4s; 40, 40, 170, 680)\ \forall\ s \in \mathbb{N}$.

Είναι προφανές, ότι οι προτεινόμενες πολλαπλασιαστικές μέθοδοι κατασκευής για ορθογώνιους σχεδιασμούς και ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης, είναι χρήσιμες στην κατασκευή μεγάλων ορθογώνιων σχεδιασμών. Επιπλέον, πιστεύουμε ότι αυτές οι μέθοδοι κατασκευής θα φανούν επίσης χρήσιμες στη θεωρητική μελέτη των ορθογώνιων σχεδιασμών και των ασυμπτωτικών ιδιοτήτων τους.

§3.2.3 Ορθογώνιοι Σχεδιασμοί από Σχεδόν-Κανονικές Ακολουθίες

Οι κατευθυνόμενες ακολουθίες, όπως ήδη αναφέραμε εισήχθησαν στην [153] και χρησιμοποιήθηκαν εκτεταμένα στην [58] για την κατασκευή ορθογώνιων σχεδιασμών. Βασικές ακολουθίες (Base sequences) και κανονικές ακολουθίες (normal sequences) εφαρμόστηκαν στην [58] για να κατασκευάσουν κατευθυνόμενες ακολουθίες. Σε αυτήν την ενότητα, αποδεικνύουμε ότι οι σχεδόν-κανονικές ακολουθίες (near-normal sequences) μπορούν να χρησιμοποιηθούν για την κατασκευή κατευθυνόμενων ακολουθιών και στη συνέχεια ορθογώνιων σχεδιασμών.

Συμβολισμός 2 *Χρησιμοποιούμε τους ακόλουθους συμβολισμούς σε αυτήν την ενότητα:*

1. *Κάνουμε χρήση του* $\bar{a}$ *για να συμβολίσουμε το* $-a$.
2. *Με το συμβολισμό* 0_n *υποδηλώνουμε μια ακολουθία μήκους* n, *όπου κάθε στοιχείο της είναι μηδέν.*
3. *Για δοθείσες ακολουθίες* $A = [a_1, a_2, \ldots, a_{m+1}]$ *και* $C = [c_1, c_2, \ldots, c_m]$, *η παρεμβάλλουσα ακολουθία (interleaved sequence)* A/C *της* A *και της* C *ορίζεται ως* $A/C = [a_1, c_1, a_2, c_2, \ldots, a_m, c_m, a_{m+1}]$.

Θα κάνουμε χρήση σχεδόν-κανονικών ακολουθιών μήκους $n = 4m+1$, που συμβολίζονται με $\mathrm{NNS}(n)$, έτσι ώστε να κατασκευάσουμε τέσσερις κατευθυνόμενες ακολουθίες με μήκη $2m+1$, $2m+1$, $2m$, $2m$ τύπου (n, n) που έχουν NPAF μηδέν. Για τους ορισμούς των βασικών και σχεδόν-κανονικών ακολουθιών, παραπέμπουμε στις [122, 143] και στο δεύτερο κεφάλαιο της διατριβής.

Ορισμένα σύνολα από σχεδόν-κανονικές ακολουθίες μπορούν να βρεθούν στις [147] και [240]. Μια πλήρης ταξινόμηση για σχεδόν-κανονικές ακολουθίες $\mathrm{NNS}(n)$ μήκους $n = 4m+1$ για $1 \leq m \leq 11$, και μερικά αποτελέσματα για $m = 12, 13, 14$ και 15 δόθηκε στην [142] και στον Πίνακα 2.2.1.

Θεώρημα 13 *Έστω* $n = 4m + 1$. *Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη* $2m + 1$, $2m + 1$, $2m$, $2m$ *τύπου* (n, n) *που έχουν NPAF μήδεν αν και μόνον αν υπάρχουν σχεδόν-κανονικές ακολουθίες* $\mathrm{NNS}(n)$.

Απόδειξη. Μια τετράδα ακολουθιών $(E, F; G, H)$ όπου $E = [1, X/O_{m-1}]$ και $F = [Y/O_{m-1}]$, είναι σχεδόν-κανονικές ακολουθίες, αν και μόνον αν οι $(1, -1)$ ακολουθίες $A = [1, X/Y]$, $B = [1, X/-Y]$, $C = G + H$, $D = G - H$ με μήκη $2m + 1$, $2m + 1$, $2m$, $2m$, αντίστοιχα, είναι βασικές ακολουθίες ([147, 240]). Εφαρμόζοντας το Θεώρημα 5 της [58] στις παραγόμενες ακολουθίες έχουμε ότι υπάρχουν βασικές ακολουθίες $\mathrm{BS}(2m+1, 2m)$ αν και μόνον αν υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη $2m+1$, $2m+1$, $2m$, $2m$ τύπου $(4m+1, 4m+1) = (n, n)$ που έχουν NPAF μηδέν.

□

Οι νέες κατευθυνόμενες ακολουθίες με μήκη $2m+1, 2m+1, 2m, 2m$ τύπου $(4m + 1, 4m + 1)$ για $m = 1, \ldots, 15$ που παράγονται από τις γνωστές σχεδόν-κανονικές ακολουθιές που δίνονται στις [142, 147, 240] και το Θεώρημα 13 μπορούν να βρεθούν στο τέλος αυτής της ενότητας.

Παρατήρηση 9 *Οι κατευθυνόμενες ακολουθίες που παράγονται από το Θεώρημα 13 δεν μπορούν άμεσα να χρησιμοποιηθούν σε κάποιο σχηματισμό για την κατασκευή ορθογώνιων σχεδιασμών λόγω των άνισων μηκών τους. Τα μήκη τους όμως μπορούν να γίνουν ίσα, προσθέτοντας μηδενικά στο τέλος αυτών των ακολουθιών. Συνεπώς, οι νέες ακολουθίες* $[A, B, [C, 0], [D, 0]]$ *θα έχουν μήκη* $2m + 1, 2m + 1, 2m + 1, 2m + 1$ *και NPAF μηδέν, και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για να παράγουν ορθογώνιους σχεδιασμούς σε δύο μεταβλητές τύπου* $\mathrm{OD}(4(2m + 1); 4m + 1, 4m + 1)$ *(βλ. Παρατήρηση 5).*

Όπως ήδη αναφέραμε, το βασικό πλεονέκτημα των κατευθυνόμενων ακολουθιών, η πολλαπλασιαστική τους ιδιότητα, είναι ότι μπορούμε να αντικαταστήσουμε τις μεταβλητές τους με ακολουθίες με NPAF μηδέν για να παράγουμε μεγαλύτερες ακολουθίες διαφορετικού τύπου, που θα έχουν NPAF μηδέν, κατάλληλες για την κατασκευή μεγάλων ορθογώνιων σχεδιασμών. Αυτή η ιδιότητα, περιγράφεται στο Παράδειγμα 16. Σημειώνουμε ότι, για να κατασκευάσουμε ορθογώνιους σχεδιασμούς από οκτώ κυκλικούς πίνακες χρησιμοποιούμε το σχηματισμό Kharaghani ή K-σχηματισμό (βλ. [112, 121]).

Παράδειγμα 16 Οι ακολουθίες $E = [c, d]$ και $F = [c, -d]$ έχουν NPAF μηδέν και μπορούν να χρησιμοποιηθούν για την κατασκευή ενός ορθογώνιου σχεδιασμού $OD(4; 2, 2)$. Χρησιμοποιώντας τις κατευθυνόμενες ακολουθίες

$$A = [a, a, b],\ B = [-a, b, b],\ C = [a, -a, 0],\ D = [-b, b, 0],$$

που μπορούν να βρεθούν στο τέλος αυτής της ενότητας και εφαρμόζοντας την Παρατήρηση 9, αντικαθιστούμε το a με την ακολουθία E, το b με την ακολουθία F και το 0 με την ακολουθία 0_2, και παράγουμε τις νέες ακολουθίες:

$$A' = [c, d, c, d, c, -d],\ B' = [-c, -d, c, -d, c, -d],$$
$$C' = [c, d, -c, -d, 0, 0],\ D' = [-c, d, c, -d, 0, 0]$$

Είναι εύκολο να επαληθεύσουμε ότι οι ακολουθίες $[A', 0_k]$, $[B', 0_k]$, $[C', 0_k]$ και $[D', 0_k]$ έχουν NPAF μηδέν και συνεπώς μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για την κατασκευή ενός ορθογώνιου σχεδιασμού $OD(4(6 + k); 10, 10)$, για κάθε $k \geq 0$.

Επιπλέον, μπορούμε να παράγουμε έναν $OD(8(6 + k); 10, 10, 10, 10)$, για κάθε $k \geq 0$, μέσω των ακολουθιών $A_1 = [A', 0_k]$, $A_2 = [B', 0_k]$, $A_3 = [C', 0_k]$, $A_4 = [D', 0_k]$, $A_5 = [E', 0_k]$, $A_6 = [F', 0_k]$, $A_7 = [G', 0_k]$ και $A_8 = [H', 0_k]$, όπου

$$E' = [e, f, e, f, e, -f],\ F' = [-e, -f, e, -f, e, -f],$$
$$G' = [e, f, -e, -f, 0, 0],\ H' = [-e, f, e, -f, 0, 0]$$

και οι αντίστοιχοι κυκλικοί πίνακες ικανοποιούν τη σχέση $(A'E'^T - E'A'^T) + (B'F'^T - F'B'^T) + (C'G'^T - G'C'^T) + (D'H'^T - H'D'^T) = 0$.

Πόρισμα 10 *Υποθέτουμε ότι υπάρχουν δύο ακολουθίες E και F μήκους s και τύπου (u_1, u_2) με NPAF μηδέν. Τότε υπάρχουν τέσσερις ακολουθίες μήκους $(2m+1)\cdot s$ και τύπου $(u_1\cdot(4m+1), u_2\cdot(4m+1))$ με NPAF μηδέν, οι οποίες μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για την κατασκευή ενός $OD(4 \cdot ((2m + 1) \cdot s); u_1 \cdot (4m + 1), u_2 \cdot (4m + 1))$, για κάθε $m = 1, \ldots, 15$. Επιπλέον, υπάρχουν οκτώ ακολουθίες μήκους $(2m+1)\cdot s$ και τύπου $(u_1\cdot(4m+1), u_1\cdot(4m+1), u_2\cdot(4m+1), u_2\cdot(4m+1))$ οι οποίες μπορούν να χρησιμοποιηθούν στον K-σχηματισμό για την κατασκευή ενός ορθογώνιου σχεδιασμού $OD(8 \cdot ((2m + 1) \cdot s); u_1 \cdot (4m + 1), u_1 \cdot (4m + 1), u_2 \cdot (4m + 1), u_2 \cdot (4m + 1))$, για κάθε $m = 1, \ldots, 15$.*

Απόδειξη. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες A, B, C, D με μήκη $2m+1$ (ίσα μήκη, βλ. Παρατήρηση 9) και τύπου $(4m+1, 4m+1)$, οι οποίες κατασκευάζονται μέσω του Θεωρήματος 13. Αντικαθιστούμε τα στοιχεία αυτών των κατευθυνόμενων ακολουθιών με τις δοθείσες ακολουθίες και παίρνουμε το επιθυμητό αποτέλεσμα. Για την ακρίβεια, αντικαθιστούμε το στοιχείο a των κατευθυνόμενων ακολουθιών με την E, το b με την F και το 0 με την 0_s. Οι παραγόμενες τέσσερις ακολουθίες έχουν μήκος $(2m+1) \cdot s$ και τύπο $(u_1 \cdot (4m+1), u_2 \cdot (4m+1))$ με NPAF μηδέν και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για να παράγουν τον επιθυμητό ορθογώνιο σχεδιασμό $OD(4 \cdot ((2m+1) \cdot s); u_1 \cdot (4m+1), u_2 \cdot (4m+1))$.

Για την κατασκευή του ορθογώνιου σχεδιασμού $OD(8 \cdot ((2m+1) \cdot s); u_1 \cdot (4m+1), u_1 \cdot (4m+1), u_2 \cdot (4m+1), u_2 \cdot (4m+1))$ θα χρειαστεί να βρούμε οκτώ ακολουθίες $A', B', C', D', E', F', G', H'$ με NPAF μηδέν, των οποίων οι αντίστοιχοι κυκλικοί πίνακες ικανοποιούν τη σχέση

$$(A'E'^T - E'A'^T) + (B'F'^T - F'B'^T) + (C'G'^T - G'C'^T) + (D'H'^T - H'D'^T) = 0$$

Κατασκευάζουμε τις A', B', C', D' με τον ίδιο τρόπο, όπως στο πρώτο μέρος αυτής της απόδειξης. Αντιγράφουμε αυτές τις ακολουθίες, και καλούμε τις νέες ακολουθίες E', F', G', H' αντικαθιστώντας τις μεταβλητές τους με καινούργιες (δηλαδή, αντικαθιστούμε την e με g και την f με h). Μπορούμε εύκολα να επαληθεύσουμε ότι αυτές είναι οι ζητούμενες ακολουθίες, που μπορούν να χρησιμοποιηθούν στον K-σχηματισμό για την κατασκευή ενός ορθογώνιου σχεδιασμού $OD(8 \cdot ((2m+1) \cdot s); u_1 \cdot (4m+1), u_1 \cdot (4m+1), u_2 \cdot (4m+1), u_2 \cdot (4m+1))$.

□

Το Πόρισμα 10 χρίζει ιδιαίτερης προσοχής, όταν η κατασκευή μεγάλων ορθογώνιων σχεδιασμών είναι επιθυμητή. Στο Παράδειγμα 17 θα κάνουμε χρήση των γνωστών ορθογώνιων σχεδιασμών σε δύο μεταβλητές και των κατασκευαζόμενων κατευθυνόμενων ακολουθιών, για να παρουσιάσουμε ορισμένες άπειρες οικογένειες από μεγάλους ορθογώνιους σχεδιασμούς.

Θέτουμε $N = \{(3,1,4), (6,2,8), (6,5,5), (10,10,10), (10,4,16), (14,13,13), (18,5,20), (20,8,32), (24,17,17), (26,26,26), (30,10,40), (30,25,25), (40,34,34), (42,13,52)\}$.

Παράδειγμα 17 Υπάρχουν οι ακόλουθες άπειρες οικογένειες ορθογώνιων σχεδιασμών:

- $OD(4\cdot(2m+1+k);4m+1,4m+1)$ και $OD(8\cdot(2m+1+k);4m+1,4m+1,4m+1,4m+1)$ φορ αλλ $m=1,\ldots,15$ για κάθε $k\geq 0$. (Χρησιμοποιούμε τις τέσσερις κατευθυνόμενες ακολουθίες της κατασκευής που δίνεται στο Θεώρημα 13).
- $OD(4\cdot(2^t\cdot(2m+1)+k);2^t\cdot(4m+1),2^t\cdot(4m+1))$ και $OD(8\cdot(2^t\cdot(2m+1)+k);2^t\cdot(4m+1),2^t\cdot(4m+1),2^t\cdot(4m+1),2^t\cdot(4m+1))$ για κάθε $t\geq 0$, $m=1,\ldots,15$ και για κάθε $k\geq 0$. (Χρησιμοποιούμε τις τέσσερις κατευθυνόμενες ακολουθίες της κατασκευής που δίνεται στο Θεώρημα 13 και τις δύο ακολουθίες μήκους 2 και τύπου $(2,2)$, που έχουν NPAF μηδέν, που δίνονται στην [153]).
- $OD(4\cdot(s\cdot(2m+1)+k);u_1\cdot(4m+1),u_2\cdot(4m+1))$ και $OD(8\cdot(s\cdot(2m+1)+k);u_1\cdot(4m+1),u_1\cdot(4m+1),u_2\cdot(4m+1),u_2\cdot(4m+1))$ για όλες τις τριάδες $(s,u_1,u_2)\in N$, και για κάθε $m=1,\ldots,15$, $k\geq 0$. (Χρησιμοποιούμε τις τέσσερις κατευθυνόμενες ακολουθίες της κατασκευής που δίνεται στο Θεώρημα 13 και τις δύο ακολουθίες μήκους s και τύπου (u_1,u_2), που έχουν NPAF μηδέν, που δίνονται στην [153]).

Θεώρημα 14 *Αν υπάρχουν δύο κατευθυνόμενες ακολουθίες μήκους* s *και τύπου* (u_1,u_2) *με NPAF μηδέν και δύο ακολουθίες μήκους* t *και τύπου* (u_3,u_4) *επίσης με NPAF μηδέν, τότε υπάρχει ένας ορθογώνιος σχεδιασμός* $OD(4\cdot s\cdot t\cdot(2m+1);u_1\cdot u_3\cdot(4m+1),u_2\cdot u_4\cdot(4m+1))$ *για κάθε* $m=1,\ldots,15$.

Απόδειξη. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες μήκους $2m+1$ και τύπου $(4m+1,4m+1)$ μέσω της κατασκευής του Θεωρήματος 13, για κάθε $m=1,\ldots,15$. Αν αντικαθιστήσουμε τις δύο μεταβλητές αυτών των ακολουθιών με τις δύο κατευθυνόμενες ακολουθίες μήκους s και τύπου (u_1,u_2), παράγουμε τέσσερις κατευθυνόμενες ακολουθίες μήκους $s\cdot(2m+1)$ και τύπου $(u_1\cdot(4m+1),u_2\cdot(4m+1))$ με NPAF μηδέν. Τότε, οι μεταβλητές των παραγόμενων κατευθυνόμενων ακολουθιών αντικαθιστώνται με τις δύο ακολουθίες μήκους t και τύπου (u_3,u_4) που έχουν NPAF μηδέν. Οι τελευταίες ακολουθίες, δίνουν το επιθυμητό αποτέλεσμα.

□

Θέτουμε $M = \{(2,2,2),\ (6,5,5),\ (10,10,10),\ (14,13,13),\ (24,17,17),\ (26,26,26),\ (30,25,25),\ (40,34,34)\}$.

Πόρισμα 11 *Έστω* $x_1 \geq 0, x_2 \geq 0, \ldots, x_8 \geq 0, k \geq 0$ *να είναι ακέραιοι αριθμοί. Τότε υπάρχει ένας ορθογώνιος σχεδιασμός* $\mathrm{OD}(4(\cdot t \cdot 2^{x_1} \cdot 6^{x_2} \cdot 10^{x_3} \cdot 14^{x_4} \cdot 24^{x_5} \cdot 26^{x_6} \cdot 30^{x_7} \cdot 40^{x_8} \cdot (2m+1)+k); u_1 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1), u_2 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1))$ *για κάθε* $(t, u_1, u_2) \in N$ *και* $m = 1, \ldots, 15$.

Απόδειξη. Υπάρχουν κατευθυνόμενες ακολουθίες μήκους s και τύπου (t_1, t_2) με NPAF μηδέν για κάθε $(s, t_1, t_2) \in M$ (βλ. [153]). Για καθένα από τους ακεραίους $x_1 \geq 0, x_2 \geq 0, \ldots, x_8 \geq 0$ μπορούμε να κατασκευάσουμε κατευθυνόμενες ακολουθίες με NPAF μηδέν, οι οποιές θα έχουν μήκος $2^{x_1} \cdot 6^{x_2} \cdot 10^{x_3} \cdot 14^{x_4} \cdot 24^{x_5} \cdot 26^{x_6} \cdot 30^{x_7} \cdot 40^{x_8}$ και τύπο $(2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8}, 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8})$. Αυτές οι ακολουθίες στη συνέχεια εφαρμόζονται στις τέσσερις κατευθυνόμενες ακολουθίες του Θεωρήματος 13 για να παράγουν τις επιθυμητές κατευθυνόμενες ακολουθίες. Τότε, για κάθε $(t, u_1, u_2) \in N$, χρησιμοποιούμε τις ακολουθίες με NPAF μηδέν από την [153], παραθέτοντας στο τέλος αυτών k μηδενικά και το αποτέλεσμα έπεται.

□

Παράδειγμα 18 Για $x_2 = 1$, $x_5 = 1$ και $x_i = 0$ για $i = 1, 3, 4, 6, 7, 8$, παράγουμε δύο κατευθυνόμενες ακολουθίες μήκους 144 και τύπου $(85, 85)$. Χρησιμοποιώντας τις τέσσερις κατευθυνόμενες ακολουθίες μήκους 9 και τύπου $(17, 17)$ (οι οποίες παράγονται από τις $\mathrm{NNS}(17)$, βλ. Θεώρημα 13 και Παρατήρηση 9), παράγουμε τέσσερις κατευθυνόμενες ακολουθίες με μήκη 1296 και τύπου $(1445, 1445)$ που έχουν NPAF μηδέν. Υπάρχουν δύο ακολουθίες μήκους 3 και τύπου $(1, 4)$ με NPAF μηδέν. Συνεπώς, μπορούμε να κατασκευάσουμε τέσσερις ακολουθίες μήκους 3888 και τύπου $(1445, 5780)$ οι οποίες μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για να παράγουν έναν ορθογώνιο σχεδιασμό $\mathrm{OD}(15552 + 4k; 1445, 5780)$, για κάθε $k \geq 0$.

Πόρισμα 12 *Έστω* $x_1 \geq 0, x_2 \geq 0, \ldots, x_8 \geq 0, k \geq 0$ *να είναι ακέραιοι αριθμοί. Τότε υπάρχει ένας ορθογώνιος σχεδιασμός* $\mathrm{OD}(8(\cdot t \cdot 2^{x_1} \cdot 6^{x_2} \cdot 10^{x_3} \cdot 14^{x_4} \cdot 24^{x_5} \cdot 26^{x_6} \cdot 30^{x_7} \cdot 40^{x_8} \cdot (2m+1)+k); u_1 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1), u_2 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1), u_1 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1), u_2 \cdot 2^{x_1} \cdot 5^{x_2} \cdot 10^{x_3} \cdot 13^{x_4} \cdot 17^{x_5} \cdot 26^{x_6} \cdot 25^{x_7} \cdot 34^{x_8} \cdot (4m+1))$ *για κάθε* $(t, u_1, u_2) \in N$ *και* $m = 1, \ldots, 15$.

Απόδειξη. Κατασκευάζουμε τις ακολουθίες με NPAF μηδέν όπως στο Πόρισμα 11. Στη συνέχεια, αντιγράφουμε αυτές τις ακολουθίες και μετονομάζουμε τις μεταβλητές τους. Οι παραγόμενες ακολουθίες είναι οι επιθυμητές οκτώ ακολουθίες που μπορούν να χρησιμοποιηθούν στον K-σχηματισμό για να παράγουν το επιθυμητό αποτέλεσμα.

□

Και σε αυτήν την ενότητα, θα θέλαμε να αναφέρουμε ότι οι προτεινόμενες πολλαπλασιαστικές μέθοδοι κατασκευής για ορθογώνιους σχεδιασμούς και ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης, είναι χρήσιμες στην κατασκευή μεγάλων ορθογώνιων σχεδιασμών. Επιπλέον, πιστεύουμε ότι αυτές οι μέθοδοι κατασκευής θα φανούν επίσης χρήσιμες στη θεωρητική μελέτη των ορθογώνιων σχεδιασμών και των ασυμπτωτικών ιδιοτήτων τους.

Οι Νέες Κατευθυνόμενες Ακολουθίες Στον Πίνακα 3.2.3, παρουσιάζουμε τις νέες κατευθυνόμενες ακολουθίες με μήκη $2m+1, 2m+1, 2m, 2m$ και τύπο $(4m+1, 4m+1)$ για $m = 1, \ldots, 15$, οι οποίες παράγονται από τις γνωστές σχεδόν-κανονικές ακολουθίες που δίνονται στις [142, 147, 240] μέσω του Θεωρήματος 13.

§3.2.4 Ορθογώνιοι Σχεδιασμοί από Ακολουθίες Golay

Θεώρημα 15 *Υποθέτουμε ότι υπάρχουν* $GS(g_1)$ *και* $GS(g_2)$. *Τότε υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για κατευθυνόμενες CS και ορθογώνιους σχεδιασμούς:*

(i) $GS(g_1) \times GS(g_2) \to 4-NPAF(g_1+2g_2+s; 4g_1, 4g_2, 4g_2)\ \forall\ s \in \mathbb{N}$.

(ii) $GS(g_1) \times GS(g_2) \to OD(4\cdot(g_1+2g_2+s); 4g_1, 4g_2, 4g_2)\ \forall\ s \in \mathbb{N}$.

Απόδειξη.

(i) Υπάρχει η ακόλουθη κατασκευή που δίνεται στο Θεώρημα 10 της [156] και συνδυάζοντας τη με την κατασκευή (3.7) παίρνουμε: $GS(g_1)\times GS(g_2) \to 4-NPAF(g_1+2g_2; 4g_1, 4g_2, 4g_2) \to 4-NPAF(g_1+2g_2+s; 4g_1, 4g_2, 4g_2)$. Επιπλέον, η κατασκευή (3.9) διασφαλίζει ότι

m	A	B	C	D
1	a a b	$\bar{a}$ b b	a $\bar{a}$	$\bar{b}$ b
2	a a b a $\bar{b}$	a b $\bar{a}$ b b	a $\bar{b}$ b $\bar{a}$	$\bar{b}$ $\bar{a}$ a b
3	a $\bar{a}$ b a b a b	$\bar{a}$ b $\bar{a}$ b $\bar{a}$ $\bar{b}$ b	a b b $\bar{b}$ $\bar{b}$ $\bar{a}$	$\bar{b}$ a a $\bar{a}$ $\bar{a}$ b
4	a $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b a $\bar{b}$	a b $\bar{a}$ b a $\bar{b}$ $\bar{a}$ $\bar{b}$ b	a $\bar{a}$ a a a a a $\bar{a}$	$\bar{b}$ b b b b b $\bar{b}$ b
5	a a $\bar{b}$ a b a b $\bar{a}$ $\bar{b}$ a b	$\bar{a}$ b a $\bar{b}$ $\bar{a}$ b $\bar{a}$ b a b b	b a $\bar{a}$ b $\bar{a}$ a $\bar{b}$ a a $\bar{b}$	a b b a b $\bar{b}$ $\bar{a}$ $\bar{b}$ b $\bar{a}$
6	a a $\bar{b}$ $\bar{a}$ $\bar{b}$ a b a b a $\bar{b}$ a b	$\bar{a}$ b a b $\bar{a}$ b $\bar{a}$ b a $\bar{b}$ a b b	b a $\bar{a}$ a a b $\bar{b}$ a $\bar{a}$ $\bar{a}$ $\bar{a}$ $\bar{b}$	a $\bar{b}$ $\bar{b}$ $\bar{b}$ b a $\bar{a}$ b b $\bar{b}$ b $\bar{a}$
7	a a b a $\bar{b}$ $\bar{a}$ b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b	$\bar{a}$ $\bar{b}$ $\bar{a}$ b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b b	b a $\bar{a}$ $\bar{b}$ b a a a a b $\bar{b}$ a $\bar{a}$ b	$\bar{a}$ $\bar{b}$ b a $\bar{a}$ b b b b $\bar{a}$ a $\bar{b}$ b $\bar{a}$
8	a a b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ b a b $\bar{a}$ b a b $\bar{a}$ $\bar{b}$	$\bar{a}$ $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ a b $\bar{a}$ b b	$\bar{b}$ a a b $\bar{a}$ b a $\bar{b}$ b a b a $\bar{b}$ a $\bar{a}$ $\bar{b}$	a $\bar{b}$ b a b $\bar{a}$ b $\bar{a}$ a b $\bar{a}$ $\bar{b}$ $\bar{a}$ b b a
9	a a b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ b a b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ $\bar{b}$	$\bar{a}$ $\bar{b}$ $\bar{a}$ b a $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ a $\bar{b}$ a b b	a b $\bar{a}$ $\bar{b}$ $\bar{a}$ a a $\bar{b}$ b $\bar{b}$ b a a a b a $\bar{b}$ a	$\bar{b}$ a $\bar{b}$ $\bar{a}$ b b b $\bar{a}$ a $\bar{a}$ a b b $\bar{b}$ a $\bar{b}$ $\bar{a}$ b
10	a a b a $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ $\bar{b}$ $\bar{a}$ b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$	a b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ a $\bar{b}$ $\bar{a}$ b a $\bar{b}$ $\bar{a}$ $\bar{b}$ a b b	$\bar{b}$ a $\bar{b}$ a $\bar{b}$ b a b a a $\bar{a}$ a b a $\bar{b}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ a b	$\bar{a}$ b a $\bar{b}$ a a b $\bar{a}$ b $\bar{b}$ b b $\bar{a}$ b $\bar{a}$ a b a b a

Πίνακας 3.1: Κατευθυνόμενες ακολουθίες A, B, C, D με μήκη $2m+1, 2m+1, 2m, 2m$ και τύπο $(4m+1, 4m+1) = (n, n)$, οι οποίες κατασκευάζονται από τις NNS(n), για $n = 4m + 1$

n	A	B	C	D
11	a $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ a b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b a b a b	$\bar{a}$ b $\bar{a}$ b $\bar{a}$ $\bar{b}$ $\bar{a}$ b a $\bar{b}$ a b $\bar{a}$ b a b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ b	b a a b $\bar{a}$ a a a b $\bar{b}$ $\bar{a}$ a $\bar{b}$ $\bar{b}$ a a a $\bar{a}$ b a $\bar{a}$ $\bar{b}$	a $\bar{b}$ b $\bar{a}$ $\bar{b}$ b b b a a b $\bar{b}$ a $\bar{a}$ b b b $\bar{b}$ $\bar{a}$ b $\bar{a}$
12	a a b a $\bar{b}$ a b a $\bar{b}$ a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ b a b a $\bar{b}$ a $\bar{b}$ $\bar{a}$ b	$\bar{a}$ $\bar{b}$ a b $\bar{a}$ $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ a b a $\bar{b}$ $\bar{a}$ b a b $\bar{a}$ b b	$\bar{b}$ b a $\bar{b}$ b a b a $\bar{a}$ $\bar{a}$ $\bar{a}$ a a a $\bar{a}$ a $\bar{a}$ b a $\bar{b}$ $\bar{b}$ a $\bar{b}$ $\bar{b}$	a a b a a b $\bar{a}$ $\bar{b}$ b $\bar{b}$ b b b $\bar{b}$ $\bar{b}$ $\bar{b}$ b $\bar{a}$ b $\bar{a}$ a b $\bar{a}$ a
13	a $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b a $\bar{b}$ a b a $\bar{b}$ a $\bar{b}$ b	$\bar{a}$ b a $\bar{b}$ a $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ $\bar{a}$ b a $\bar{b}$ a b a $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$	$\bar{b}$ b a a $\bar{a}$ a $\bar{b}$ $\bar{b}$ a $\bar{a}$ $\bar{a}$ $\bar{b}$ b b $\bar{b}$ a a a b $\bar{b}$ $\bar{a}$ a a b b	$\bar{a}$ $\bar{a}$ b b b $\bar{b}$ a $\bar{a}$ b b b a $\bar{a}$ $\bar{a}$ a $\bar{b}$ $\bar{b}$ b a a b $\bar{b}$ $\bar{b}$ b $\bar{a}$ a
14	a $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b a b a b $\bar{b}$ $\bar{a}$ b	$\bar{a}$ $\bar{b}$ a b $\bar{a}$ b a b $\bar{a}$ b a b $\bar{a}$ $\bar{b}$ a b $\bar{a}$ b a $\bar{b}$ $\bar{a}$ $\bar{b}$ a $\bar{b}$ b	a a $\bar{b}$ a $\bar{b}$ a b a a a $\bar{a}$ $\bar{a}$ b a $\bar{a}$ $\bar{b}$ a a a a $\bar{a}$ a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ a	b $\bar{b}$ a $\bar{b}$ a $\bar{b}$ a a b $\bar{b}$ b b b a $\bar{b}$ b $\bar{a}$ $\bar{b}$ b b b $\bar{a}$ b a b a b b
15	a $\bar{a}$ b $\bar{a}$ b $\bar{a}$ b $\bar{a}$ b $\bar{a}$ $\bar{b}$ a $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ a b a b a $\bar{b}$ a b $\bar{a}$ $\bar{b}$ a b	$\bar{a}$ b a $\bar{b}$ a b $\bar{a}$ b $\bar{a}$ b $\bar{a}$ b $\bar{a}$ b a $\bar{b}$ $\bar{a}$ $\bar{b}$ a b a $\bar{b}$ $\bar{a}$ $\bar{b}$ $\bar{a}$ b $\bar{a}$ $\bar{b}$ b	$\bar{a}$ $\bar{a}$ b $\bar{b}$ $\bar{a}$ a b a b $\bar{a}$ a a $\bar{b}$ a $\bar{a}$ b a a a $\bar{b}$ a b $\bar{a}$ $\bar{a}$ a b b $\bar{a}$ a	b $\bar{b}$ $\bar{a}$ a b $\bar{b}$ $\bar{b}$ a b b b $\bar{a}$ $\bar{b}$ b a $\bar{b}$ $\bar{a}$ b a b b $\bar{b}$ a $\bar{a}$ $\bar{b}$ $\bar{b}$

Πίνακας 3.1: Κατευθυνόμενες ακολουθίες A, B, C, D με μήκη $2m+1, 2m+1, 2m, 2m$ και τύπο $(4m+1, 4m+1) = (n, n)$, οι οποίες κατασκευάζονται από τις $NNS(n)$, για $n = 4m + 1$ (Συνέχεια)

οι ενδιάμεσες ακολουθίες είναι κατευθυνόμενες. Οι υπόλοιποι όροι στο NPAF των παραγόμενων ακολουθιών είναι μηδέν χωρίς να εξαρτώνται από τη μεταθετικότητα των μεταβλητών.

(ii) Εφαρμόζουμε την κατασκευή (3.4) στα αποτελέσματα του (i) ερωτήματος.

□

Σημειώνουμε ότι, η ειδική περίπτωση του Θεωρήματος 15, η οποία παράγει πλήρεις ορθογώνιους σχεδιασμούς, μελετήθηκε στην [156]. Η εφαρμογή του Θεωρήματος 15 περιγράφεται από το ακόλουθο παράδειγμα.

Παράδειγμα 19 Υπάρχουν $GS(10)$ από την [71], και εφαρμόζοντας την κατασκευή (3.8) έχουμε, $GS(10) \to 2-NPAF(10;20)$. Από την κατασκευή (3.9) υπάρχουν $GS(2) \to 2 - NPAF(4;4,4)$, ως ακολούθως:

$$P' = [x, x, y, -y] \quad \text{ανδ} \quad Q' = [-x, x, -y, -y].$$

Τότε από το Θεώρημα 15, μπορούμε να κατασκευάσουμε $GS(10) \times GS(2) \to 4 - NPAF(14;8,8,40)$.

Εφαρμόζοντας τις απεικονίσεις (3.7) και (3.4) παίρνουμε:
$4 - NPAF(14;8,8,40) \to 4 - NPAF(14+s;8,8,40) \to OD(56+4s;8,8,40)\ \forall\ s \in \mathbb{N}$.

Οι ακολουθίες Golay χρησιμοποιούνται σε διάφορες περιοχές όπως είναι η Οπτική και οι τηλεπικοινωνίες, καθώς και στη Συνδυαστική για την κατασκευή ορθογώνιων σχεδιασμών και πινάκων Hadamard. Αναδιατυπώνουμε στη συνέχεια την κατασκευή μας για ορθογώνιους σχεδιασμούς που παράγονται μέσω ακολουθιών Golay, εφαρμόζοντας την προηγούμενη σύνθετη κατασκευή.

Πόρισμα 13 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών σε τρείς μεταβλητές,* $OD(4\cdot(2^a\cdot 10^b\cdot 26^c + 2^{e+1}\cdot 10^f\cdot 26^g + s); 2^{a+2}\cdot 10^b\cdot 26^c, 2^{e+2}\cdot 10^f\cdot 26^g, 2^{e+2}\cdot 10^f\cdot 26^g)$ *για κάθε* $s \geq 0$ *όπου* a, b, c, d, e, f *είναι μη-αρνητικοί ακέραιοι.*

Απόδειξη. Μπορούμε να κατασκευάσουμε A, B και G, H ακολουθίες Golay με μήκη $n_1 = 2^a\cdot 10^b\cdot 26^c$ και $n_2 = 2^e\cdot 10^f\cdot 26^g$, αντίστοιχα, όπου a, b, c, d, e, f είναι μη-αρνητικοί ακέραιοι μέσω της κατασκευής (3.10). Εφαρμόζοντας αυτές τις ακολουθίες στην κατασκευή του Θεωρήματος 15 παράγουμε το επιθυμητό αποτέλεσμα. Ιδιαίτερα, οι ακολουθίες $P' =$

$[Gx \mid Hy]$ και $Q' = [H^{\star}x \mid -G^{\star}y]$ είναι $2 - \mathrm{NPAF}(2^{e+1} \cdot 10^{f} \cdot 26^{g}; 2^{e+1} \cdot 10^{f} \cdot 26^{g}, 2^{e+1} \cdot 10^{f} \cdot 26^{g})$ ακολουθίες. Αυτό το ζεύγος ακολουθιών Golay μετέπειτα διπλασιάζεται στην κατασκευή του Θεωρήματος 15:

$$\begin{array}{l} P = [\ \ A \mid \ \ \ P' \ \ ] \\ Q = [\ \ A \mid -P' \ \ ] \\ R = [\ \ B \mid \ \ \ Q' \ \ ] \\ S = [\ \ B \mid -Q' \ \ ] \end{array} \qquad (3.12)$$

και το αποτέλεσμα έπεται.

□

§3.2.5 Νέοι Πίνακες Στάθμισης από Συμπληρωματικές Ακολουθίες

Ορθογώνιοι σχεδιασμοί σε λιγότερες μεταβλητές μπορούν να παραχθούν μέσω της τεχνικής της "εξίσωσης και διαγραφής μεταβλητών" (βλ. [70]), από τους ορθογώνιους σχεδιασμούς που κατασκευάζονται μέσω συμπληρωματικών και κατευθυνόμενων ακολουθιών, και παράγουν πίνακες στάθμισης καθώς ένας ορθογώνιος σχεδιασμός $\mathrm{OD}(n; k)$ είναι ισοδύναμος με έναν πίνακα στάθμισης $W = W(n, k)$. Με παρόμοιο τρόπο, οι ορθογώνιοι σχεδιασμοί που παρήχθησαν μέσω των συμπληρωματικών ακολουθιών αυτού του κεφαλαίου (δηλαδή, από ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης) μπορούν να παράγουν άπειρες οικογένειες πινάκων στάθμισης.

Μια Άπειρη Οικογένεια από $W(156 + 4k, 125)$ Πίνακες Στάθμισης

Πόρισμα 14 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών* $\mathrm{OD}(156 + 4k; 25, 100)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(156 + 4k, 125)$, *για κάθε* $k \geq 0$.

Απόδειξη. Χρησιμοποιούμε τις δύο ακολουθίες μήκους 3 και τύπου $(1, 4)$ με NPAF μηδέν από την [153]. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη 13 (ίσα μήκη, βλ. Παρατήρηση 9) τύπου $(25, 25)$ που κατασκευάζονται μέσω του Θεωρήματος 13. Εφαρμόζοντας το Πόρισμα 10 παράγουμε μια άπειρη οικογένεια ορθογώνιων σχεδιασμών

$\mathrm{OD}(156{+}4\mathrm{k}; 25, 100)$. Εξισώνοντας τις μεταβλητές στην προηγούμενη οικογένεια και αντικαθιστώντας τες με 1 παράγουμε τέσσερις ακολουθίες μήκους 39 με NPAF μηδέν, στις οποίες παραθέτουμε k μηδενικά για να πάρουμε μια άπειρη οικογένεια από πίνακες στάθμισης $W(156{+}4\mathrm{k}, 125)$, για κάθε $\mathrm{k} \geq 0$:

```
++-++--0---+-0-++-+0+++-+0+++--0-++-+0+
--++0+++-+0+--++0+--++0+++--0-++-+0++0+
+0+++---+++-++-+0+-0-++---+--+--+-0-000
++--0--0--0-+0+++---++0++0+-0-+0+--+000
```

□

Μια Άπειρη Οικογένεια από $W(144 + 4s, 144)$ Πίνακες Στάθμισης

Πόρισμα 15 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών,* $\mathrm{OD}(144 + 4s; 32, 32, 80)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(144 + 4\mathrm{s}, 144)$, $\forall\ s\ \in \mathbb{IN}$.

Απόδειξη. Υπάρχουν $\mathrm{GS}(20)$ και $\mathrm{GS}(8)$ μέσω της κατασκευής (3.10), $\mathrm{GS}(2) \times \mathrm{GS}(10) \to \mathrm{GS}(20)$ και $(\mathrm{GS}(2) \times \mathrm{GS}(2)) \times \mathrm{GS}(2) \to \mathrm{GS}(8)$.
Από το Θεώρημα 15 παίρνουμε $\mathrm{GS}(20) \times \mathrm{GS}(8) \to 4 - \mathrm{NPAF}(36 + s; 32, 32, 80)$. Χρησιμοποιώντας την κατασκευή (3.4) παράγουμε έναν $\mathrm{OD}(144 + 4s; 32, 32, 80)$, $\forall\ s\ \in \mathbb{IN}$. Εφαρμόζοντας την κατασκευή (3.5) παράγουμε $4 - \mathrm{NPAF}(36; 32, 32, 80) \to 4 - \mathrm{CS}(36, 144)$:

```
++----+--+----+-++-+++-++-++-+++---
++----+--+----+-++----+--+--+---+++
+--+-+++-+++-+----++---+++-+-+--+---
+--+-+++-+++-+----++++---+-+-++-+++
```

όπου συνδυάζοντας τις απεικονίσεις (3.6) και (3.3) παίρνουμε:
$4 - \mathrm{CS}(36, 144) \to 4 - \mathrm{CS}(36 + \mathrm{s}, 144) \to W(144 + 4\mathrm{s}, 144)$, $\forall\ s\ \in \mathbb{IN}$.

□

Μια Άπειρη Οικογένεια από $W(160 + 4\mathrm{k}, 144)$ Πίνακες

Πόρισμα 16 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών* $\mathrm{OD}(160 + 4\mathrm{k}; 72, 72)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(160 + 4\mathrm{k}, 144)$, *για κάθε* $\mathrm{k} \geq 0$.

Απόδειξη. Χρησιμοποιούμε τις δύο ακολουθίες μήκους 8 και τύπου $(8, 8)$ με NPAF μηδέν από την [153]. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη 5 (ίσα μήκη, βλ. Παρατήρηση 9) τύπου $(9, 9)$ που κατασκευάζονται μέσω του **Θεωρήματος** 13. Εφαρμόζοντας το Πόρισμα 10 παράγουμε μια άπειρη οικογένεια ορθογώνιων σχεδιασμών $\mathrm{OD}(160 + 4\mathrm{k}; 72, 72)$. Εξισώνοντας τις μεταβλητές στην προηγούμενη οικογένεια και αντικαθιστώντας τες με 1 παράγουμε τέσσερις ακολουθίες μήκους 39 με NPAF μηδέν, στις οποίες παραθέτουμε k μηδενικά για να πάρουμε μια άπειρη οικογένεια από πίνακες στάθμισης $W(160+4\mathrm{k}, 144)$, για κάθε $\mathrm{k} \geq 0$:

```
++-++++-++-++++-+---+++++++++--+++-+--
++-++++-+---+-++--+----++---+-+++---+-++
++-++++--+++-+--+---+-++--+----+00000000
-+++-+----+---+++-++++-+---+-++00000000
```

□

Μια Άπειρη Οικογένεια από $W(200 + 4\mathrm{k}, 196)$ **Πίνακες Στάθμισης**

Πόρισμα 17 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών* $\mathrm{OD}(200 + 4\mathrm{k}; 98, 98)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(200 + 4\mathrm{k}, 196)$, *για κάθε* $\mathrm{k} \geq 0$.

Απόδειξη. Χρησιμοποιούμε τις δύο ακολουθίες μήκους 2 και τύπου $(2, 2)$ με NPAF μηδέν από την [153]. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη 25 (ίσα μήκη, βλ. Παρατήρηση 9) τύπου $(49, 49)$ που κατασκευάζονται μέσω του **Θεωρήματος** 13. Εφαρμόζοντας το Πόρισμα 10 παράγουμε μια άπειρη οικογένεια ορθογώνιων σχεδιασμών $\mathrm{OD}(200+4\mathrm{k}; 98, 98)$. Εξισώνοντας τις μεταβλητές στην προηγούμενη οικογένεια και αντικαθιστώντας τες με 1 παράγουμε τέσσερις ακολουθίες μήκους 39 με NPAF μηδέν, στις οποίες παραθέτουμε k μηδενικά για να πάρουμε μια άπειρη οικογένεια από πίνακες στάθμισης $W(200 + 4\mathrm{k}, 196)$, για κάθε $\mathrm{k} \geq 0$:

```
++-++++-++-+--+---++++---+---++++-+++---+-+++-+-
----+----+--+---+-++-+---+--+-++-+---++++---+-+++-
++++-+---+--+---++-++--+-+-+-+--++++-+++---++00
+--+--+---+-+++-+++++++++--+++--+---+++-++++-+-00
```

□

Μια Άπειρη Οικογένεια από $W(224+4s,196)$ Πίνακες Στάθμισης

Πόρισμα 18 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών,* $\mathrm{OD}(224+4s;34,34,64,64)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(224+4s,196)$, $\forall\ s\ \in \mathbb{IN}$.

Απόδειξη. Υπάρχουν $2-\mathrm{NPAF}(24;17,17)$ ακολουθίες από την [153] και $\mathrm{GS}(16)$ μέσω της κατασκευής (3.10), $((\mathrm{GS}(2)\times\mathrm{GS}(2))\times\mathrm{GS}(2))\times\mathrm{GS}(2)\rightarrow \mathrm{GS}(16)$.
Από το Θεώρημα 12 παράγουμε $2-\mathrm{NPAF}(24;17,17)\times\mathrm{GS}(16)\rightarrow 4-\mathrm{NPAF}(56+s;34,34,64,64)$ ακολουθίες. Χρησιμοποιώντας την κατασκευή (3.4) παίρνουμε έναν ορθογώνιο σχεδιασμό $\mathrm{OD}(224+4s;34,34,64,64)$, $\forall\ s\ \in \mathbb{IN}$. Εφαρμόζοντας την κατασκευή (3.5) παίρνουμε $4-\mathrm{NPAF}(56;34,34,64,64)\rightarrow 4-\mathrm{CS}(56,196)$:

```
+-+0-000+++-+-0++0-0++-++++-++-++-+++---+++---+-+-++-+++
+-+0-000+++-+-0++0-0++-+---+--+--+---+++---+++-+-+--+---
+-++0-0++0------000+0-+-+++-++-+-+---++++++---+--+--+---
+-++0-0++0------000+0-+----+--+-+-+++------+++-++-++-+++
```

όπου συνδυάζοντας τις απεικονίσεις (3.6) και (3.3) παίρνουμε:
$4-\mathrm{CS}(56,196)\rightarrow 4-\mathrm{CS}(56+s,196)\rightarrow W(224+4s,196)$, $\forall\ s\ \in \mathbb{IN}$.

□

Μια Άπειρη Οικογένεια από $W(276+4k,225)$ Πίνακες Στάθμισης

Πόρισμα 19 *Υπάρχει μια άπειρη οικογένεια ορθογώνιων σχεδιασμών,* $\mathrm{OD}(276+4k;45,180)$. *Επιπλέον, υπάρχει μια άπειρη οικογένεια από πίνακες στάθμισης* $W(276+4k,225)$, *για κάθε* $k\geq 0$.

Απόδειξη. Χρησιμοποιούμε τις δύο ακολουθίες μήκους 3 και τύπου $(1,4)$ με NPAF μηδέν από την [153]. Υπάρχουν τέσσερις κατευθυνόμενες ακολουθίες με μήκη 23 (ίσα μήκη, βλ. Παρατήρηση 9) τύπου $(45,45)$ που κατασκευάζονται μέσω του Θεωρήματος 13. Εφαρμόζοντας το Πόρισμα 10 παράγουμε μια άπειρη οικογένεια ορθογώνιων σχεδιασμών $\mathrm{OD}(276+4k;45,180)$. Εξισώνοντας τις μεταβλητές στην προηγούμενη οικογένεια και αντικαθιστώντας τες με 1 παράγουμε τέσσερις ακολουθίες μήκους 69 με NPAF μηδέν, στις οποίες παραθέτουμε k μηδενικά για να πάρουμε μια άπειρη οικογένεια από πίνακες στάθμισης $W(276+4k,225)$, για κάθε $k\geq 0$:

```
++--0-++--0---++0+--+-0-++-+0+--+-0---+-0-++-+0+++-+0+++-+0+++-+0++0+
--+--++0+--++0+--++0+--++0+++--0-++--0---++0+++--0---+-0-++-+0+++-+0+
++-+0+++--0---+--+++---+++-+0++0+0+-0-++-++---+++-++-+0+--++0+++-000
+0+--+-0---++0++0+-0-+0++0+++---+--+--++0+-0-+0+-0--0-++-+0+--++0+000
```

□

Οι Νέοι Πίνακες Στάθμισης Στον ακόλουθο πίνακα, η πρώτη στήλη δίνει τη νέα οικογένεια από πίνακες στάθμισης, ενώ η δεύτερη στήλη δίνει το εύρος αυτής της οικογένειας. Η τρίτη στήλη δίνει το βάρος της οικογένειας, ενώ η τέταρτη στήλη δίνει την τάξη n του κάθε πίνακα στάθμισης. Κάνουμε χρήση της ακόλουθης σύμβασης: αν η τάξη εμφανίζεται χωρίς παρενθέσεις στην εγγραφή που αντιστοιχεί στο w, τότε ο $W(n, w)$ πίνακας στάθμισης είναι γνωστός (βλ. [35]). Αν η τάξη n εμφανίζεται σε παρενθέσεις, τότε η ύπαρξη αυτού του πίνακα στάθμισης ήταν καταχωρημένη ως άγνωστη στη δεύτερη έκδοση του Εγχειριδίου Συνδυαστικών Σχεδιασμών (Handbook of Combinatorial Designs). Επιπλέον, η τελευταία στήλη του πίνακα δίνει το συνολικό αριθμό των ανοιχτών περιπτώσεων που επιλύσαμε από τις αντίστοιχες οικογένειες των πινάκων στάθμισης που δίνονται στον πίνακα αυτό.

Οικογένεια	Εύρος	Βάρος	Τάξη					Σύνολο
$W(156+4s, 125)$	$0 \le s \le 4$	125	156	160	(164)	168	(172)	2
$W(144+4s, 144)$	$0 \le s \le 9$	144	144	(148)	(152)	(156)	160	6
			(164)	168	(172)	(176)	180	
$W(200+4s, 196)$	$0 \le s \le 29$	196	200	(204)	208	(212)	(216)	20
			(220)	(224)	228	(232)	(236)	
			240	(244)	(248)	(252)	256	
			(260)	(264)	(268)	272	(276)	
			(280)	(284)	288	(292)	(296)	
			300	304	(308)	312	(316)	
$W(276+4s, 225)$	$0 \le s \le 9$	225	(276)	(280)	(284)	288	(292)	7
			(296)	300	304	(308)	(312)	

Πίνακας 3.2: Νέες Οικογένειες από Πίνακες Στάθμισης μέσω Συμπληρωματικών Ακολουθιών

Οι νέοι αυτοί πίνακες στάθμισης που ανανεώνουν το Εγχειρίδιο Συνδυαστικών Σχεδιασμών, μπορούν να βρεθούν και στην ιστοσελίδα `http://www.cems.uvm.edu/~dinitz/part5.newresults.html`.

§3.3 Ορθογώνιοι Σχεδιασμοί από Πίνακες Στάθμισης

Σε αυτήν την ενότητα, θα παρουσιάσουμε μια μέθοδο κατασκευής ορθογώνιων σχεδιασμών από πίνακες στάθμισης και τριαδικά συμπληρωματικά ζεύγη ακολουθιών.

§3.3.1 Η Έννοια της Διάδοσης για Ακολουθίες με Μηδενική Περιοδική Συνάρτηση Αυτοσυσχέτισης

Η έννοια της διάδοσης ή εξάπλωσης δύο ακολουθιών με PAF μηδέν, δόθηκε στην [138]. Δίνουμε κάποιους απαραίτητους ορισμούς, που θα χρειαστούμε για τα αποτελέσματα αυτής της ενότητας, παρακάτω.

Ορισμός 19 *Μια ακολουθία* $A = [a_1, \cdots, a_n]$ *μήκους* n *θα λέμε ότι έχει διάδοση (spread) (των μηδενικών)* $\sigma = \sigma(A)$*, αν το μεγαλύτερο τμήμα (block) συνεχόμενων μηδενικών που συμβαίνουν σε αυτή είναι μήκους* σ*.*

Σημειώνουμε ότι, για μια ακολουθία $A = [a_1, \cdots, a_n]$ με διάδοση σ μπορεί να υπάρχουν περισσότερα από σ μηδενικά, συνολικά.

Παράδειγμα 20 Οι παρακάτων ακολουθίες μήκους $n = 7$, έχουν διάδοση $\sigma = 3$:

- $[0, 0, 0, \underbrace{a_4}_{\neq 0}, a_5, a_6 \underbrace{a_7}_{\neq 0}]$ όπου τα a_5, a_6 μπορεί να είναι μηδέν
- $[\underbrace{a_1}_{\neq 0}, 0, 0, 0, \underbrace{a_5}_{\neq 0}, a_6, a_7]$ όπου τα a_6, a_7 μπορεί να είναι μηδέν

Ορισμός 20 *Για δύο ακολουθίες* $A = [a_1, \cdots, a_n]$ *και* $B = [b_1, \cdots, b_n]$ *μήκους* n*, θα λέμε ότι έχουν διάδοση* $\sigma = \sigma(A, B)$*, αν* $s = \min(\sigma(A), \sigma(B))$*.*

Σημειώνουμε ότι δύο ακολουθίες μήκους n και διάδοσης σ, έχουν n κάθεμια τουλάχιστον σ συνεχόμενα μηδενικά στοιχεία.

Παράδειγμα 21 Τα ακόλουθα ζεύγη ακολουθιών μήκους $n = 7$, έχουν διάδοση $\sigma = 3$:

- $[0, 0, 0, \underbrace{a_4,}_{\neq 0} a_5, a_6, \underbrace{a_7}_{\neq 0}]$ και $[0, 0, 0, 0, \underbrace{b_5,}_{\neq 0} b_6, \underbrace{b_7}_{\neq 0}]$
- $[\underbrace{a_1,}_{\neq 0} 0, 0, 0, \underbrace{a_5,}_{\neq 0} a_6, a_7]$ και $[\underbrace{b_1,}_{\neq 0} 0, 0, 0, 0, \underbrace{b_6,}_{\neq 0} b_7]$

Ορισμός 21 *Για δύο ακολουθίες* $A = [a_1, \cdots, a_n]$ *και* $B = [b_1, \cdots, b_n]$ *μήκους* n *και διάδοσης* σ*, θα λέμε ότι έχουν κανονικοποιημένη διάδοση (spread-normalized) αν η κάθεμια μετατοπίζεται κυκλικά (shifted cyclically) έτσι ώστε το μεγαλύτερο τμήμα συνεχόμενων μηδενικών να εμφανίζεται στις θέσεις* $1, 2, \ldots, \sigma(A)$ *και* $1, 2, \ldots, \sigma(B)$ *για τις* A *και* B *αντίστοιχα.*

Παράδειγμα 22 Τα άκολουθα ζεύγη ακολουθιών μήκους $n = 7$ έχουν κανονικοποιημένη διάδοση $\sigma = 3$:

- $[0, 0, 0, \underbrace{a_4,}_{\neq 0} a_5, a_6, \underbrace{a_7}_{\neq 0}]$ και $[0, 0, 0, 0, \underbrace{b_5,}_{\neq 0} b_6, \underbrace{b_7}_{\neq 0}]$
- $[0, 0, 0, 0, \underbrace{a_5,}_{\neq 0} a_6, \underbrace{a_7}_{\neq 0}]$ και $[0, 0, 0, \underbrace{b_4,}_{\neq 0} b_5, b_6, \underbrace{b_7}_{\neq 0}]$

Υπενθυμίζουμε τον ακόλουθο ορισμό από την [153]:

Ορισμός 22 *Δυο ακολουθίες μήκους* n*, με PAF ή NPAF μηδέν, έχουν τύπο* (u, v) *αν οι ακολουθίες αποτελούνται από δυο μεταβλητές, έστω* a *και* b*, έτσι ώστε το* a *και το* $-a$ *να εμφανίζονται συνολικά* u *φορές, και το* b *και το* $-b$ *να εμφανίζονται συνολικά* v *φορές. Δηλαδή, τα στοιχεία των ακολουθιών παίρνουν τιμές από το σύνολο* $\{a, -a, b, -b\}$*.*

Σημειώνουμε ότι, δύο ακολουθίες τύπου (u, v) μπορούν να χρησιμοποιηθούν ως οι πρώτες γραμμές αντίστοιχων κυκλικών πινάκων στο Θεώρημα 1 για να παράγουν έναν $OD(2n; u, v)$. Για τις ακολουθίες A, B, όπου $A = [a_1, \ldots, a_n]$, ορίζουμε $A \otimes B = [a_1 B, \ldots, a_n B]$, όπου με $a_i B$ θα συμβολίζουμε το βαθμωτό πολλαπλασιασμό (scalar multiplication) και με $A^* = [a_n, \ldots, a_1]$ την αντίστροφη ακολουθία της A.

§3.3.2 Ορθογώνιοι Σχεδιασμοί από Πίνακες Στάθμισης και Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών

Στη συνέχεια, δείχνουμε πώς να συνδυάσουμε ακολουθίες με PAF μηδέν που έχουν διάδοση σ με τριαδικά ζεύγη συμπληρωματικών ακολουθιών έτσι ώστε να παράγουμε νέες κατασκευές για ορθογώνιους σχεδιασμούς. Οι ακολουθίες με PAF μηδέν προέρχονται από $W(2n, 2n-k)$ πίνακες στάθμισης που κατασκευάζονται από δύο κυκλικούς πίνακες. Υπενθυμίζουμε ότι, ένα τριαδικο συμπληρωματικό ζεύγος ακολουθιών (ternary complementary pair) $\mathrm{TCP}(n, w)$, αποτελείται από δύο $\{-1, 0, +1\}$ ακολουθίες A και B μήκους n, που έχουν w μη-μηδενικά στοιχεία συνολικά, και έχουν NPAF μηδέν. Επίσης, από την [36] το στήριγμα μιας ακολουθίας είναι το σύνολο των θέσεων, για τις οποίες τα στοιχεία αυτής είναι μη-μηδενικά. Ένα ζεύγος ακολοθιών θα καλείται ασύνδετο ή ξένο (disjoint) αν το στήριγμα των δύο ακολουθιών είναι ξένο και συνδεδεμένο (conjoint) αν οι δύο ακολουθίες έχουν το ίδιο στήριγμα (αυτό είναι δυνατό μόνον όταν το w είναι άρτιο σε ένα $\mathrm{TCP}(n, w)$).

Θεώρημα 16 *Υποθέτουμε ότι υπάρχει ένας πίνακας στάθμισης $W(2n, 2n-k)$ που κατασκευάζεται από δύο κυκλικούς πίνακες, όπου οι πρώτες τους γραμμές έχουν διάδοση σ. Επίσης, υποθέτουμε ότι υπάρχει ένα ξένο ζεύγος τριαδικών συμπληρωματικών ακολουθιών μήκους σ και βάρους w, δηλαδή ένα $\mathrm{TCP}(\sigma, w)$. Τότε υπάρχει ένας ορθογώνιος σχεδιασμός, $\mathrm{OD}(4n; 2w, 2w, 4n-2k)$.*

Απόδειξη. Έστω C και D οι πρώτες γραμμές των δύο κυκλικών πινάκων που κατασκευάσουν τον $W(2n, 2n-k)$ πίνακα στάθμισης. Φέρνουμε τις C και D σε μορφή κανονικοποιήμενης διάδοσης και καλούμε τις παραγόμενες $\{0, \pm 1\}$ ακολουθίες A και B αντίστοιχα. Πολλαπλασιάζουμε τις A και B με τη μεταβλητή α και παίρνουμε:

$$\begin{aligned} A = [\ \underbrace{0, \cdots, 0,}_{\sigma\ \text{μηδενικά}}\ a_{\sigma+1},\ \cdots,\ a_n] \\ B = [\ \underbrace{0, \cdots, 0,}_{\sigma\ \text{μηδενικά}}\ b_{\sigma+1},\ \cdots,\ b_n] \end{aligned} \qquad (3.13)$$

όπου $a_k, b_k \in \{0, \pm\alpha\}, k = \sigma+1, \ldots, n$ και είτε $a_{\sigma+1} \neq 0$ ή $b_{\sigma+1} \neq 0$.

Στη συνέχεια, συμβολίζουμε τις δύο ακολουθίες μήκους σ με NPAF μηδέν του ξένου $TCP(\sigma, w)$ με $F = [f_1, \cdots, f_\sigma]$ και $G = [g_1, \cdots, g_\sigma]$. Μπορούμε να κατασκευάσουμε τις ακολουθίες $P' = [xF+yG]$ και $Q' = [yF^\star - xG^\star]$ μήκους σ που έχουν NPAF μηδέν και τύπο (w, w). Οι ακολουθίες $P' = [p_1, \cdots, p_\sigma] = [xf_1 + yg_1, \cdots, xf_\sigma + yg_\sigma]$ και $Q' = [q_1, \cdots, q_\sigma] = [yf_\sigma - xg_\sigma, \cdots, yf_1 - xg_1]$ μπορούν να χρησιμοποιηθούν στο Θεώρημα 1 για να παράγουν έναν $OD(2\sigma; w, w)$. Τότε ο ζητούμενος $OD(4n; 2w, 2w, 4n - 2k)$ μπορεί να κατασκευαστεί σχηματίζοντας τους τέσσερις κυκλικού πίνακες που έχουν πρώτες γραμμές P, Q, R, S όπως παρακάτω, που στη συνέχεια χρησιμοποιούνται στο σχηματισμό Goethals-Seidel.

$$\begin{array}{lcccccccc} P = [& p_1, & p_2, & \cdots, & p_\sigma, & a_{\sigma+1}, & \cdots, & a_n] \\ Q = [& -p_1, & -p_2, & \cdots, & -p_\sigma, & a_{\sigma+1}, & \cdots, & a_n] \\ R = [& q_1, & q_2, & \cdots, & q_\sigma, & b_{\sigma+1}, & \cdots, & b_n] \\ S = [& -q_1, & -q_2, & \cdots, & -q_\sigma, & b_{\sigma+1}, & \cdots, & b_n] \end{array} \qquad (3.14)$$

Οι ακολουθίες P, Q, R, S έχουν PAF μηδέν. Αυτό συμβαίνει διότι, οποιαδήποτε γινόμενα τα οποία προκύπτουν στο PAF της P από τα στοιχεία της P' με τα στοιχεία της ακολουθίας $[a_{\sigma+1}, \cdots, a_n]$ διαγράφονται στο PAF της Q από τα γινόμενα των στοιχείων της $-P'$ με τα στοιχεία της ακολουθίας $[a_{\sigma+1}, \cdots, a_n]$. Ομοίως για την Q' και την ακολουθία $[b_{\sigma+1}, \cdots, b_n]$ στις R και S. Το άθροισμα των γινομένων των στοιχείων της ακολουθίας $[a_{\sigma+1}, \cdots, a_n]$ με τα γινόμενα των στοιχείων της ακολουθίας $[b_{\sigma+1}, \cdots, b_n]$ είναι ίσο με μηδέν στο PAF των P, Q, R, S, καθώς οι ακολουθίες A και B έχουν PAF μηδέν. Ομοίως για το άθροισμα των γινομένων των στοιχείων της ακολουθίας P' με τα γινόμενα των στοιχείων της Q' στο PAF των P, Q, R, S, καθώς αυτές οι ακολουθίες έχουν NPAF μηδέν. Αυτό δίνει και τον ζητούμενο $OD(4n; 2w, 2w, 4n - 2k)$.

□

Στη συνέχεια περιγράφουμε την εφαρμογή του Θεωρήματος 16 με το ακόλουθο παράδειγμα:

Παράδειγμα 23 Έστω $n = 11$, $k = 13$ και θεωρούμε ένα πίνακα στάθμισης κανονικοποιημένης διάδοσης $W(2 \cdot 11, 2 \cdot 11 - 13) = W(2 \cdot 11, 9)$ που κατασκευάζεται από δύο κυκλικούς πίνακες και έχει $\sigma = 2$

```
A = [0, 0, 0, 0,  0, 1, 0, -1, 0, -1, 1]
B = [0, 0, 1, 0, -1, 0, 0,  1, 0,  1, 1]
```

Σημειώνουμε ότι, $\sigma = \min(s(A), s(B)) = \min(5, 2) = 2$. Πολλαπλασιάζουμε τις A και B με τη μεταβλητή α και παίρνουμε:

$$\begin{aligned} A &= [0,\ 0,\ 0,\ 0,\ \ 0,\ \alpha,\ 0,\ -\alpha,\ 0,\ -\alpha,\ \alpha] \\ B &= [0,\ 0,\ \alpha,\ 0,\ -\alpha,\ 0,\ 0,\ \ \alpha,\ 0,\ \ \alpha,\ \alpha] \end{aligned}$$

Στη συνέχεια θεωρούμε το ξένο τριαδικό συμπληρωματικό ζεύγος ακολουθιών μήκους $\sigma = 2$, βάρους $w = 2$ με NPAF μηδέν να είναι:

$$F = [1, 0] \quad \text{και} \quad G = [0, 1].$$

Τότε οι αντίστροφες ακολουθίες $F^\star$ και $G^\star$ των F και G είναι:

$$F^\star = [0, 1] (= G) \quad \text{και} \quad G^\star = [1, 0] (= F).$$

Οι ακολουθίες $P' = [xF + yG]$ και $Q' = [yF^\star - xG^\star]$ που έχουν NPAF μηδέν είναι:

$$P' = [x, y] \quad \text{ανδ} \quad Q' = [-x, y].$$

Τότε, οι ακολουθίες P, Q, R, S που θα έχουν PAF μηδέν είναι οι:

$$\begin{aligned} P &= [\ \ x,\ \ \ y,\ \ 0,\ 0,\ \ 0,\ \alpha,\ 0,\ -\alpha,\ 0,\ -\alpha,\ \alpha] \\ Q &= [\ -x,\ -y,\ \ 0,\ 0,\ \ 0,\ \alpha,\ 0,\ -\alpha,\ 0,\ -\alpha,\ \alpha] \\ R &= [\ -x,\ \ y,\ \ \alpha,\ 0,\ -\alpha,\ 0,\ 0,\ \ \alpha,\ 0,\ \ \alpha,\ \alpha] \\ S &= [\ \ x,\ -y,\ \ \alpha,\ 0,\ -\alpha,\ 0,\ 0,\ \ \alpha,\ 0,\ \ \alpha,\ \alpha] \end{aligned}$$

και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για την κατασκευή ενός $OD(4n; 2w, 2w, 4n - 2k)$, δηλαδή, ενός $OD(44; 4, 4, 18)$.

Παρατήρηση 10 *Σημειώνουμε ότι μπορούμε να γενικεύσουμε το Θεώρημα 16 αφαιρώντας την υπόθεση του ξένου TCP, καθώς μπορούμε πάντα να κατασκευάσουμε ένα ξένο TCP από ένα γνωστό ζεύγος με μετατόπιση του τελευταίου. Αυτή η ιδιότητα περιγράφεται με το ακόλουθο παράδειγμα.*

Παράδειγμα 24 Έστω $n = 15$, $k = 21$ και θεωρούμε ένα πίνακα στάθμισης κανονικοποιημένης διάδοσης $W(2\cdot 15, 2\cdot 15-21) = W(2\cdot 15, 9)$ που κατασκευάζεται από δύο κυκλικούς πίνακες και έχει $\sigma = 5$

```
A = [0, 0, 0, 0, 0, 0, -1, 1, 0,  0, 0, 1, 0, 1,  1]
B = [0, 0, 0, 0, 0, 1,  0, 0, 0, -1, 0, 0, 1, 0, -1]
```

Σημειώνουμε ότι, $\sigma = \min(s(A), s(B)) = \min(6, 5) = 5$. Πολλαπλασιάζουμε τις A και B με τη μεταβλητή α και παίρνουμε:

$$A = [0,\ 0,\ 0,\ 0,\ 0,\ 0,\ -\alpha,\ \alpha,\ 0,\ 0,\ 0,\ \alpha,\ 0,\ \alpha,\ \alpha]$$
$$B = [0,\ 0,\ 0,\ 0,\ 0,\ \alpha,\ 0,\ 0,\ 0,\ -\alpha,\ 0,\ 0,\ \alpha,\ 0,\ -\alpha]$$

Στη συνέχεια, θεωρούμε το τριαδικό συμπληρωματικό ζεύγος ακολουθιών μήκους $\sigma' = 3 < 5 = \sigma$, βάρους $w = 4$ με NPAF μηδέν να είναι:

$$F' = [1, 0, 1] \quad \text{και} \quad G' = [1, 0, -1].$$

Προσθέτοντας ένα μηδενικό στο τέλος κάθε ακολουθίας και μετατοπίζοντας κυκλικά (cyclically shifting) τη G' [36], κατασκευάζουμε το ακόλουθο ξένο $TCP(4, 4)$, $[1, 0, 1, 0]; [0, 1, 0, -1]$. Σημειώνουμε ότι η παράθεση μηδενικών σε NPAF ακολουθίες, δεν αλλάζει τα πρόσημα του NPAF, και ότι η πράξη της μετατόπισης είναι ένας ισοδύναμος μετασχηματισμός για TCP ([36]). Καθώς, η κατασκευή του Θεωρήματος 16 απαιτεί η διάδοση των δύο αρχικών ακολουθιών να είναι ίση με το μήκος του τριαδικού συμπληρωματικού ζεύγους ακολουθιών, παραθέτουμε στο τέλος του προηγουμένως παραγόμενου TCP ένα επιπλέον μηδενικό. Συνεπώς, μπορούμε να κατασκευάσουμε το ακόλουθο ξένο τριαδικό συμπληρωματικό ζεύγος ακολουθιών μήκους $\sigma = 5$ και βάρους $w = 4$:

$$F = [1, 0, 1, 0, 0] \quad \text{και} \quad G = [0, 1, 0, -1, 0].$$

Τότε, οι αντίστροφες ακολουθίες $F^\star$ και $G^\star$ των F και G είναι:

$$F^\star = [0, 0, 1, 0, 1] \quad \text{και} \quad G^\star = [0, -1, 0, 1, 0].$$

Στη συνέχεια, θεωρούμε τις ακολουθίες $P' = [xF + yG]$ και $Q' = [yF^\star - xG^\star]$ με NPAF μηδέν να είναι:

$$P' = [x, y, x, -y, 0] \quad \text{και} \quad Q' = [0, x, y, -x, y].$$

Παράδειγμα 25 (Συνέχεια του Παραδείγματος 24) Τότε, οι επιθυμητές ακολουθίες P, Q, R, S που θα έχουν PAF μηδέν θα είναι οι:

$$\begin{array}{lllllllllllllll} P & = [& x, & y, & x, & -y, & 0, & 0, & -\alpha, & \alpha, & 0, & 0, & 0, & \alpha, & 0, & \alpha, & \alpha] \\ Q & = [& -x, & -y, & -x, & y, & 0, & 0, & -\alpha, & \alpha, & 0, & 0, & 0, & \alpha, & 0, & \alpha, & \alpha] \\ R & = [& 0, & x, & y, & -x, & y, & \alpha, & 0, & 0, & 0, & -\alpha, & 0, & 0, & \alpha, & 0, & -\alpha] \\ S & = [& 0, & -x, & -y, & x, & -y, & \alpha, & 0, & 0, & 0, & -\alpha, & 0, & 0, & \alpha, & 0, & -\alpha] \end{array}$$

και μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel για την κατασκευή ενός $OD(4n; 2w, 2w, 4n - 2k)$, δηλαδή, ενός $OD(60; 8, 8, 18)$.

§3.4 Ένα Νέο Κριτήριο Αποδοτικότητας για Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών

Για να είμαστε σε θέση να αποδείξουμε παρόμοια αποτελέσματα με αυτά του Θεωρήματος 16, εισάγουμε για πρώτη φόρα το κριτήριο της *ζ-αποδοτικότητας (ζ-efficiency)* για ένα τριαδικό συμπληρωματικό ζεύγος ακολουθιών, βασιζόμενοι σε μια ελαφρά παραλλαγή του ορισμού της μετατόπισης των TCP που δίνεται στην [36].

Ορισμός 23 *Μετατόπιση (shifting) για δοθέν TCP είναι η διαδικασία παράθεσης μηδενικών στο τέλος και των δύο ακολουθιών, και η κυκλική μετάθεση αυτών μέχρι το ζεύγος (ακολουθιών) να γίνει ξένο.*

Ορισμός 24 *Ορίζουμε ως ζ-αποδοτικότητα (ζ-efficiency) ενός τριαδικού συμπληρωματικού ζεύγους ακολουθιών* $\mathrm{TCP}(n, w)$ *και θα τη συμβολίζουμε με ζ, τον ελάιστο αριθμό μηδενικών που απαιτούνται έτσι ώστε να μετασχηματίσουμε ένα δοθέν* $\mathrm{TCP}(n, w)$ *σε ένα ξένο* $\mathrm{TCP}(n', w)$ *με τη διαδικασία της μετατόπισης, όπου* $n' \geq n$*, δηλαδή* $n' = n + \zeta$.

Μπορούμε στη συνέχεια, να αποδείξουμε το ακόλουθο θεώρημα.

Θεώρημα 17 *Υποθέτουμε ότι, υπάρχει ένας πίνακας στάθμισης* $W(2n, 2n - k)$ *που κατασκευάζεται από δύο κυκλικούς πίνακες, όπου οι πρώτες τους γραμμές έχουν διάδοση* σ*. Επίσης, υποθέτουμε ότι υπάρχει ένα τριαδικό συμπληρωματικό ζεύγος ακολουθιών μήκους* σ' *και βάρους* w*, δηλαδή ένα* $\mathrm{TCP}(\sigma', w)$ *με ζ-αποδοτικότητα ίση με ζ. Αν ισχύει,* $\sigma' + \zeta \leq \sigma$ *τότε υπάρχει ένας ορθογώνιος σχεδιασμός,* $OD(4n; 2w, 2w, 4n - 2k)$.

Απόδειξη. Αρκεί να κατασκευάσουμε τις ξένες ακολουθίες F και G της απόδειξης του Θεωρήματος 16. Θεωρούμε τις δύο ακολουθίες μήκους σ' με NPAF μηδέν του $\mathrm{TCP}(\sigma', w)$. Καθώς, το $\mathrm{TCP}(\sigma', w)$ έχει ζ-αποδοτικότητα ίση με ζ με τη διαδικασία της μετατόπισης παράγουμε ένα ξένο $\mathrm{TCP}(\sigma' + \zeta, w)$. Μετέπειτα, παραθέτουμε στις ακολουθίες, που παρήγαμε από τη μετατόπιση, $\sigma - (\sigma' + \zeta)$ μηδενικά. Η υπόλοιπη απόδειξη είναι όμοια με αυτή του Θεωρήματος 16.

□

Στη συνέχεια, μελετούμε ορισμένες βασικές ιδιότητες της ζ-αποδοτικότητας για τα TCP. Στο συνδυαστικό χώρο των TCP οι δύο ακραίες περιπτώσεις, είναι τα ξένα TCP και τα συνδεδεμένα. Προφανώς, από τον ορισμό της ζ-αποδοτικότητας ένα ξένο TCP έχει $\zeta = 0$. Μελετούμε αυτές τις δύο περιπτώσεις, παρακάτω.

Λήμμα 3 *Η ζ-αποδοτικότητα ενός ξένου* $\mathrm{TCP}(n, w)$ *είναι ίση με μηδέν, δηλαδή* $\zeta = 0$.

Απόδειξη. Καθώς το δοθέν $\mathrm{TCP}(n, w)$ είναι ξένο, δεν χρειάζεται να παραθέσουμε επιπλέον μηδενικά στο τέλος των δύο ακολουθιών, συνεπώς ο αριθμός των επιπλέον μηδενικών που χρειάζεται να προστεθούν είναι ίσος με 0.

□

Λήμμα 4 *Έστω* $F; G$ *ένα συνδεδεμένο* $\mathrm{TCP}(n, w)$. *Ας συμβολίσουμε με* S_t *το στήριγμα του συνδεδεμένου* $\mathrm{TCP}(n, w)$, *και έστω* $|S_t| = t$. *Τότε, η ζ-αποδοτικότητα του συνδεδεμένου* $\mathrm{TCP}(n, w)$ *είναι πάνω φραγμένη από* t, *δηλαδή* $\zeta \leq t = \frac{w}{2}$.

Απόδειξη. Καθώς οι F και G έχουν το ίδιο στήριγμα, τα t μη-μηδενικά στοιχεία βρίσκονται στις ίδιες θέσεις στις δύο ακολουθίες. Παραθέτοντας στο τέλος και των δύο ακολουθιών t μηδενικά και μετατοπίζοντας τις κυκλικά, τις μετασχηματίζουμε σε ξένες. Καθώς, η ζ-αποδοτικότητα είναι ο ελάχιστος αριθμός των μηδενικών που χρειάζεται να παρατεθούν, η ύπαρξη κατάλληλων τμημάτων από μηδενικά στις F και G μπορεί να απαιτεί να προστεθούν λιγότερα από t μηδενικά. Συνεπώς, έχουμε ότι $\zeta \leq t$. Καθώς, το βάρος w είναι ο αριθμός των μη-μηδενικών στοιχείων που συμβαίνουν και στις δύο ακολουθίες έχουμε ότι $w = 2t$ και $\zeta \leq \frac{w}{2}$.

□

Τα προηγούμενα λήμματα υποδεικνύουν ότι η ζ-αποδοτικότητα μπορεί να θεωρηθεί ως ένα επιπλέον κριτήριο του πόσο κοντά βρίσκεται

ένα δοθέν TCP στην ισοδύναμη ξένη μορφή του. Παρόλο, πού όπως αναφέρεται στην [36] κάθε TCP είναι ισοδύναμο με ένα ξένο TCP, ενώ ένα δοθέν TCP μπορεί να είναι ή να μην είναι ισοδύναμο με ένα συνδεδεμένο TCP, δεν υπάρχει κάποια κλειστή σχέση ως προς το πως μπορεί να επιτευχθεί αυτό. Συνεπώς, χρειαζόμαστε καλύτερα και πιο γενικά φράγματα για τη ζ-αποδοτικότητα, καθώς και περιορισμούς όταν το ζ είναι μικρό. Αυτο μπορεί να επιτευχθεί συσχετίζοντας τη ζ-αποδοτικότητα με τη μη-αποδοτικότητα (deficiency) ([36]), δ, ενός $\mathsf{TCP}(n, w)$ που ορίζεται ως $\delta = 2n - w$, δηλαδή είναι ο αριθμός των μηδενικών που συμβαίνουν και στις δύο ακολουθίες.

Είναι αρκετά γνωστό ότι για δοθέν ξένο $\mathsf{TCP}(n, w)$, μπορούμε να διπλασιάσουμε το βάρος αυτού του ζεύγους (Λήμμα 11, [36]) και να παράγουμε ένα συνδεδεμένο TCP. Επαναδιατυπώνουμε αυτό το αποτέλεσμα, κάνοντας χρήση του κριτηρίου της ζ-αποδοτικότητας για κάθε $\mathsf{TCP}(n, w)$.

Λήμμα 5 *Έστω* $\mathsf{F}; \mathsf{G}$ *ένα* $\mathsf{TCP}(n, w)$ *με ζ-αποδοτικότητα ίση με ζ. Τότε, υπάρχει ένα συνδεδεμένο* $\mathsf{TCP}(n + \zeta, 2w)$.

Απόδειξη. Καθώς, το δοθέν $\mathsf{TCP}(n, w)$ έχει ζ-αποδοτικότητα ίση με ζ, τότε υπάρχει ένα ξένο TCP μήκους $n + \zeta$ και βάρους w που παράγεται με μετατόπιση. Στη συνέχεια, από το Λήμμα 11 της [36], μπορούμε να κατασκευάσουμε ένα συνδεδεμένο $\mathsf{TCP}(n + \zeta, 2w)$.

□

§3.4.1 ζ-Αποδοτικότητα για Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών όταν η Μη-Αποδοτικότητα, δ, είναι Μικρή

Αναμένεται πως όταν η μη-αποδοτικότητα, δ, ενός TCP είναι μικρή, τότε η ζ-αποδοτικότητα θα πρέπει να είναι αρκετά μεγάλη. Είναι ενδιαφέρον να εκτιμήσουμε τις ακριβές τιμές της ζ για συγκεκριμένες τιμές της δ.

Είδαμε νωρίτερα ότι μια από τις χειρότερες περιπτώσεις για τη ζ-αποδοτικότητα συμβαίνει στα συνδεδεμένα TCP. Το ερώτημα όμως είναι αν αυτή είναι η χείριστη περίπτωση. Αν υποθέσουμε ότι $\delta = 0$ τότε

έχουμε ότι οι ακολουθίες που συνθέτουν το TCP, είναι στην πραγματικότητα ακολουθίες Golay, που συμβολίζονται με $GS(n)$ για μήκος n. Προφανώς, αυτές οι ακολουθίες έχουν το ίδιο στήριγμα και συνεπώς μπορούν να θεωρηθούν ως ένα συνδεδεμένο TCP. Η ζ-αποδοτικότητα σε αυτήν την περίπτωση είναι ακριβώς το πάνω φράγμα που δίνεται στο Λήμμα 4, όπως ήταν αναμενόμενο.

Λήμμα 6 *Έστω* $F; G$ *να είναι ένα* $TCP(n, 2n) = GS(n)$. *Τότε, αυτό έχει ζ-αποδοτικότητα ίση με* n, *δηλαδή* $\zeta = n$.

Απόδειξη. Το δοθέν TCP είναι συνδεδεμένο με $\delta = 0$. Πρέπει να παραθέσουμε την ακολουθία 0_n των n συνεχόμενων μηδενικών σε κάθε ακολουθία F και G και να εφαρμόσουμε τη διαδικασία της μετατόπισης για να παράγουμε το ξένο $TCP(n+n, 2n)$, $[F, 0_n]; [0_n, G]$. Καθώς, ο αριθμός των μηδενικών που προστίθενται είναι n, έχουμε ότι το $TCP(n, 2n)$ έχει ζ-αποδοτικότητα ίση με n.

□

Είναι γνωστό από την [55], ότι η περίπτωση $\delta = 1$ συμβαίνει μόνο για $TCP(1, 1)$ ή $TCP(3, 5)$.

Λήμμα 7 *Έστω* $F; G$ *ένα* $TCP(n, 2n-1)$. *Τότε, αυτό έχει ζ-αποδοτικότητα ίση με* ζ, *όπου* $\zeta = 0$ *ή* $\zeta = 3$.

Απόδειξη. Έχουμε δύο περιπτώσεις για $\delta = 1$. Η πρώτη είναι για το τετριμμένο $TCP(1, 1)$ που δίνεται από $1; 0$. Καθώς, αυτό το TCP είναι ξένο έχουμε ότι έχει ζ-αποδοτικότητα ίση με μηδέν. Η άλλη περίπτωση είναι το $TCP(3, 5)$ που δίνεται από τις $[1, 0, 1]; [1, 1, -1]$ (λαμβάνοντας υπόψιν την ισοδυναμία). Η απουσία μηδενικών στη δεύτερη ακολουθία απαιτεί ότι πρέπει να προστεθούν τουλάχιστον τρία μηδενικά στο τέλος κάθε ακολουθίας, έτσι ώστε το TCP που θα παραχθεί μέσω της διαδικασίας της μετατόπισης να είναι ξένο. Συνεπώς, έχει ζ-αποδοτικότητα ίση με $\zeta = 3$.

□

§3.4.2 ζ-Αποδοτικότητα για Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών Δοθείσας Μη-Αποδοτικότητας δ

Καθώς, έχουμε ένα μέτρο για τον αριθμό των μηδενικών που συμβαίνουν σε ένα TCP, τη μη-αποδοτικότητα, μπορούμε να εξάγουμε το ακόλουθο φράγμα για τη ζ-αποδοτικότητα.

Λήμμα 8 *Για δοθέν* $\mathsf{TCP}(n, w)$*, η ζ-αποδοτικότητα του είναι κάτω φραγμένη από* $w - n$*, δηλαδή* $\zeta \geq w - n$*.*

Απόδειξη. Για να έχουμε ένα ζεύγος ακολουθιών $A; B$ όπου το στήριγμα τους είναι ξένο, και αυτό συνθέτει το $\mathsf{TCP}(n, w)$, θα πρέπει να εμφανίζονται τμήματα $[a_i; b_i]$ στις ακολουθίες $A; B$ όπου τουλάχιστον ένα από τα a_i ή b_i είναι μηδέν. Συνεπώς, ο ελάχιστος αριθμός των μηδενικών που πρέπει να προστεθούν στις δύο ακολουθίες και μετέπειτα να εφαρμοστεί η διαδικασία της μετατόπισης είναι τουλάχιστον $\zeta \geq n - \delta$, όπου $\delta = 2n - w$ είναι η μη-αποδοτικότητα του TCP. Με αντικατάσταση, έχουμε $\zeta \geq n - (2n - w)$ και παίρνουμε το επιθυμητό αποτέλεσμα.

□

Προφανώς, το προηγούμενο φράγμα δεν είναι πάντα ακριβές ή οξύ (sharp). Η παρουσία πιθανών τμημάτων από μηδενικά $[0; 0]$ στις ίδιες θέσεις, απαιτεί την προσθήκη επιπλέον μηδενικών. Αυτή η εξαίρεση, μπορεί να μελετηθεί καλύτερα αν θεωρήσουμε τις μη-αποδοτικότητες των ακολουθιών, ξεχωριστά σε κάθε περίπτωση.

Παρατήρηση 11 *Έχουμε ότι,* $\zeta + \delta \geq n$*. Αυτό το φράγμα είναι ακριβές, στην περίπτωση των συνδεδεμένων TCP με μηδενική μη-αποδοτικότητα (βλ. Λήμμα 6). Σε αυτή την περίπτωση, έχουμε δύο συμπληρωματικά κριτήρια που αθροίζουν στο μήκος* n*.*

Παρατήρηση 12 *Στην περίπτωση όπου το δοθέν* $\mathsf{TCP}(n, w)$ *είναι ξένο, συνεπώς* $\zeta = 0$ *έχουμε ότι* $n \geq w$*, δηλαδή ακολουθίες που έχουν* w *μη-μηδενικά στοιχεία πρέπει να αναζητηθούν σε μήκη μεγαλύτερα ή ίσα του* w*, έτσι ώστε αυτές να είναι ξένες.*

§3.4.3 Πίνακες στάθμισης από Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών Δοθείσας Αποδοτικότητας ζ

Εφόσον, έχουμε επιτύχει ένα φράγμα για τη ζ-αποδοτικότητα, θα ήταν επιθυμητή μια κατασκευή για ορθογώνιους σχεδιασμούς ή πίνακες στάθμισης n οποία θα περιλαμβάνει ξένα TCP. Με $\mathbb{N} = \{0, 1, 2, \ldots\}$ συμβολίζουμε το σύνολο των φυσικών αριθμών για το υπόλοιπο αυτού του κεφαλαίου. Είναι αρκετά γνωστή, η ύπαρξη των ακολούθων κατασκευών (απεικονίσεων) για TCP και πίνακες στάθμισης:

1. $\mathrm{TCP}(n, w) \rightarrow W(2n, w)$ (Χρησιμοποιούμε τις δύο ακολουθίες του TCP στην κατασκευή του Θεωρήματος 1).
2. $\mathrm{TCP}(n, w) \rightarrow \mathrm{TCP}(n + k, w), k \in \mathbb{N}$ (παραθέτοντας μηδενικά στο τέλος των ακολουθιών ενός TCP, δεν μεταβάλλονται τα πρόσημα του NPAF).
3. $\mathrm{TCP}(m, w) \times \mathrm{TCP}(n, z) \rightarrow \mathrm{TCP}(mn, wz)$, αν ένα από τα ζεύγη ακολουθιών είναι ξένο (πολλαπλασιαστική μέθοδος των TCP, βλ. Θεώρημα 14 της [36]).

Λήμμα 9 *Έστω ένα* $\mathrm{TCP}(n, w)$ *με* ζ*-αποδοτικότητα ίση με* ζ*. Τότε, υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις):*

(i) $\mathrm{TCP}(n, w) \rightarrow \mathrm{TCP}(n^2 + n\zeta, w^2)$.

(ii) $\mathrm{TCP}(n, w) \rightarrow \mathrm{TCP}(n^2 + n\zeta + k, w^2), k \in \mathbb{N}$.

(iii) $\mathrm{TCP}(n, w) \rightarrow W(2n^2 + 2n\zeta + 2k, w^2), k \in \mathbb{N}$.

Απόδειξη.

(i) Μπορούμε να κατασκευάσουμε ένα ξένο $\mathrm{TCP}(n + \zeta, w)$ από δοθέν $\mathrm{TCP}(n, w)$. Εφαρμόζοντας αυτά τα δύο ζεύγη ακολουθιών στην κατασκευή 3 έχουμε ότι $\mathrm{TCP}(n, w) \times \mathrm{TCP}(n + \zeta, w) \rightarrow \mathrm{TCP}(n(n + \zeta), w^2)$.

(ii) Εφαρμόζουμε την κατασκευή 2 στα αποτελέσματα του (i) ερωτήματος.

(iii) Εφαρμόζουμε την κατασκευή 1 στα αποτελέσματα του (ii) ερωτήματος.

□

Εικασία 1 (Εικασία 2, [36]) *Αν ένα* $\mathrm{TCP}(n, w)$ *υπάρχει και* $p \mid w$*, τότε υπάρχει και ένα* $\mathrm{TCP}(m, p)$*, για κάποιο* m*.*

Είναι ενδιαφέρον, να εξετάσουμε το αντίστροφο του Λήμματος 9, που δίνεται παρακάτω, και μπορεί να θεωρηθεί επίσης ως ειδική περίπτωση της Εικασίας 1, για τετραγωνικά βάρη.

Ερευνητικό Πρόβλημα 4 *Ποιο είναι το ελάχιστο μήκος* m*, για το οποίο αποδεικνύεται η ύπαρξη ενός* $\mathrm{TCP}(m, w^2)$*.*

Όπως αναφέρεται στην [36], ένας προφανής τρόπος απόδειξης αυτής της εικασίας θα περιλάμβανε να δείξουμε ότι, αν το w είναι σύνθετο (composite), τότε ένα $\mathrm{TCP}(n, w)$ πρέπει να παραγοντοποιείται μέσω της πολλαπλασιαστικής μεθόδου των TCP. Καθώς, αυτή η εικασία στη γενική της περίπτωση είναι ακόμα ανοιχτή, αποτελέσματα που υποδεικνύουν το αληθές αυτής δόθηκαν στην [37]. Στην περίπτωση μας, προφανώς ισχύει $w = p \mid w^2$ και $m \leq n^2 + n\zeta$ από το Λήμμα 9. Επιπλεόν, θεωρώντας το κάτω φράγμα της ζ-αποδοτικότητας, μπορούμε επιπλέον να συμπεράνουμε το ακόλουθο:

$$\zeta \geq w - n \Rightarrow n\zeta \geq nw - n^2 \Rightarrow n^2 + n\zeta \geq nw$$

Αυτό το αποτέλεσμα, μας υποδεικνύει ότι από δοθέν $\mathrm{TCP}(n, w)$ για να είμαστε σε θέση να κατασκευάσουμε ένα TCP με τετράγωνο βάρος, δηλαδή ένα $\mathrm{TCP}(m, w^2)$, θα πρέπει να αναζητήσουμε NPAF ακολουθίες που έχουν μήκος m τουλάχιστον ίσο με nw.

Ελάχιστα Μήκη Τριαδικών Συμπληρωματικών Ζευγών Ακολουθιών με Γνωστά Τετράγωνα Βάρη Η ύπαρξη των TCP, είναι ένα από τα πιο σημαντικά προβλήματα στη Θεωρία των TCP. Αν θεωρήσουμε την ταξινόμηση των TCP κατά βάρος (βλ. [36, 37, 38]), μας ενδιαφέρει το ελάχιστο μήκος για το οποίο υπάρχει ένα TCP με γνωστό βάρος.

Έχουμε ήδη αποδείξει ότι ένα $\mathrm{TCP}(n, w)$ υποδηλώνει την ύπαρξη ενός $\mathrm{TCP}(n^2 + n\zeta, w^2)$. Καθώς, το επιχείρημά μας είναι κατασκευαστικό θα συγκρίνουμε το κάτω φράγμα $m = n^2 + n\zeta$ για τετράγωνα βάρη w εώς το 100 με τα τωρινά ελάχιστα μήκη r γνωστών TCP που έχουν αυτά τα βάρη. Υπάρχουν $\mathrm{TCP}(r, w^2)$ για $(r, w^2) \in S$ όπου $S = \{(2, 4), (8, 16), (18, 25), (32, 64)\}$, βλ. [36].

Πρόταση 12 *Έστω ένα* $\mathrm{TCP}(r, w^2)$ *για* $(r, w^2) \in S$. *Τότε το φράγμα* $m \geq n^2 + n\zeta$ *είναι ακριβές, δηλαδή* $m = r$. *Ιδιαίτερα, υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για* $\mathrm{TCP}(n^2 + n\zeta, w^2)$*:*

(i) $\mathrm{TCP}(1, 2) \rightarrow \mathrm{TCP}(2, 4)$

(ii) $\mathrm{TCP}(2, 4) \rightarrow \mathrm{TCP}(8, 16)$

(iii) $\mathrm{TCP}(3, 5) \rightarrow \mathrm{TCP}(18, 25)$

(iv) $\mathrm{TCP}(4, 8) \rightarrow \mathrm{TCP}(32, 64)$

Απόδειξη.

(i) Υπάρχει ένα $\mathrm{TCP}(1, 2) = \mathrm{GS}(1)$ (βλ. Πίνακα I της [36]). Από το Λήμμα 6 αυτό έχει $n = \zeta = 1$, και από το Λήμμα 9 μπορούμε να κατασκευάσουμε ένα $\mathrm{TCP}(n^2 + n\zeta, 4) = \mathrm{TCP}(2, 4)$.

(ii) Υπάρχει ένα $\mathrm{TCP}(2, 4) = \mathrm{GS}(2)$ (βλ. Πίνακα II της [36]). Από το Λήμμα 6 αυτό έχει $n = \zeta = 2$, και από το Λήμμα 9 μπορούμε να κατασκευάσουμε ένα $\mathrm{TCP}(n^2 + n\zeta, 16) = \mathrm{TCP}(8, 16)$.

(iii) Υπάρχει ένα $\mathrm{TCP}(3, 5)$ (βλ. Πίνακα I της [36]). Από το Λήμμα 7 αυτό έχει $n = \zeta = 3$, και από το Λήμμα 6 μπορούμε να κατασκευάσουμε ένα $\mathrm{TCP}(n^2 + n\zeta, 25) = \mathrm{TCP}(18, 25)$.

(iv) Υπάρχει ένα $\mathrm{TCP}(4, 8) = \mathrm{GS}(4)$ (βλ. Πίνακα II της [36]). Από το Λήμμα 6 αυτό έχει $n = \zeta = 4$, και από το Λήμμα 9 μπορούμε να κατασκευάσουμε ένα $\mathrm{TCP}(n^2 + n\zeta, 64) = \mathrm{TCP}(32, 64)$.

□

Άπειρες Κλάσεις Πινάκων Στάθμισης από Τριαδικά Συμπληρωματικά Ζεύγη Ακολουθιών Ως εφαρμογή, δίνουμε τις παρακάτω οικογένειες από πίνακες στάθμισης, $W(2n^2 + 2n\zeta + 2k, w^2), k \in \mathbb{N}$, που παράγονται μέσω της θεωρίας που έχουμε αναπτύξει εώς τώρα.

Πόρισμα 20 *Υπάρχουν άπειρες οικογένειες από πίνακες στάθμισης για τις ακόλουθες περιπτώσεις:*

(i) $W(4 + 2k, 4), k \in \mathbb{N}$.

(ii) $W(16 + 2k, 16), k \in \mathbb{N}$.

(iii) $W(36 + 2k, 25), k \in \mathbb{N}$.

(iv) $W(64 + 2k, 64), k \in \mathbb{N}$.

Απόδειξη. Συνδυάζοντας τις κατασκευές του Λήμματος 9 με τα αποτελέσματα της Πρότασης 12 υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις):

(i) $\mathrm{TCP}(1,2) \to \mathrm{TCP}(2,4) \to \mathrm{TCP}(2+k,4) \to W(4+2k,4), k \in \mathbb{IN}$.

(ii) $\mathrm{TCP}(2,4) \to \mathrm{TCP}(8,16) \to \mathrm{TCP}(8+k,16) \to W(16+2k,16), k \in \mathbb{IN}$.

(iii) $\mathrm{TCP}(3,5) \to \mathrm{TCP}(18,25) \to \mathrm{TCP}(18+k,25) \to W(36+2k,25), k \in \mathbb{IN}$.

(iv) $\mathrm{TCP}(4,8) \to \mathrm{TCP}(32,64) \to \mathrm{TCP}(32+k,64) \to W(64+2k,64), k \in \mathbb{IN}$.

□

Στο πεδίο της Συνδυαστικής Θεωρίας Σχεδιασμών είναι συνήθες να αναζητούμε κατασκευές για πίνακες στάθμισης $W(n,k)$, οι οποίες πολλαπλασιάζουν το μήκος n και/ή το βάρος k με έναν παράγοντα λ. Δίνουμε μια κατασκευή για $\lambda = 4$, χρησιμοποιώντας τα TCP και το κριτήριο της ζ-αποδοτικότητας.

Θεώρημα 18 *Έστω* $\mathrm{TCP}(n,w)$ *με* ζ*-αποδοτικότητα ίση με* ζ*, τότε υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για πίνακες στάθμισης:*

(i) $\mathrm{TCP}(n,w) \to W(4n',4w)$, $n' = n+\zeta$.

(ii) $\mathrm{TCP}(n,w) \to W(4n'+2k,4w)$, $n' = n+\zeta, k \in \mathbb{IN}$.

Απόδειξη.

(i) Για κάθε $\mathrm{TCP}(n,w)$ μπορούμε να κατασκευάσουμε ένα ξένο ζεύγος ακολουθιών που συνθέτουν ένα $\mathrm{TCP}(n',w)$, όπου $n' = n+\zeta$. θεωρώντας το συνδεδεμένο $\mathrm{TCP}(2,4) = \mathrm{GS}(2)$, εφαρμόζουμε αυτά τα ζεύγη ακολουθιών στην κατασκευή 3, δηλαδή $\mathrm{TCP}(n',w) \times \mathrm{TCP}(2,4) \to \mathrm{TCP}(2n',4w)$. Εφαρομόζοντας την κατασκευή 1. έχουμε ότι$\mathrm{TCP}(2n',4w) \to W(4n',4w)$.

(ii) Εφαρμόζουμε την κατασκευή 2. στο $\mathrm{TCP}(2n',4w)$ του (i) ερωτήματος και στη συνέχεια θεωρούμε την κατασκευή 1.

□

Κλείνουμε αυτήν την παράγραφο, δίνοντας ορισμένες άπειρες κλασεις πινάκων στάθμισης που προκύπτουν μέσω του προηγούμενου θεωρήματος.

Πόρισμα 21 *Υπάρχουν άπειρες οικογένειες από πίνακες στάθμισης για τις ακόλουθες περιπτώσεις:*

(i) $W(76+2k,52), k \in \mathbb{IN}$.

(ii) $W(100+2k,68), k \in \mathbb{IN}$.

Απόδειξη.

(i) Υπάρχει ένα $\mathrm{TCP}(17,13)$ από την [37] με $\zeta = 2$. Χρησιμοποιώντας τις δύο ακολουθίες $[1,1]; [1,-1]$ που συνθέτουν το $\mathrm{TCP}(2,4) = \mathrm{GS}(2)$ παίρνουμε από την κατασκευή, $\mathrm{TCP}(19,13) \times \mathrm{TCP}(2,4) \rightarrow \mathrm{TCP}(38,52)$ τις ακολουθίες,

```
++00+-++00++00--++++++---+---0000++00-+
-+00---+00-+00+--+-+--+---+-0000-+00++
```

οι οποίες μπορούν να χρησιμοποιηθούν για να παράγουν μια άπειρη οικογένεια από $W(76+2k,52), k \in \mathbb{IN}$ πίνακες στάθμισης.

(ii) Υπάρχει ένα $\mathrm{TCP}(14,17)$ από την [37] με $\zeta = 11$. Χρησιμοποιώντας τις δύο ακολουθίες $[1,1]; [1,-1]$ που συνθέτουν το $\mathrm{TCP}(2,4) = \mathrm{GS}(2)$ παίρνουμε από την κατασκευή, $\mathrm{TCP}(25,17) \times \mathrm{TCP}(2,4) \rightarrow \mathrm{TCP}(50,68)$ τις ακολουθίες,

```
+-00+-00+-000000+-+--++++--+00++++00------00++--++
--00--00--000000----++-+--++00-+-+00+-+-+-00-++--+
```

οι οποίες μπορούν να χρησιμοποιηθούν για να παράγουν μια άπειρη οικογένεια από $W(100+2k,68), k \in \mathbb{IN}$ πίνακες στάθμισης.

□

§3.5 Μια Νέα Πολλαπλασιαστική Μέθοδος για Ακολουθίες με Μηδενική Περιοδική Συνάρτηση Αυτοσυσχέτισης

Σε αυτήν την ενότητα, δίνουμε μια νέα πολλαπλασιαστική μέθοδο για ακολουθίες με PAF μηδέν. Αυτή η μέθοδος, προκύπτει με φυσικό

τρόπο από τις κατασκευές που παρουσιάσαμε εώς τώρα για τις συμπληρωματικές ακολουθίες. Η μέθοδός μας μπορεί να θεωρηθεί και ως η εκδοχή της πολλαπλασιαστικής μεθόδου των TCP (βλ. κατασκευή 3., $\mathrm{TCP}(m, w) \times \mathrm{TCP}(n, z) \rightarrow \mathrm{TCP}(mn, wz)$) για ακολούθίες με PAF μηδέν.

Παρόλο που υπάρχουν αρκετές πολλαπλασιαστικές μέθοδοι για συμπληρωματικές ακολουθίες, αναφέρουμε ενδεικτικά τις [34, 36, 70, 122, 143, 148, 147, 153] (όπου με την έννοια του πολλαπλασιασμού για ένα σύνολο ακολουθιών, εννοούμε ότι υπάρχουν φυσικοί αριθμοί (λ_1, λ_2) οι οποίοι πολλαπλασιάζουν το μήκος και/ή το βάρος των αρχικών ακολουθιών), η πλειοψηφία αυτών (των μεθόδων) περιλαμβάνει κατασκευές για συμπληρωματικές ακολουθίες που έχουν PAF ή NPAF μηδέν. Η έννοια ενός μικτού γινομενού, το οποίο περιλαμβάνει τμήματα από ακολουθίες με PAF μηδέν και ακολουθίες με NPAF μηδέν, είναι σπάνια όταν συγκρίνεται με τις τωρινές γνωστές πολλαπλασιαστικές μεθόδους. Οι πολλαπλασιαστικές μέθοδοι, προσφέρουν σημαντική ευελιξία όταν κατασκευάζουμε μεγάλες ακολουθίες από αρκετά μικρότερες.

Για τα αποτελέσματα αυτής της ενότητας, υπενθυμίζουμε ότι ένα $\mathrm{DC}(n, k)$ ζεύγος ακολουθιών είναι δύο $\{0, \pm 1\}$ ακολουθίες μήκους n, συνολικού βάρους k που έχουν PAF μηδέν.

Θεώρημα 19 *Υποθέτουμε ότι* $A; B$ *είναι ένα* $\mathrm{DC}(n, k)$ *ζεύγος ακολουθιών,* $C; D$ *είναι ένα* $\mathrm{TCP}(m, w)$*, και ένα από τα ζεύγη ακολουθιών είναι ξένο. Τότε, υπάρχει η κατασκευή (απεικόνιση)*

$$\mathrm{DC}(n, k) \times \mathrm{TCP}(m, w) \rightarrow \mathrm{DC}(nm, kw).$$

Απόδειξη. Κατασκευάζουμε τις ακολουθίες $U; V$ του $\mathrm{DC}(nm, kw)$ ζεύγους ακολουθιών ως,

$$\begin{aligned} U &= A \otimes C + B \otimes D; \\ V &= A \otimes D^* - B \otimes C^* \end{aligned}$$

Προφανώς, οι $U; V$ είναι τριαδικές ακολουθίες και το άθροισμα των περιοδικών συναρτήσεων αυτοσυσχέτισης τους είναι μηδέν, θεωρώντας το άθροισμα των Hall και Laurent πολυωνύμων των U και V, με παρόμοιο τρόπο όπως αναφέρεται στην απόδειξη του Θεωρήματος 14 της [36]. □

Σημειώνουμε ότι, το γινόμενο στην προηγούμενή του μορφή δεν είναι μεταθετικό, δηλαδή αν θεωρήσουμε τις ίδιες συμπληρωματικές ακολουθίες όπως προηγουμένως έχουμε $\mathrm{TCP}(m, w) \times \mathrm{DC}(n, k) \nrightarrow \mathrm{DC}(mn, wk)$. Όμως, μπορούμε να θεωρήσουμε μια ισοδύναμη αλλά διαφορετική κατασκευή των παραγόμενων ακολουθιών $U; V$, η οποία περιλαμβάνει πάλι

το γινόμενο Kronecker ακολουθιών και το γινόμενο να γίνει μεταθετικό. Ιδιαίτερα, έχουμε ότι υπάρχει n απεικόνιση $\mathrm{TCP}(m,w)\times \mathrm{DC}(n,k)\to \mathrm{DC}(mn,wk)$ για ακολουθίες $E=[C\otimes A+D\otimes B];F=[D\otimes A^{*}-C\otimes B^{*}]$ όπου τα $A;B$ και $C;D$ είναι όπως στο Θεώρημα 19 και $E;F$ είναι ένα ισοδύναμο ζεύγος (ακολουθιών) του $U;V$.

Επιπλέον, μπορούμε να γενικεύσουμε το Θεώρημα 19 αφαιρώντας την υπόθεση του ξένου ζεύγους για ένα από τα δύο συμπληρωματικά ζεύγη ακολουθιών, θεωρώντας το κριτήριο της ζ-αποδοτικότητας για TCP. Ιδιαίτερα, έχουμε το ακόλουθο πόρισμα.

Πόρισμα 22 *Υποθέτουμε ότι* $A;B$ *είναι ένα* $\mathrm{DC}(n,k)$ *ζεύγος ακολουθιών και* $C;D$ *ειναι ένα* $\mathrm{TCP}(m,w)$ *με ζ-αποδοτικότητα ίση με ζ. Τότε, υπάρχει η κατασκευή (απεικόνιση)*

$$\mathrm{DC}(n,k)\times \mathrm{TCP}(m+\zeta,w)\to \mathrm{DC}(nm+n\zeta,kw).$$

Απόδειξη. Προφανώς, $\mathrm{TCP}(m,w)\to \mathrm{TCP}(m+\zeta,w)$ και θεωρούμε ότι οι παραγόμενες ακολουθίες του ξένου $\mathrm{TCP}(m+\zeta,w)$ είναι $E;F$. Εφαρμόζοντας το ζεύγος ακολουθιών $(C,D)=(E,F)$ στο Θεώρημα 19 το αποτέλεσμα έπεται.

□

Αξίζει να αναφερθεί ότι το Πόρισμα 22 είναι εφαρμόσιμο για κάθε δυνατό DC ζεύγος ή TCP. Επιπλέον, η εμφάνιση ενός κριτηρίου για TCP (η ζ-αποδοτικότητα) στο παραγόμενο μήκος του DC ζεύγους ακολουθιών είναι αξιοσημείωτο γεγονός και μπορεί να οδηγήσει σε περαιτέρω συμπεράσματα για αυτά τα ζεύγη.

§3.5.1 Ορισμένες Συνέπειες για Ακολουθίες με Μηδενική Περιοδική Συνάρτηση Αυτοσυσχέτισης

Σε αυτήν την ενότητα, μελετάμε ορισμένες συνέπειες για οικογένειες από DC ζεύγη ακολουθιών που προκύπτουν με φυσικό τρόπο, από τη νέα πολλαπλασιαστική μέθοδο. Η ακόλουθη απεικόνιση για πίνακες στάθμισης, είναι αρκετά γνωστή:

$$4.\ \mathrm{DC}(n,k)\to W(2n,k)$$

Για την κατασκευή 4., χρησιμοποιούμε τις δύο ακολουθίες του DC ζεύγους στο Θεώρημα 1.
Η απουσία μιας απεικόνισης της μορφής, $\mathrm{DC}(n,k) \to \mathrm{DC}(n+m,k), m \in \mathbb{N}$ (παραθέτοντας ένα DC ζεύγος ακολουθιών με μηδενικά, δεν διατηρείται η μηδενική αυτοσυσχέτιση), στη θεωρία των ακολουθιών με PAF μηδέν δεν μας επιτρέπει να κατασκευάσουμε άμεσα άπειρες οικογένειες από DC ζεύγη ακολουθιών ή πινάκων στάθμισης για δοθέν DC ζεύγος. Δίνουμε στη συνέχεια, μια αναδιατύπωση μιας γνωστής πολλαπλασιαστικής μεθόδου για DC ζεύγη ακολουθιών (βλ. [153]), κάνοντας χρήση της πολλαπλασιαστικής μεθόδου για DC ζεύγη.

Λήμμα 10 *Για κάθε* $\mathrm{DC}(n,w)$*, υπάρχει μια άπειρη οικογένεια από* $\mathrm{DC}(pn,w) \to W(2pn,w), p \in \mathbb{N}$ *πίνακες στάθμισης.*

Απόδειξη. Το τετριμμένο $\mathrm{TCP}(1,1)$ που αποτελείται από τις $1;0$ είναι ξένο. Προφανώς, ισχύει οτι $\mathrm{TCP}(1,1) \to \mathrm{TCP}(1+k,1), k \in \mathbb{N}$. Από το Θεώρημα 19 παίρνουμε ότι $\mathrm{DC}(n,w) \times \mathrm{TCP}(1+k,1) \to \mathrm{DC}(n+nk,w)$. Θέτοντας $k+1 = p \in \mathbb{N}$ παράγουμε μια άπειρη οικογένεια από $\mathrm{DC}(pn,w)$ ζεύγη ακολουθιών για $p \in \mathbb{N}$ και κατά συνέπεια μια άπειρη οικογένεια από $W(2pn,w)$ πίνακες στάθμισης για $p \in \mathbb{N}$.

□

Θεωρώντας γνωστές οικογένειες από DC ζεύγη ακολουθιών ή TCP, μπορούμε να κατασκευάσουμε αρκετά μεγάλες οικογένειες από DC ζεύγη. Ένα $\mathrm{DC}(n,2n)$ συμβολίζεται με $\mathrm{PCS}(n,2)$ στη βιβλιογραφία [122], και είναι γνωστό ότι PCS ζεύγη μπορούν να παράγουν έναν πίνακα Hadamard τάξης $2n$, δηλαδή έναν $H(2n)$. Επιπλέον, πολλαπλασιαστικές μέθοδοι για PCS ζεύγη είναι αρκετά σπάνιες και μια γνωστή οικογένεια από τέτοια ζεύγη, αναδιατυπώνεται στη συνέχεια. Επιπρόσθετα, δίνουμε μια κατασκευή για μια οικογένεια από DC ζεύγη ακολουθιών n οποία προκύπτει από ακολουθίες Golay.

Πρόταση 13 *Έστω ένα ξένο DC ζεύγος ακολουθιών. Τότε, υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για οικογένειες από DC ζεύγη και πίνακες στάθμισης,*

(i) $\mathrm{DC}(n,k) \times \mathrm{TCP}(m,2m) \to \mathrm{DC}(nm,2km) \to W(2nm,2km)$

(ii) $\mathrm{DC}(n,n) \times \mathrm{TCP}(m,2m) \to \mathrm{DC}(nm,2nm) = \mathrm{PCS}(nm,2) \to W(2nm,2nm) = H(2nm)$

όπου m *είναι το μήκος των* $\mathrm{GS}(m)$*, δηλαδή* $m \in \{2^a 10^b 26^c : a,b,c \in \mathbb{N}\}$.

Απόδειξη.

(i) Υπάρχουν $GS(m) = TCP(m, 2m)$ για $m \in \{2^a 10^b 26^c : a, b, c \in \mathbb{N}\}$. Χρησιμοποιούμε τα δύο ζεύγη των $DC(n, k)$ και $TCP(m, 2m)$ στο Θεώρημα 19 για να παράγουμε ένα $DC(nm, 2km)$ ζεύγος. Εφαρμόζουμε την κατασκευή 4. στις παραγόμενες ακολουθίες για να πάρουμε έναν $W(2nm, 2km)$ πίνακα στάθμισης.

(ii) Όπως και προηγουμένως, εφαρμόζουμε το Θεώρημα 19 και την κατασκευή 4. στα δοθείσα ζεύγη ακολουθιών.

□

Είναι γνωστό ότι υπάρχουν ακολουθίες Golay, $GS(m)$ για μήκη $m = 1, 2$. Συνεπώς, οι ακόλουθες οικογένειες από DC ζεύγη ακολουθιών είναι απλά μια (τετριμμένη) εφαρμογή της προηγούμενης πρότασης, αλλά θα φανεί χρήσιμη και στην κατασκευή πινάκων στάθμισης όπως θα δούμε στη συνέχεια.

Πόρισμα 23 *Έστω ένα ξένο* $DC(n, k)$ *ζεύγος ακολουθιών. Τότε, υπάρχουν οι ακόλουθες κατασκευές (απεικονίσεις) για DC ζεύγη,*

(i) $DC(n, k) \times TCP(1, 2) \to DC(n, 2k) \to W(2n, 2k)$.

(ii) $DC(n, k) \times TCP(2, 4) \to DC(2n, 4k) \to W(4n, 4k)$.

Απόδειξη.

(i) Χρησιμοποιούμε το $TCP(1, 2)$, που δίνεται από τις $[1]; [-1]$, στην Πρόταση 13.

(ii) Χρησιμοποιούμε το $TCP(2, 4)$, που δίνεται από τις $[1, 1]; [1, -1]$, στην Πρόταση 13.

□

§3.5.2 Πίνακες Στάθμισης από Ακολουθίες με Μηδενική Περιοδική Συνάρτηση Αυτοσυσχέτισης

Σε αυτήν την παράγραφο, παρουσιάζουμε ορισμένους πίνακες στάθμισης, που κατασκευάζονται από ένα DC ζεύγος ακολουθιών μέσω της νέα πολλαπλασιαστικής μεθόδου.

Λήμμα 11 *Υπάρχει ένα* $\mathrm{DC}(n,k) \to W(2n,k)$ *για τις περιπτώσεις:*

(i) $n = 29$ *και* $k = 36$.

(ii) $n = 74$ *και* $k = 144$.

Απόδειξη.

(i) Μπορούμε να κατασκευάσουμε ένα ξένο $\mathrm{DC}(29,18)$ ζεύγος ακολουθιών από την [63]:

```
-+0-0-000-00000000000-+0000+-
00-000+0+0+---0000--000000000
```

Εφαρμόζουμε αυτές τις ακολουθίες στο Πόρισμα 23, για να πάρουμε ένα $\mathrm{DC}(29,18) \times \mathrm{TCP}(1,2) \to \mathrm{DC}(29,36)$:

```
-++-0--0---+++0000++0-+0000+-
+-++0+-0-+-+++0000++0+-0000-+
```

Στη συνέχεια, θεωρούμε την κατασκευή 4. για να παράγουμε έναν $W(58,36)$ πίνακα στάθμισης.

(ii) Υπάρχει ένα ξένο $\mathrm{DC}(37,36)$ ζεύγος ακολουθιών από την [153]:

```
++--0-0-++0+00++0+0+00-+0+000-0+00000
0000-0+000+0--00-0-0+-00+0++-0-0++-+0
```

Εφαρμόζουμε αυτές τις ακολουθίες στο Πόρισμα 23, για να πάρουμε ένα $\mathrm{DC}(37,36) \times \mathrm{TCP}(2,4) \to \mathrm{DC}(74,144)$:

```
++++-----+--+---+++++-++-+++++-+++-+++++-+--+++-+++-+--+---++++-+--++-00
-+-++-+-+++---+--+-+---++++-+-+++-+++-+--+++--+---+----+++-++-+----++--00
```

Στη συνέχεια, θεωρούμε την κατασκευή 4. για να παράγουμε έναν $W(148, 144)$ πίνακα στάθμισης.

□

Σημειώνουμε ότι, η ύπαρξη των $W(58, 36)$ και $W(148, 144)$ είναι καταχωρημένη ως άγνωστη στη δεύτερη έκδοση του Εγχειριδίου Συνδυαστικών Σχεδιασμών, βλ. [35]. Όμως, ένα $DC(29, 36)$ ζεύγος και συνεπώς ένας $W(58, 36)$ πίνακας στάθμισης μπορεί να κατασκευαστεί από κατευθυνόμενες ακολουθίες μήκους 29 και τύπου $(18, 18)$ (βλ. [63]), άμεσα με αντικατάσταση των μεταβλητών τους με 1. Επιπλέον, ένας $W(148, 144)$ πίνακας στάθμισης κατασκευάστηκε πρόσφατα από τέσσερις συμπληρωματικές ακολουθίες με NPAF μηδέν (βλ. [158] και τη δεύτερη ενότητα αυτού του κεφαλαίου).

Στην [36], όπου και δόθηκε η πολλαπλασιαστική μέθοδος των TCP, η θεωρία που αναπτύχθηκε αποδείχθηκε αρκετά συμπαγής (compact), υπό την έννοια ότι όλες οι γνωστές περιπτώσεις για TCP μπορούσαν να κατασκευαστούν από ένα μικρό σύνολο πρωταρχικών (primitive) περιπτώσεων. Θα ήταν λογικό να υποθέσουμε ότι η πολλαπλασιαστική μέθοδος για DC ζεύγη ακολουθιών που δίνεται από το Θεώρημα 19, θα μπορούσε να θεωρηθεί το αρχικό στάδιο έρευνας πρωταρχικών περιπτώσεων για ακολουθίες με PAF μηδέν. Υποδηλώνοντας με αυτό το τρόπο ότι θα μπορούσαμε να κατασκευάσουμε όλα τα γνωστά DC ζεύγη από ένα αρχικό γνωστό σύνολο ακολουθιών με PAF μηδέν.

Παρόλο, που μπορούμε να θεωρήσουμε ανάλογες κατασκευές (απεικονίσεις) για DC ζεύγη ακολουθιών, παρόμοιες με αυτές που δίνονται στην Πρόταση 13, είναι προφανές ότι δεν μπορούμε να παράγουμε πρώτα βάρη για DC ζεύγη καθώς η προσέγγιση μας είναι πολλαπλασιαστική στα βάρη των DC ζευγών και των TCP. Όμως, θα μπορούσαμε να θεωρήσουμε τα DC ζεύγη που έχουν πρώτα βάρη ως τις αρχικές πρωταρχικές περιπτώσεις. Καθότι, η θεωρία που αναπτύξαμε δίνει ισχυρά επιχειρήματα για μια δραστική προσέγγιση ταξινόμησης DC ζευγών ακολουθιών κατά βάρος (κάτι το οποίο θα ήταν εντελώς ανάλογο της ταξινόμησης των TCP), η απουσία μιας απεικόνισης της μορφής $DC(n, k) \to DC(n + m, k), m \in \mathbb{N}$ είναι ένα επιχείρημα εναντίον αυτής της προσέγγισης.

Κλείνουμε αυτήν την ενότητα, με την ακόλουθη εικασία που εστιάζει στα DC ζεύγη ακολουθιών που έχουν πρώτα βάρη. Αυτή η εικασία, θα μπορούσε επίσης να θεωρηθεί και ως μια ειδική περίπτωση του Θεωρήματος 19.

Εικασία 2 *Αν υπάρχει ένα* $\mathrm{DC}(\mathrm{n}, w)$ *ζεύγος ακολουθιών και το* $\mathrm{p} \mid w$*, τότε υπάρχει ένα* $\mathrm{TCP}(\mathrm{m}, \mathrm{p})$ *ή ένα* $\mathrm{DC}(\mathrm{m}, \mathrm{p})$ *ζεύγος, για κάποιο* m*.*

Ένας προφανής τρόπος, για την απόδειξη της αλήθειας αυτής της εικασίας θα περιελάμβανε να δείξουμε ότι αν το w είναι σύνθετο, τότε ένα $\mathrm{DC}(\mathrm{n}, w)$ ζεύγος ακολουθιών θα πρέπει να παραγοντοποιείται μέσω κάποιου μικτού γινομένου DC ζευγών και TCP.

Man's longing for perfection finds expression in the theory of optimization.

Beightler, Phillips and Wilde (1979)

4

Εξελικτικοί Αλγόριθμοι Βελτιστοποίσης για Πίνακες Στάθμισης

Στο τέταρτο αυτό κεφάλαιο, παρουσιάζοτνται διάφοροι εξελικτικοί αλγόριθμοι (evolutionary algorithms) βελτιστοποίησης για την εύρεση πινάκων στάθμισης. Ιδιαίτερα, αποδεικνύεται ότι το πρόβλημα εύρεσης πινάκων στάθμισης μπορεί να θεωρηθεί ως ένα πρόβλημα ελαχιστοποίησης ή μετάθεσης (minimization or permutation problem) μέσω της χρήσης δύο εξελιγμένων γενετικών αλγορίθμων τελευταίας γενίας (competent genetic algorithms, εν συντομία CGA), που επιτρέπει την εύρεση βέλτιστων σημείων ή κοινών ακεραίων σε δύο τριαδικές ακολουθίες ή δύο ταξινομημένες λίστες, αντίστοιχα. Είχαμε ως κίνητρο, να μοντελοποιήσουμε τον "ακατάστατο ή περιπλεγμένο" γενετικό αλγόριθμο (messy genetic algorithm, εν συντομία, mGA) λόγω των πρωτοποριακών αποτελεσμάτων του Goldberg, σχετικών με την ικανότητα του mGA να θεωρεί ότι γονίδια που φέρουν συγκεκριμένες ιδιότητες μπορούν να σχηματίσουν ομάδες και να τοποθετηθούν μαζί σε μια λύση. Αυτή η ιδιότητα, αντιστοιχεί σε δομημένα πρότυπα (structural patterns) των πινάκων στάθμισης.

Για να μπορέσουμε να εκμεταλλευτούμε συγκεκριμένες ιδιότητες δύο ακολουθιών με μηδενική αυτοσυσχέτιση, χρησιμοποιήσαμε μια εκδοχή του γρήγορου περιπλεγμένου GA (fast messy GA, εν συντομία fmGA), όπου συνδυάζουμε τον mGA με εξελιγμένες τεχνικές. Επιπλέον, για να εκμεταλλευτούμε και την πρόσφατη κωδικοποίηση της συνάρτησης αυτοσυσχέτισης δύο ακολουθιών μέσω των στηριγμάτων τους (βλ. πρώτο κεφάλαιο), χρησιμοποιήσαμε μια εκδοχή του διατεταγμένου περιπλεγμένου GA (ordering messy GA, εν συντομία OmeGA), όπου σε αυτή την περίπτωση συνδυάζουμε τον fmGA με τυχαία κλειδιά (random keys) για να αναπαριστήσουμε τις δύο ακολουθίες που αναζητούμε μέσω μετα-

θέσεων. Αυτός ο μετασχηματισμός του προβλήματος εύρεσης πινάκων στάθμισης σε ένα στιγμιότυπο (instance) ενός προβλήματος συνδυαστικής βελτιστοποίησης (combinatorial optimization problem), φαίνεται να είναι ιδιαίτερα αποδοτικός καθώς οδηγεί στην εύρεση νέων πινάκων στάθμισης.

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στην επιστημονική εργασία [163].

§4.1 Εισαγωγή και Προηγούμενη Συνεισφορά

Ένας τετραγωνικός $n \times n$ πίνακας με στοιχεία $\{-1, 0, 1\}$ τέτοιος ώστε να ισχύει η σχέσητ $WW^T = wI_n$, όπου με W^T συμβολίζουμε τον ανάστροφο πίνακα του πίνακα W, θα καλείται ένας πίνακας στάθμισης τάξης n και βάρους w, και θα συμβολίζεται με $W(n, w)$. Για κατασκευές που αφορούν τους πίνακες στάθμισης παραπέμπουμε στις [33, 153]. Σε αυτό το κεφάλαιο, θα εστιάσουμε την προσοχή μας σε πίνακες στάθμισης που κατασκευάζονται μέσω δύο κυκλικών πινάκων (βλ. Θεώρημα 1, και γενικότερα την Ενότητα 1.1.1 για στοιχεία Θεωρίας πινάκων στάθμισης).

Όλοι οι πίνακες στάθμισης που κατασκευάζονται από δύο κυκλικούς πίνακες μέχρι το 1999, περιγράφονται στο Λήμμα 11 της οφ [153]. Είναι γνωστό ότι, αν η διοφαντική εξίσωση $a^2 + b^2 = w$ δεν έχει λύσεις, τότε δεν υπάρχει ένας $W(2n, w)$ που κατασκευάζεται από δύο κυκλικούς πίνακες, και κατά συνέπεια εστιάζουμε την προσοχή μας στις επιτρεπτές περιττές τιμές του n, δηλαδή εκείνες για τις οποίες η διοφαντική εξίσωση $a^2 + b^2 = w$ έχει λύσεις. Πρόσφατα, το πρόβλημα εύρεσης πινάκων στάθμισης μελετήθηκε μέσω αλγορίθμων βελτιστοποίησης, βλ. [137]. Σε αυτή την εργασία, μελετήθηκαν πίνακες στάθμισης που κατασκευάζονται από δύο κυκλικούς πίνακες για μεγάλα βάρη.

Ένας τρόπος να μειωθεί η υπολογιστική πολυπλοκότητα όταν αναζητούμε $W(2n, 2n - \alpha)$ πίνακες στάθμισης που κατασκευάζονται από δύο κυκλικούς πίνακες, είναι να εκφράσουμε το βάρος $w = 2n - \alpha$ ως μια συνάρτηση της τάξης n, και να αναγνωρίσουμε δομημένα πρότυπα για τη θέση των α μηδενικών στις δύο ακολουθίες $[a_1, \ldots, a_n]$ και $[b_1, \ldots, b_n]$ (που παράγουν τους κυκλικούς πίνακες, και κατά συνέπεια μέσω του Θεωρήματος 1 τον επιθυμητό πίνακα στάθμισης). Αυτή η μέθοδος μελετήθηκε στην [137], και έδωσε αξιοσημείωτα αποτελέσματα.

Σε αυτό το κεφάλαιο, ακολουθούμε μια διαφορετική προσέγγιση βασιζόμενοι στην έκφραση αυτών των δομημένων προτύπων μέσω τεχνικών σύνδεσης μάθησης (linkage learning techniques) έτσι ώστε να κάνουμε χρήση εξελιγμένων γενετικών αλγορίθμων. Ιδιαίτερα, θα μοντελοποιήσουμε τον γρήγορο περιπλεγμένο γενετικό αλγόριθμο για δύο ακολουθίες με μηδενική περιοδική συνάρτηση αυτοσυσχέτισης, και στη συνέχεια θα τον εμπλουτίσουμε με την τεχνική των τυχαίων κλειδιών για να αναπαραστήσουμε τα χρωμοσώματα. Αυτή η τεχνική, έχει το πλεονέκτημα ότι ο fmGA μετασχηματίζεται εύκολα σε ένα γενετικό αλγόριθμο επίλυσης μεταθέσεων, τον αποκαλούμενο διατεταγμένο περιπλεγμένο

γενετικό αλγόριθμο (OmeGA). Θα θέλαμε να σημειώσουμε ότι αυτή είναι η πρώτη φορά που μεταευρετικοί (metaheuristics) αλγόριθμοι αυτής της κατηγορίας των εξελικτικών αλγορίθμων, χρησιμοποιούνται για την εύρεση νέων πινάκων στάθμισης.

§4.1.1 Εφαρμογές των Πινάκων Στάθμισης

Οι πίνακες στάθμισης και οι βέλτιστοι σχεδιασμοί στάθμισης έχουν εκτεταμένα μελετηθεί για τις εφαρμογές τους σε στατιστικά πειράματα όπως πρώτος παρατήρησε ο Hotelling [114], αργότερα ο Raghavarao [199], και άλλοι ερευνητές [152]. Οι πίνακες στάθμισης επίσης μπορούν να χρησιμοποιηθούν για να παράγουν γραμμικούς κώδικες με καλές ιδιότητες, όπως για παράδειγμα αναφέρεται στην [3]. Επιπλέον, η σπουδαιότητα των πινάκων στάθμισης αναδείχθηκε και σε άλλες περιοχές, όπως για παράδιγμα στην Κβαντομηχανική [39]. Επιπρόσθετα, μια σύνδεση μεταξύ πρακτικών εφαρμογών και πινάκων στάθμισης εδραιώθηκε στην [152], όπου οι πίνακες στάθμισης χρησιμοποιήθηκαν στην Οπτική.

§4.2 Εξελιγμένοι Γενετικοί Αλγόριθμοι για Πίνακες Στάθμισης

Μετά τις πρωτοποριακές εργασίες των Holland (βλ. [111]) και De Jong (βλ. [118]) αρκετοί ερευνητές ακολούθησαν τα βήματα τους, και παρουσιάστηκαν αρκετές διαφορετικές προσεγγίσεις στο σχεδιασμό εξελιγμένων γενετικών αλγορίθμων. Στη Θεωρία των γενετικών αλγορίθμων κεντρική θέση διαδραματίζουν τα λεγόμενα δομικά στοιχεία (building blocks, εν συντομία BB, βλ. [74]). Όταν θα επικαλούμαστε τα δομικά στοιχέια, θα εννοούμε μερικές λύσεις του προβλήματος. Οι γενετικοί αλγόριθμοι χειραγωγούν ένα μεγάλο αριθμό δομικών στοιχείων μέσω των τελεστών της επιλογής (selection) και της αναπαραγωγής (reproduction). Αυτή η διαδικασία εξαρτάται από την κατανόηση της ανάμιξης των δομικών στοιχείων (building block mixing, βλ. [79]). Ένα από τα προβλήματα που αντιμετώπισαν οι απλοί γενετικοί αλγόριθμοι είναι το πρόβλημα σύνδεσης (linkage problem), δηλαδή η διαταραχή των δομικών

στοιχείων. Σύμφωνα με τις [235, 105], σύνδεση (linkage) είναι η τάση για αλληλόμορφα (alleles) διαφορετικά γονίδια, να μεταπηδήσουν από τη μια γενιά στην επόμενη στο πεδίο της Γενετικής. Αυτή η τάση αποτελεί ένδειξη ότι αυτα τα γονίδια να είναι στενά συνδεδεμένα στο ίδιο χρωμόσωμα. Για να ξεπεραστούν οι περιορισμοί των απλών γενετικών αλγορίθμων που οδηγούν σε τέτοιου είδους προβλήματα, προτάθηκε η περιπλεγμένη κωδικοποίηση των χρωμοσωμάτων [75].

Είχαμε ως κίνητρο, να μοντελοποιήσουμε τον "περιπλεγμένο" γενετικό αλγόριθμο (messy genetic algorithm, εν συντομία, mGA) λόγω των πρωτοποριακών αποτελεσμάτων του Goldberg [75, 76], σχετικών με την ικανότητα του mGA να θεωρεί ότι γονίδια που φέρουν συγκεκριμένες ιδιότητες μπορούν να σχηματίσουν ομάδες και να τοποθετηθούν μαζί σε μια λύση, για παράδειγμα $(0000 * *)$. Αυτή η ιδιότητα, αντιστοιχεί σε δομημένα πρότυπα (structural patterns) των πινάκων στάθμισης, όπως αναφέραμε νωρίτερα, και την μελετούμε στα πλαίσια της συνδυαστικής βελτιστοποίησης. Η εύρεση προσεγγίσεων για τεχνικές σύνδεσης μάθησης είναι μια ιδιαίτερα δημοφιλής προσέγγιση στους εξελικτικούς αλγορίθμους [26]. Μια επισκόπηση αυτών των τεχνικών για γενετικούς αλγορίθμους μπορεί να βρεθεί στην [26], ενώ για μια πιο γενική επισκόπηση μεταευρετικών αλγορίθμων παραπέμπουμε στην [11].

Μοντελοποίηση του Προβλήματος Εύρεσης Πινάκων Στάθμισης Ο mGA αντιμετωπίζει το πρόβλημα σύνδεσης βρίσκοντας δομικά στοιχεία με καλές ιδιότητες, και στη συνέχεια εφαρμόζει συγκεκριμένους τελεστές. Η αναγνώριση αυτών των συνδεδεμένων γονιδίων, είναι αρκετά σημαντική κατά τη διαδικασία της βελτιστοποίησης. Αυτός ο μηχανισμός μάθησης μπορεί να χρησιμοποιηθεί για να αποτρέψει την καταστροφή των BB από τους γενετικούς τελεστές (όπως είναι για παράδειγμα, η διασταύρωση στους απλούς γενετικούς αλγορίθμους, βλ. και Σχήμα 4.2.4). Εφαρμόσαμε μια βελτιωμένη εκδοχή του mGA όπως δίνεται στην [77, 78], για την αποφυγή προβλημάτων αρχικοποίησης, το γρήγορο περιπλεγμένο GA (fmGA).

Ερευνητικό Πρόβλημα 5 *Οι στόχοι που θέτουμε κατά τη μοντελοποίηση του προβλήματος εύρεσης πινάκων στάθμισης είναι:*

- *Η αναγνώριση δομημένων προτύπων πινάκων στάθμισης με όρους περιπλεγμένης κωδικοποίησης.*
- *Η αντιστοίχιση εννοιών της Συνδυαστικής Θεωρίας Σχεδιασμών με όρους της Θεωρίας γενετικών αλγορίθμων.*
- *Ο μετασχηματισμός του προβλήματος εύρεσης πινάκων στάθμισης σε ένα στιγμιότυπο προβλήματος βελτιστοποίησης, που απαιτεί τη χρήση εξελιγμένων γενετικών αλγορίθμων για την επίλυση του.*

§4.2.1 Σχήματα και Δομικά Στοιχεία για τη Μοντελοποίηση Πινάκων Στάθμισης

Τα *σχήματα (schemata)* ορίζονται ως πρότυπα ομοιότητας (similarity templates) που περιγράφουν ένα υποσύνολο χρωμοσωμάτων, που έχει ομοιότητες γύρω από ενα συγκεκριμένο τόπο (loci) [74]. Για τη μοντελοποίηση πινάκων στάθμισης αποκλίνουμε από την κλασική δυαδική αναπαράσταση, καθώς αυτοί οι πίνακες έχουν στοιχεία από το σύνολο $\{-1, 0, 1\}$. Κάνουμε χρήση ενός επιπλέον "αδιάφορου" συμβόλου που το αναπαριστούμε με έναν αστερίσκο ("*") για να συμπληρώσουμε το αλφάβητων των σχημάτων. Αυτού του είδους η αναπαράσταση δεν είναι νέα στη Συνδυαστική Θεωρία Σχεδιασμών. Πρότυπα ομοιότητας για ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης, έχουν χρησιμοποιηθεί στην [37], και καλούνται αφίξεις (affixes). Για παράδειγμα, ας θεωρήσουμε το σχήμα $H(-101*; 1100)$ μήκους 8, το οποίο αναπαριστά τις τρεις συνεχόμενες συμβολοσειρές `{-1010;1100,-101-1;1100,-1011;1100}` και αντιστοιχεί σε τρία ζεύγη τριαδικών ακολουθιών. Επιπλέον, αυτό το σχήμα είναι τάξης $o(H) = 7$, καθώς η τάξη του σχήματος ορίζεται ως το πλήθος των σταθερών θέσεων.

Ένα σχήμα αναμένεται να μεγαλώσει σε διαδοχικές γενιές αν (1) αν έχει τιμή αντικειμενικής συνάρτησης πάνω από το μέσο όρο, (2) είναι σχετικά μικρό, και (3) είναι μικρής τάξης. Όταν και οι τρείς αυτές συνθήκες ικανοποιούνται, λέμε ότι το εν λόγω σχήμα είναι ένα δομικό στοιχείο (building block, εν συντομία BB) [74]. Τα BB μπορούν να θεω-

ρηθούν ως τμήματα μιας λύσης που συνεισφέρει στο ολικό βέλτιστο. Με βάση την [37], ορίζουμε ένα σχεδόν-DC ζεύγος ακολουθιών μήκους n, βάρους w και σφάλματος ε, που θα το συμβολίζουμε με $\mathrm{NDC}(n, w, \varepsilon)$, να είναι ένα ζεύγος τριαδικών ακολουθιών μήκους n, με w μη-μηδενικά στοιχεία, όπου ε είναι το άθροισμα των τετραγώνων των συντελεστών αυτοσυσχέτισης. Τότε, κάθε ζεύγος τριαδικών ακολουθιών μπορεί να θεωρηθεί ως ένα NDC για κάποιο ε, αν και ενδιαφερόμαστε κυρίως για ζεύγη με $\varepsilon \ll w$. Σημειώνουμε ότι, ένα DC ζεύγος ακολουθιών έχει $\varepsilon = 0$. Θεωρούμε το ακόλουθο $\mathrm{NDC}(3, 3, 2)$ ζεύγος,

$$[1, 0, 0]; [1, -1, 0]$$

που μπορεί να αναπαρασταθεί από το σχήμα $\mathrm{H}(1 * 0; 1 * 0)$ τάξης 4. Σκοπός μας είναι η αναγνώριση ενσωματωμένων (embedded) DC ζευγών μικρού μήκους σε μεγαλύτερες ακολουθίες, όπου με αυτή την αναπαράσταση βλέπουμε ότι οι σταθερές θέσεις $[1, 0]; [1, 0]$ σχηματίζουν ένα $\mathrm{DC}(2, 2)$ ζεύγος ακολουθιών. Συνεπώς, μπορούμε να συμπεράνουμε ότι τα BB στους πίνακες στάθμισης αντιστοιχούν σε σχεδόν-DC ζεύγη ακολουθιών. Ιδιαίτερα, BB τάξης k αντιστοιχούν σε σχεδόν-DC ζεύγη μήκους $\lfloor k/2 \rfloor$. Τα βέλτιστα BB όπως παρατηρήσαμε νωρίτερα, αντιστοιχούν σε ενσωματωμένα DC ζεύγη ακολουθιών. Στη Συνδυαστική Θεωρία Σχεδιασμών, είναι συνήθες να συνδυάζουμε μικρά DC ζεύγη ακολουθιών έτσι ώστε να σχηματίσουμε ένα μεγαλύτερο ζεύγος (βλ. [208] και τρίτο κεφάλαιο). Αυτή η διαδικασία είναι εντελώς ανάλογη της περίφημης "Εικασίας των Δομικών Στοιχείων" ("Building Block Hypothesis", βλ. [74]), η οποία δηλώνει ότι η συνεχής παράθεση και επιλογή των BB σχηματίζει διαρκώς καλύτερες λύσεις με την πάροδο του χρόνου, οδηγώντας με αυτόν τον τρόπο στο ολικό μέγιστο του χώρου του προβλήματος.

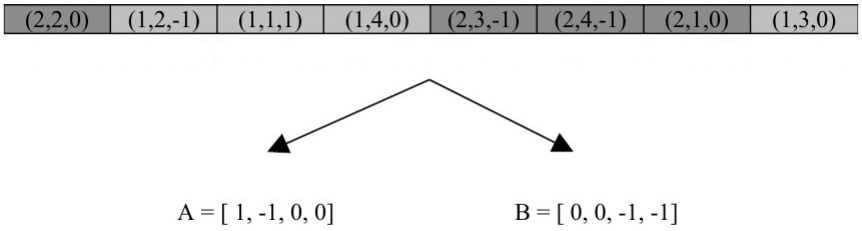
§4.2.2 Περιπλεγμένη Αναπαράσταση Πινάκων Στάθμισης

Θυμίζουμε ότι οι επιτρεπτές τιμές για τους δύο κυκλικούς υποπίνακες που σχηματίζουν ένα πίνακα στάθμισης είναι στοιχεία του συνόλου $\{-1, 0, 1\}$. Για την αναπαράσταση γονιδίων με συνηθισμένους ακεραίους αριθμούς, οι γενετικοί αλγόριθμοι για συνδυαστικά προβλήματα βελτιστοποίησης κάνουν χρήση μιας κωδικοποίησης ακεραίων για τα

χρωμοσώματα, βλ. [200]. Τα περιπλεγμένα γονίδια (messy genes) αναπαριστώνται με πλειάδες (tuples) που ορίζουν τη θέση τους (locus) και την τιμή τους (allele). Κάνουμε χρήση ενός επιπλέον δείκτη για να υποδηλώσουμε ποια ακολουθία έχουμε μοντελοποιήσει,

$$\text{περιπλεγμένο γονίδιο } g : (\text{δείκτης ακολουθίας}, \text{θέση}, \text{τιμή}).$$

Το μεγάλο πλεονέκτημα των mGA είναι ότι θεωρούν λύσεις μεταβλητού μήκους. Για παράδειγμα, στην προηγούμενη περιπλεγμένη κωδικοποίηση που αναπτύξαμε, οι λύσεις $g_1 = ((1,1,0),(2,1,-1),(2,2,0))$ και $g_2 = ((1,1,1),(1,2,1),(2,1,1),(2,2,-1),(2,2,0))$ είναι και οι δύο έγκυρες για ενα 4-bit πρόβλημα εύρεσης πινάκων στάθμισης τάξεως 4. Η πρώτη λύση αποκωδικοποιείται ως $[0,*]$ και $[-1,0]$, καθώς η πλειάδα $(1,1,0)$ δηλώνει ότι στην πρώτη ακολουθία, η πρώτη θέση είναι μηδέν. Δεν θα πρέπει να υπάρξει σύγχυση με το πρόβλημα του υπό-καθορισμού (underspecification) στην πρώτη λύση (δεν υπάρχει δεύτερο bit στην πρώτη ακολουθία) και του υπέρ-καθορισμού (overspecification) στην δεύτερη λύση (υπάρχουν δύο, δεύτερα bits στη δεύτερη ακολουθία).



Σχήμα 4.1: Περιπλεγμένη κωδικοποίηση ενός $DC(4,4)$ ζεύγους ακολουθιών

Συνεπώς, το πρόβλημα εύρεσης πινάκων στάθμισης μοντελοποιείται ως ένα $2n$ bit πρόβλημα θεωρώντας την ακόλουθη συνάρτηση κωδικοποίησης των NDC σε χρωμοσώματα,

$$\begin{aligned} gmp &: \Lambda^{2n} \to \{1,2\} \times S_\ell \times S_\ell \times \Lambda^\ell \\ gmp([a_1,\ldots,a_n],[b_1,\ldots,b_n]) &= g \end{aligned} \tag{4.1}$$

όπου $\Lambda = \{-1,0,1\}$, S_ℓ είναι το σύνολο όλων των διαφορετικών μεταθέσεων των ακεραίων από 1 εώς ℓ, και g είναι το περιπλεγμένο γονίδιο

που ορίσαμε προηγουμένως. Κατά συνέπεια, το περιπλεγμένο χρωμόσωμα είναι η παράθεση όλων των περιπλεγμένων γονιδίων. Η συνάρτηση αποκωδικοποίησης, gpm είναι η αντίστροφη διαδικασία, καθώς $gpm = gmp^{-1}$.

Δύο καθοριστικοί παράγοντες για την επιτυχή μοντελοποίηση ενός GA, που είναι η κατάλληλη ανάπτυξη και ανάμειξη καλών δομικών στοιχείων δεν επιτυγχάνεται συχνά [79]. Η περιπλεγμένη κωδικοποίηση προλαμβάνει τη διαταραχή σημαντικών δομικών στοιχείων καθώς η ικανότητα του μηχανισμού σύνδεσης μάθησης που έχει δίνει τη δυνατότητα στον mGA να θεωρήσει ότι ομάδες γονιδίων είναι στενά συνδεδεμένες στο ίδιο χρωμόσωμα, βλ. Σχήμα 4.2.4. Αυτή η ιδιότητα αντιστοιχεί σε δομημένα πρότυπα για πίνακες στάθμισης στη Συνδυαστική Θεωρία Σχεδιασμών, βλ. [137]. Ένα δομημένο πρότυπο για $W(2n, 2n-\alpha)$ πίνακες στάθμισης που κατασκευάζονται από δύο κυκλικούς πίνακες αφορά την τοποθεσία των α μηδενικών στις δύο ακολουθίες $[a_1, \ldots, a_n]$ και $[b_1, \ldots, b_n]$. Σε αυτή την ενότητα, ένα $(p, \alpha - p)$ δομημένο πρότυπο είναι μια δήλωση της μορφής:

Υπάρχουν p *μηδενικά στην* $[a_1, \ldots, a_n]$ *και* $\alpha - p$ *στην* $[b_1, \ldots, b_n]$.

Αυτή η παρατήρηση, όπως είδαμε στο τρίτο κεφάλαιο οδήγησε στην έννοια της διάδοσης (spread), των μηδενικών, δύο ακολουθιών [138]. Συνεπώς, όταν αναζητούμε πίνακες στάθμισης τάξεως $2n$ που προέρχονται από ακολουθίες με διάδοση s, μπορούμε να μειώσουμε το $2n$ bit πρόβλημα εύρεσης πινάκων στάθμισης σε $2(n-s)$ bits. Είναι ουσιώδες να παρατηρήσουμε ότι η διατήρηση καλών BB, δηλαδή δομικών στοιχείων της μορφής $(000**)$ αντιστοιχεί σε πολλαπλασιασμούς με μηδέν στο PAF μιας ακολουθίας.

Αντιμετώπιση του Υπέρ-Καθορισμού των Περιπλεγμένων Χρωμοσωμάτων Όπως αναφέραμε, ένα από τα μεγάλα πλεονεκτήματα του mGA είναι ότι θεωρεί λύσεις μεταβλητού μήκους. Αυτό είναι ένα χαρακτηριστικό που δίνει στον mGA το δικαίωμα, να αποκαλείται "περιπλεγμένος ή ακατάστατος". Για παράδειγμα, κανόντας χρήση της περιπλεγμένης κωδικοποίησης για πίνακες στάθμισης η λύση

$$g_1 = ((1,1,1),(1,2,1),(2,1,1),(2,2,-1),(2,2,0))$$

είναι έγκυρη για ένα 4-bit πρόβλημα εύρεσης πινάκων στάθμισης τάξεως 4. Λόγω του υπέρ-καθορισμού των χρωμοσωμάτων, απαιτείται να επιλέξουμε μεταξύ αντιφατικών γονιδίων σε μια συμβολοσειρά λύσεως. Στην περίπτωσή μας, μεταξύ των γονιδίων $(2,2,-1)$ και $(2,2,0)$.

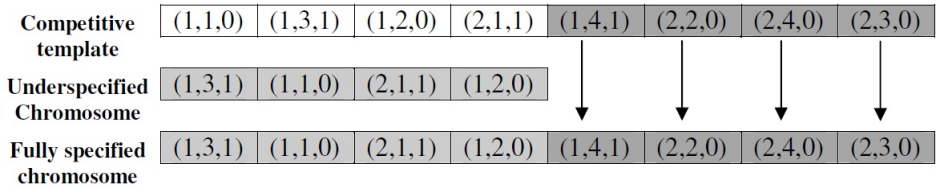
Ο υπέρ-καθορισμός είναι η πιο εύκολη περίπτωση που καλούμαστε να αντιμετωπίσουμε μεταξύ των δυϊκών προβλημάτων που κληρονομεί η περιπλεγμένη κωδικοποίηση (η άλλη περίπτωση είναι ο υπό-καθορισμός των χρωμοσωμάτων). Ο Goldberg [75], προτείνει ένα τελεστή έκφρασης των γονιδίων που κάνει χρήση του κανόνα "first-come-first-served", σε μια ανίχνευση από αριστερά προς δεξιά των γονιδίων. Δηλαδή, στην προηγούμενη λύση αυτή η ανίχνευση απορρίπτει τη δεύτερη πλειάδα $(2,2,0)$, παράγωντας τις έγκυρες δύο ακολουθίες $\mathrm{gpm(g1)} \rightarrow [1,1];[1,-1] \rightarrow \mathrm{DC}(2,4)$, που στη συνέχεια σχηματίζουν τον πίνακα στάθμισης.

Αντιμετώπιση του Υπό-Καθορισμού των Περιπλεγμένων Χρωμοσωμάτων Στην περίπτωση του υπό-καθορισμού, τα υπό-καθορισμένα γονίδια συμπληρώνονται κάνοντας χρήση ενός ανταγωνιστικού προτύπου (competitive template), που είναι ένα πλήρως καθορισμένο χρωμόσωμα και από το οποίο εκλειπόντα γονίδια κληρονομούνται άμεσα στο χρωμόσωμα. Για παράδειγμα, χρησιμοποιώντας ως ανταγωνιστικό πρότυπο το περιπλεγμένο χρωμόσωμα $((1,1,1),(1,1,-1),(2,1,-1),(2,2,0))$, στην λύση g_1 κληρονομείται ένα -1 στο δεύτερο bit της πρώτης ακολουθίας, δηλαδή έχουμε ότι το g_1 αναπαριστά τις ακολουθίες $[0,-1]$ και $[-1,0]$. Προφανώς, γονίδια που είναι ήδη καθορισμένα στην λύση δεν λαμβάνουν υπόψιν ο ανταγωνιστικό πρότυπο.

Αυτή η περίπτωση, έχει ιδιαίτερο ενδιαφέρον καθώς μας δίνεται η δυνατότητα να καθοδηγήσουμε τον αλγόριθμο σε ένα συγκεκριμένο τμήμα του χώρου λύσεων. Επιλέξαμε να χρησιμοποιήσουμε ανταγωνιστικά πρότυπα, τα δομημένα πρότυπα για πίνακες στάθμισης που αποδείχθηκαν αρκετά επιτυχημένα στο παρελθόν, παρέχοντας έτσι στον αλγόριθμο μια τεχνική σύνδεσης μάθησης παρόμοια με αυτή που δίνεται στην [76]. Στο ακόλουθο Σχήμα 4.2.2, περιγράφεται η χρήση ενός ανταγωνιστικού πρότυπου όπου η αποκωδικοποίηση των περιπλεγμένων χρωμοσωμάτων σε ακολουθίες υποδεικνύει ότι αυτές έχουν διάδοση ίση με 2.

§4.2.3 Μια Αντικειμενική Συνάρτηση για την Αποφυγή Πλάνης σε Πίνακες Στάθμισης

Ας υποθέσουμε ότι δύο μικρά, χαμηλής τάξης σχήματα σε συγκεκρι-



Σχήμα 4.2: Χρήση ενός ανταγωνιστικού προτύπου με διάδοση $s = 2$ όπου τα γονίδια των υπο-καθορισμένων χρωμοσωμάτων καθορίζονται από το πρότυπο

μένες θέσεις έχουν τιμή αντικειμενικής συνάρτησης πάνω από το μέσο όρο (των υπόλοιπων σχημάτων), αλλά ο συνδυασμός αυτών των δύο σχημάτων (η τομή τους) έχει τιμή αντικειμενικής συνάρτησης κάτω από το μέσο όρο. Αυτή είναι η ουσία του φαινομένου, που αποκαλείται *πλάνη (deception)* και εμπόδιζε τους απλούς γενετικούς αλγορίθμους να συγκλίνουν σε τοπικά βέλτιστα [73]. Δίνουμε ένα παράδειγμα με όρους της Συνδυαστικής Θεωρίας Σχεδιασμών όπου το ίδιο φαινόμενο είναι γνωστό, όπου η σύνθεση μικρών DC ζευγών, δεν παράγει πάντα ένα μεγαλύτερο DC ζεύγος ακολουθιών [153, 208]. Θεωρούμε τα $\mathrm{DC}(2,2)$ και $\mathrm{DC}(2,1)$ ζεύγη ακολουθιών `10;-10` και `10;00`, τα οποία μπορούν να θεωρηθούν ως μέρη των σχημάτων `10**;-10**` και `**10;**00`, αντίστοιχα. Ο συνδυασμός των τελευταίων σχημάτων παράγει την συμβολοσειρά `1010;-1000` που αναπαριστά ένα $\mathrm{NDC}(4,3,4)$ ζεύγος ακολουθιών, και κατά συνέπεια δεν είναι βέλτιστη. Για να αντιμετωπιστεί αυτή η δυσκολία, εκτός της περιπλεγμένης κωδικοποίησης στους mGA, επίσης η αντικειμενική συνάρτηση (objective function, εν συντομία OF) ορίστηκε ως το άθροισμα συγκεκριμένων υποσυναρτήσεων στην [75]. Η επιλογή της αντικειμενικής συνάρτησης για τον mGA προκύπτει με φυσικό τρόπο από τον ορισμό του σχεδόν-DC ζεύγους ακολουθιών, που εξαρτάται από το άθροισμα των τετραγώνων των συντελεστών αυτοσυχέτισης, και συνθέτεται από συγκεκριμένες υποσυναρτήσεις της μορφής $f_s(s) = (\mathrm{PAF}_A(s) + \mathrm{PAF}_B(s))^2$ (βλ. Σχέση 4.2).

Όταν η τιμή της OF γίνεται ίση με μηδέν έχουμε ανιχνεύσει ένα DC ζεύγος ακολουθιών, καθώς $\sum_{s=1}^{n-1}(\mathrm{PAF}_A(s) + \mathrm{PAF}_B(s))^2 = 0 \Longrightarrow (\mathrm{PAF}_A(s) + \mathrm{PAF}_B(s))^2 = 0 \Longrightarrow \mathrm{PAF}_A(s) + \mathrm{PAF}_B(s) = 0$ για $s = 1, \ldots, n-1$ που είναι σε απόλυτη συμφωνία με τον ορισμό του DC ζεύγους ακολουθιών (βλ. Ορισμό 2). Για όλες τις υπόλοιπες επιτρεπτές τιμές της OF, x, που είναι μεγαλύτερες από το μηδέν έχουμε ένα σχεδόν-DC ζεύγος ακολουθιών σφάλματος x. Συνεπώς, είναι προφανές ότι έχουμε ένα

πρόβλημα ελαχιστοποίησης καθώς επιθυμούμε την συνεχή ελαχιστοποίηση του σφάλματος x μέχρι αυτό να γίνει μηδενικό.

$$\begin{aligned} OF([a_1,\ldots,a_n],[b_1,\ldots,b_n]) &= \sum_{s=1}^{n-1}(PAF_A(s)+PAF_B(s))^2, \\ &= \sum_{s=1}^{n-1}\left(\sum_{i=1}^{n}a_ia_{i+s}+\sum_{i=1}^{n}b_ib_{i+s}\right)^2 \\ &= \sum_{s=1}^{n-1}\left(\sum_{i=1}^{n}(a_ia_{i+s}+b_ib_{i+s})\right)^2, \\ &\text{όπου} \quad s=1,\ldots,n-1. \end{aligned} \tag{4.2}$$

§4.2.4 Περιπλεγμένοι Τελεστές για Ακολουθίες με Μηδενική Περιοδική Συνάρτηση Αυτοσυσχέτισης

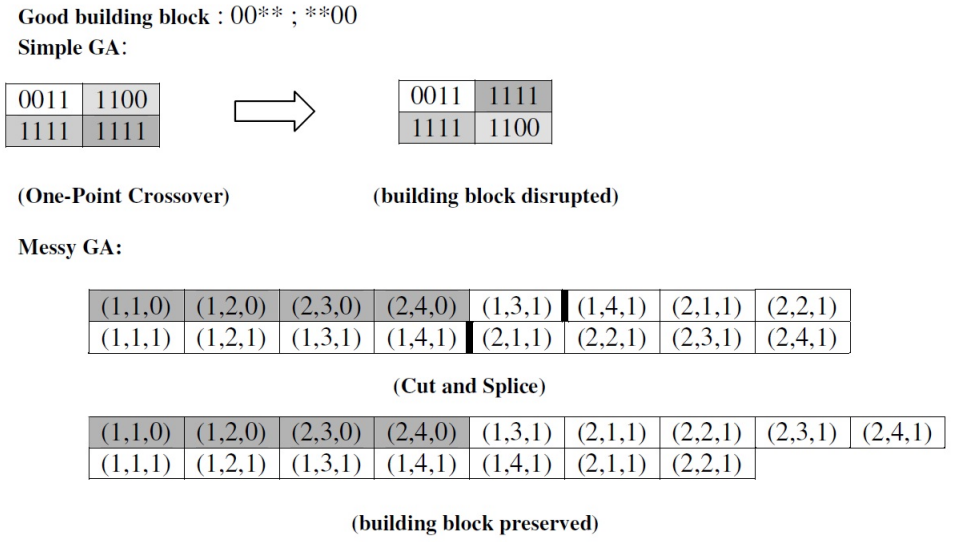
Επιτρέποντας χρωμοσώματα μεταβλητού μήκους, υπέρ-καθορισμένες ή υπό-καθορισμένες λύσεις, σημαίνει ότι ο σύνηθης απλός τελεστής της διασταύρωσης δεν δίνει επιθυμητά αποτελέσματα. Στον mGA n διασταύρωση αντικαθιστάται με δύο τελεστές, της συγκόλλησης (splice) και αποκοπής (cut) που τους εφαρμόσαμε με τον ίδιο τρόπο όπως περιγράφεται στην [75]. Ο τελεστής της αποκοπής χωρίζει ένα περιπλεγμένο χρωμόσωμα σε δύο μέρη με μια πιθανότητα αποκοπής $p_c = p_k(\lambda-1)$, όπου p_k είναι μια προκαθορισμένη bitwise πιθανότητα αποκοπής και λ είναι το μήκος του χρωμοσώματος. Η θέση αποκοπής επιλέγεται τυχαία κατά το μήκος λ. Για παράδειγμα, για $p_k = 0.1$ η πιθανότητα αποκοπής του χρωμοσώματος $((1,1,0),(1,2,0),(1,3,1),(2,1,0),(2,2,-1))$ θα ήταν 0.4. Μια αποκοπή στη θέση 3 θα είχε ως αποτέλεσμα τις δύο συμβολοσειρές $((1,1,0),(1,2,0),(1,3,1))$ και $((2,1,0),(2,2,-1))$. Ο τελεστής της συγκόλλησης, ενώνει δύο χρωμοσώματα με μια προκαθορισμένη πιθανότητα συγκόλλησης p_s. Για παράδειγμα, τα χρωμοσώματα

$$((1,1,0),(1,2,0)) \text{ και } ((1,3,1),(2,1,0),(2,2,-1))$$

θα συγκολλούνταν στο χρωμόσωμα

$$((1,1,0),(1,2,0),(1,3,1,(2,1,0),(2,2,-1)).$$

Η πιθανότητα συγκόλλησης είναι σχετικά υψηλή. Μπορούμε επίσης να ορίσουμε ένα τελεστή μετάλλαξης, ο οποίος μεταβάλλει τις τιμές του συνόλου $\{-1,0,1\}$ σύμφωνα με μια προκαθορισμένη πιθανότητα p_m. Όμως, θα υποθέσουμε ότι $p_m = 0$ για να παρατηρήσουμε καλύτερα την επίδραση της αναπαραγωγής ακολουθώντας τις συστάσεις που αναφερόνται στις [75, 77]. Στο Σχήμα 4.2.4 περιγράφεται επακριβώς η λειτουργία των τελεστών συγκόλλησης και αποκοπής.



Σχήμα 4.3: Διαταραχή των BB και η διατήρησή τους σε ένα 8-bit πρόβλημα εύρεσης πινάκων στάθμισης, όπου ο τελεστής διασταύρωσης σίγουρα θα διαταράξει το αραίο BB, 00**;**00, ενώ στον fmGA αυτό το δομικό στοιχείο πιθανότατα θα διατηρηθεί μετά την εφαρμογή των τελεστών της συγκόλλησης και αποκοπής λόγω της ευελιξίας της περιπλεγμένης κωδικοποίησης

§4.2.5 Γρήγοροι Περιπλεγμένοι Γενετικοί Αλγόριθμοι για Πίνακες Στάθμισης

Οι CGA λειτουργούν σε εντελώς διαφορετικό επίπεδο από τους SGA. Οι επαναλήψεις του γρήγορου περιπλεγμένου GA, πραγματοποιούνται πάνω από *εποχές (epochs)*, κάθεμια από τις οποίες περιέχει δύο κύριους βρόχους: έναν εξωτερικό και ένα εσωτερικό βρόχο. Ο εξωτερικός βρόχος διατρέχει την τάξη k των BB, που όπως δείξαμε νωρίτερα αντιστοιχούν σε σχεδόν-DC ζεύγη ακολουθιών μήκους $\lfloor k/2 \rfloor$. Κάθε επανάληψη του εξωτερικού βρόχου καλείται *περίοδος (era)*. Στην αρχή μιας νέας περιόδου, καλείται ο εσωτερικός βρόχος που έχει τρείς διακριτές φάσεις υπολογισμών. Αυτές οι φάσεις που περιγράφονται με τη μορφή ψευδοκώδικα στον Αλγόριθμο 19 είναι η φάση της αρχικοποίησης (initialization phase), η πρωτογενής φάση ή φάση φιλτραρίσματος των δομικών στοιχείων (primordial phase or building block filtering) και η φάση της παράθεσης (juxtapositional phase).

- Η φάση της αρχικοποίησης αποτελείται από την τυχαία δειγματοληψία χρωμοσωμάτων μήκους $\ell' = \ell - k$ όπου ℓ είναι ο αριθμός των διακριτών μεταβλητών που θέλουμε να βελτιστοποιήσουμε, και συνεπώς έχουμε ότι $\ell = 2n$ καθώς το μέγεθος του προβλήματος εύρεσης πινάκων στάθμισης είναι $2n$. Κατά συνέπεια, ισχύει $\ell' = 2n - k$. Η πιθανοθεωρητική πλήρης αρχικοποίηση (probabilistically complete initialization, εν συντομία PCI) είναι μια μέθοδος παραγωγής του αρχικού πληθυσμού. Ο σκοπός αυτής της φάσης αρχικοποίησης είναι η δημιουργία πληθυσμού που περιέχει όλους του πιθανούς γονιδιακούς συνδυασμούς για τα BB.

- Ο στόχος της πρωτογενούς φάσης είναι να παρέχει έναν πληθυσμό χρωμοσωμάτων μήκους k, από τον οποίο μπορούν να επιλεχθούν χρωμοσώματα και με μεγάλη πιθανότητα να παράγουν ένα βέλτιστο χρωμόσωμα. Όπως αναφέραμε μερικές λύσεις των DC ζευγών ακολουθιών, που αντιστοιχούν σε BB, δεν συνθέτουν πάντα μεγαλύτερες ακολουθίες. Όμως, στις [138, 70, 208] αρκετά θεωρητικά αποτελέσματα αφορούν την κατασκευή μεγάλων ακολουθιών που έχουν μηδενική συνάρτηση αυτοσυσχέτισης και συνθέτονται από μικρά DC ζεύγη. Η tournament selection είναι μια μέθοδος επιλογής που εστιάζει στην εύρεση χρωμοσωμάτων με υψηλή τι-

μή αντικειμενικής συνάρτησης, ενώ η φάση του φιλτραρίσματος των δομικών στοιχείων (BBF) είναι ένας τελεστής μετάλλαξης που χρησιμοποιείται περιοδικά για να μειώσει το μήκος των χρωμοσωμάτων.

- Η φάση της παράθεσης εφαρμόζει τους τελεστές της συγκόλλησης και της αποκοπής στα χρωμοσώματα για να κατασκευάσει λύσεις, με υψηλή τιμή αντικειμενικής συνάρτησης, μήκους $2n$ από τα χρωμοσώματα μήκους k που επέζησαν κατά την πρωτογενή φάση. Στη συνέχεια, εφαρμόζεται ο τελεστής της επιλογής για την εύρεσης καλών συνδυασμών των χρωμοσωμάτων.

Και στις δύο φάσεις, της πρωτογενούς και της παράθεσης, μια τοπικά βέλτιστη λύση, το ανταγωνιστικο πρότυπο χρησιμοποιείται για να γεμίσει τα κενά σε μερικώς καθορισμένα χρωμοσώματα.

Algorithm 19 FastMessyGA2WeighingMatrix Algorithm

```
function FmGA2WM(n, w, s)
Require: n, w, s > 0                          ▷ Input length n, weight w and spread s
    epoch ← 1
    template ← random string of spread s
    while epoch ≤ epoch_max do
        era ← 1
        while era ≤ k do
            ProbabilisticCompleteInitialization(population, era)        ▷ PCI phase
            Evaluate(population, template)
            repeat                                          ▷ Enter primordial (BBF) phase
                episode ← 0
                repeat
                    ThresholdingSelection(population)
                    episode ← episode + 1
                until episode ≤ episode_max
                GeneDeletion(population)
                Evaluate(population, template)
            until primordial termination criterion is true
            repeat                                      ▷ Enter juxtapositional phase
                Selection(population)
                CutAndSplice(population)
                Evaluate(population, template)
            until template has spread s          ▷ Juxtapositional termination criterion
            template ← Best(population)
            era ← era + 1
        end while
        epoch ← epoch + 1
    end while
end function
```

§4.2.6 Υλοποίηση του Γρήγορου Περιπλεγμένου Γενετικού Αλγορίθμου

Οι συστάσεις από τη βιβλιογράφια, αναφέρουν την εφαρμογή του γρήγορου περιπλεγμένου GA επαναληπτικά σε κάθε επίπεδο [77]. Η προσέγγιση μας κάνει χρήση πολλαπλών εποχών. Μια εποχή διατρέχει ένα μέγιστο αριθμό περιόδων. Το καλύτερο χρωμόσωμα που έχει βρεθεί σε κάθε επανάληψη χρησιμοποιείται ως ανταγωνιστικό πρότυπο, λαμβάνοντας υπόψιν τους μηχανισμούς σύνδεσης μάθησης που αναφέραμε στην αρχή αυτού του κεφαλαίου. Προσοχή χρειάζεται κατά την παραμετροποίηση του μεγέθους πληθυσμού και του αριθμού των περιόδων. Δίνουμε παρακάτω τις παραμέτρους της εκτέλεσης του fmGA για την εύρεση πινάκων στάθμισης.

Παράμετροι	Τιμή
Ελαχιστοποίηση	Αληθές
Καθοδήγηση του mGA	Αληθές
Μέγεθος προβλήμαοτς	2n
Πλήθος περιόδων	4
Πλήθος εποχών	2
Πιθανότητα αποκοπής	0.03
Πιθανότητα συγκόλλησης	1.0
Πιθανότητα μετάλλαξης	0.0
Γενιές	70
Μέγεθος Πληθυσμού	500 750 1250 1500

Πίνακας 4.1: Παράμετροι εκτέλεσης του fmGA για την εύρεση πινάκων στάθμισης

Τα πρώτα αποτελέσματα είναι ενθαρρυντικά, και δίνουμε στη συνέχεια ένα $\mathrm{DC}(35, 37)$ ζεύγος ακολουθιών με διάδοση ίση με 4, που παράγει έναν $W(2 \cdot 35, 37)$ πίνακα στάθμισης:

```
[0 0 0 0 + - + - 0 0 + 0 0 0 + - 0 0 + 0 0 0 - 0 0 + + + + + - 0 + - +]
[0 0 0 0 0 + 0 - 0 + + - 0 0 + + - 0 + - + + 0 0 0 0 + 0 - - - - - 0 +]
```

§4.2.7 Διατεταγμένοι Περιπλεγμένοι Γενετικοί Αλγόριθμοι για Πίνακες Στάθμισης

Σε αυτή την ενότητα, κάνουμε χρήση της νέας κωδικοποίησης για το PAF ενός $DC(n, w)$ ζεύγους ακολουθιών (βλ. πρώτο κεφάλαιο και [161]) μέσω της έννοιας των τυχαίων κλειδιών που δόθηκε στον random key-based simple GA, εν συντομία RKGA, [6]. Μια σημαντική εκδοχή του τελευταίου αλγορίθμου είναι ο biased random key-based simple GA, εν συντομία BRKGA, [82]. Υλοποιήσαμε τον διατεταγμένο περιπλεγμένο γενετικό αλγόριθμο (ordering messy GA, εν συντομία OmeGA, βλ. [127]), με βάση τους ακόλουθους κανόνες:

- Την εφαρμογή όλων των μηχανισμών του fmGA
- Τα αλληλόμορφα γονίδια είναι (μεγάλοι) ακέραιοι αριθμοί
- Τα αλληλόμορφα γονίδια αναπαριστώνται με τυχαία κλειδιά για να κωδικοποιήσουν μεταθέσεις

Η χρήση των τυχαίων κλειδιών για την αναπαράσταση, όπως αναφέρεται στην [6], επιτρέπει τη χρήση (μεγάλων) ακεραίων αριθμών ως κλειδιά ταξινόμησης για την αποκωδικοποίση των ακολουθιών που αναζητούμε. Σημειώνουμε ότι οι ακέραιοι αριθμοί είναι στοιχεία του στηριγμάτος των δύο ακολουθιών. Συνεπώς, επιτυγχάνουμε μια αρκετά πιο συμπαγή περιγραφή του στηρίγματος μιας ακολουθίας. Αναπαριστούμε μια μετάθεση μήκους ℓ με ένα διάνυσμα ακεραίων $\mathbf{r} = (r_1, r_2, \ldots, r_\ell)$ όπου $\mathbf{r} \in [-n, n]^\ell$. Ταξινομούμε τα τυχαία κλειδιά, στο διατεταγμένο περιπλεγμένο γονίδιο g:

$$g : (\text{δείκτης ακολουθίας}, \text{θέση}, \text{τυχαίο κλειδί})$$

με τέτοιο τρόπο έτσι ώστε να ισχύει,

$$r_{\phi(1)} \leq r_{\phi(2)} \leq \ldots \leq r_{\phi(\ell)}$$

όπου $\phi : \{1, \ldots, \ell\} \longrightarrow \{1, \ldots, \ell\}$ είναι η αντίστοιχη συνάρτηση αποκωδικοποίσης που ταξινομεί τα κλειδιά σε αύξουσα σειρά, και η μετάθεση αποκωδικοποιείται ως ακολούθως:

$$(\phi(1), \phi(2), \ldots, \phi(\ell))$$

Για το πρόβλημα εύρεσης πινάκων στάθμισης έχουμε ότι $\ell = w$, καθώς οι ακέραιοι αναπαριστούν το στήριγμα του $\mathrm{DC}(n, w)$ ζεύγους ακολουθιών.

Η επιλογή της αντικειμενικής συνάρτησης προκύπτει με φυσικό τρόπο ως ο ελάχιστος αριθμός των τυχαίων κλειδιών που πρέπει να μεταβληθούν έτσι ώστε να μετασχηματίσουμε τη μια μετάθεση στην άλλη. Προφανώς, όταν αυτή η τιμή είναι ίση με μηδέν έχουμε ότι οι υποψήφιες ακολουθίες σχηματίζουν ένα $\mathrm{DC}(n, w)$ ζεύγος ακολουθιών λόγω του υπολογισμού του PAF μέσω προσημασμένων συνόλων διαφορών όπως περιγράφει το Πόρισμα 1 μέσω της Παρατήρησης 2. Προσοχή χρειάζεται να μην υπάρξει κίνδυνος σύγχυσης ότι το στήριγμα μιας ακολουθίας είναι σύνολο, ενώ ο υπολογισμός του PAF μιας ακολουθίας (μέσω του στηρίγματος της) είναι πολυσύνολο.

Τα πρώτα αποτελέσματα της υλοποίσης του OmeGA για την εύρεση πινάκων στάθμισης είναι ενθαρρυντικά, και παρουσιάζουμε το ακόλουθο $\mathrm{DC}(61, 72)$ ζεύγος που μπορέι να χρησιμοποιηθεί στο Θεώρημα 1 για να σχηματίσει έναν $W(122, 72)$ πίνακα στάθμισης. Η ύπαρξη αυτού του πίνακα ήταν καταχωρημένη ως άγνωστη στον Πίνακα 6 της [153].

```
--000+00--0+---+---+--0+000-++000000---0++00+00-+-++-+-0+000-
--000-00--0---+-+++-++0-000+--000000++-0--00+00-+-++-+-0+000-
```

Μέρος ΙΙ

Θεωρία Κωδίκων

The most fascinating chapter of all in Coding Theory: MDS Codes.

MacWilliams and Sloane (1977)

5 Αυτοδυϊκοί Κώδικες

Στο πέμπτο αυτό κεφάλαιο, παρουσιάζεται μια γενική μέθοδος κατασκευής αυτοδυϊκών κωδίκων πάνω από το πεπερασμένο σώμα $\mathsf{GF}(p)$*, όπου* p *πρώτος, βασιζόμενη σε πίνακες skew-Hadamard. Ιδιαίτερα, δίνουμε νέους βέλτιστους τριαδικούς αυτοδυϊκούς κώδικες που έχουν κατασκευαστεί απο πίνακες skew-Hadamard. Επιπρόσθετα, παρουσιάζουμε μια πλήρη μελέτη για αυτοδυϊκούς κώδικες πάνω από το* $\mathsf{GF}(5)$ *οι οποίοι παράγονται απο τους μη-ισοδύναμους πίνακες skew-Hadamard τάξεως εώς* 28*, και δίνουμε μερικά αποτελέσματα για υψηλότερες τάξεις. Η κατασκεύη μας, δίνει βέλτιστους αυτοδυϊκούς κώδικες πάνω από το* $\mathsf{GF}(5)$ *για μήκη* 24*,* 40*,* 48 *και* 56*. Ιδιαίτερα, νέοι μη-ισοδύναμοι* $[48, 24]$ *και* $[56, 28]$ *αυτοδυϊκοί κώδικες πάνω από το* $\mathsf{GF}(5)$ *που τα ελάχιστα βάρη τους είναι* 14 *και* 16*, κατασκευάζονται από πίνακες skew-Hadamard τάξεως* 24 *και* 28*, βελτιώνοντας τους μόνους γνωστούς τετραγωνικά διπλά κυκλικούς (quadratic double circulant) κώδικες μήκους* 48 *και* 56*. Επιπρόσθετα,* $[80, 40]$ *και* $[88, 44]$ *αυτοδυικοί κώδικες που τα ελάχιστα βάρη τους είναι* 17 *και* 19 *πάνω από το* $\mathsf{GF}(5)$*, κατασκευάζονται για πρώτη φορά. Τέλος, ένας νέος* $[56, 28, 17]$ *αυτοδυϊκος κώδικας κατασκευάζεται πάνω από το* $\mathsf{GF}(7)$*, ο οποίος έχει το υψηλότερο ελάχιστο βάρος ανάμεσα σε όλους τους* $[56, 28]$ *αυτοδυϊκούς κώδικες. Αυτός ο νέος βέλτιστος κώδικας κατασκευάζεται από εναν πίνακα skew-Hadamard τάξεως* 28*, επίσης για πρώτη φορά. Επιπρόσθετα, δίνουμε ορισμένες ιδιότητες των παραγόμενων αυτοδυϊκών κωδίκων χρησιμοποιώντας όρους της αλγεβρικής θεωρίας κωδίκων, όπως τις τάξεις των ομάδων αυτομορφισμών και τους αντίστοιχους απαριθμητές βάρους.*

Στην τελευταία ενότητα του κεφαλαίου ενδιαφερόμαστε για την κατασκευή μέγιστης απόστασης διαχωρίσιμων (maximum distance separable) αυτοδυϊκών κωδίκων, εν συντομία MDS αυτοδυϊκοί κώδικες, πάνω από μεγάλα πρώτα πεπερασμένα σώματα οι οποίοι προκύπτουν από λύσεις συστημάτων διοφαντικών εξισώσεων. Με την εφαρμογή αυτής

της μεθόδου κατασκευάξουμε πολλούς αυτοδυϊκούς MDS (ή σχεδόν-MDS) κώδικες μήκους εώς 16 *πάνω από διάφορα πρώτα σώματα* $\mathsf{GF}(\mathrm{p})$, *όπου* $\mathrm{p} = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193$ *και* 197. *Επιπλέον, βέλτιστοι κώδικες παρουσιάζονται για αρκετά μήκη εώς* 40 *πάνω από μικρά πρώτα σώματα* $\mathsf{GF}(\mathrm{p})$. *Επιπρόσθετα, τα αποτελέσματα μας στο ελάχιστο βάρος των αυτοδυϊκών κωδίκων πάνω από πρώτα σώματα δίνουν ένα καλύτερο φράγμα από το φράγμα των Pless-Pierce, το οποίο προκύπτει από μια παραλλαγή του φράγματος Gilbert-Varshamov.*

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στις επιστημονικές εργασίες [154, 155] και [141].

§5.1 Εισαγωγή και Προηγούμενη Συνεισφορά

Ένας γραμμικός $[n, k]$ κώδικας C πάνω από το $GF(p)$ είναι ένας k-διάστατος διανυσματικός υπόχωρος του $GF(p)^n$, όπου $GF(p)$ είναι το πεπερασμένο σώμα Galois με p στοιχεία. Στην ενότητα αυτή, θεωρούμε την περίπτωση όπου p είναι πρώτος αριθμός. Τα στοιχεία του C καλούνται κωδικολέξεις και το (Hamming) βάρος $wt(x)$ μιας κωδικολέξης x είναι ο αριθμός των μη-μηδενικών συντεταγμένων που υπάρχουν στην x. Το ελάχιστο βάρος του C ορίζεται ως $\min\{wt(x) \mid 0 \neq x \in C\}$. Ένας $[n, k, d]$ κώδικας είναι ένας $[n, k]$ κώδικας με ελάχιστο βάρος d. Ένας πίνακας του οποίου οι γραμμές παράγουν το κώδικα C καλείται ο γεννήτορας πίνακας του C. Ο δυϊκός κώδικας $C^\perp$ του C ορίζεται ως $C^\perp = \{x \in GF(p)^n \mid x \cdot y = 0 \text{ για κάθε } y \in C\}$. Ο C είναι *αυτοδυϊκος* όταν $C = C^\perp$. Για $p \equiv 1 \pmod 4$, ένας αυτοδυϊκος $[n, n/2]$ κώδικας πάνω από το $GF(p)$ υπάρχει αν και μόνον αν το n είναι άρτιος, και για $p \equiv 3 \pmod 4$, ένας αυτοδυϊκος $[n, n/2]$ κώδικας πάνω από το $GF(p)$ υπάρχει αν και μόνον αν $n \equiv 0 \pmod 4$ [176]. Θα λέμε ότι αυτοδυϊκοί κώδικες με το μεγαλύτερο ελάχιστο βάρος ανάμεσα στους αυτοδυϊκούς κώδικες ίδιου μήκους είναι *βέλτιστοι (optimal)*. Φράγματα στην ελάχιστη απόσταση των γραμμικών κωδίκων μπορούν να βρεθούν στα [19] και [85].

Ένα κίνητρο για το ενδιαφέρον στους αυτοδυικούς κώδικες είναι ότι περιλαμβάνουν ορισμένους απο τους πιο γνωστούς κώδικες διόρθωσης σφαλμάτων, κααι οτι συνδέονται στενά με άλλες περιοχές της συνδυαστικής, της θεωρίας ομάδων και πινάκων [187], καθώς και ότι ορισμένες από τις εφαρμογές τους συναντώνται στις τηλεποικοινωνίες και στην θεωρία αριθμών και σχεδιασμών. Από το θεώρημα Gleason-Pierce [217], υπάρχουν αυτοδυϊκοί κώδικες πάνω από το $GF(p)$ για $p = 2, 3$ και 4. Συνεπώς έχει πραγματοποιηθεί εκτεταμένη έρεθνα για αυτοδυϊκούς κώδικες σε αυτά τα σώματα. Για παράδειγμα, αυτοδυϊκοί κώδικες μικρού μήκους πάνω από τα $GF(2)$, $GF(3)$ και $GF(4)$ έχουν ταξινομηθεί (βλ. [198, Ενότητες 11.3 – 11.6]), έτσι ώστε να καθοριστεί ποιοί κώδικες υπάρχουν και ποιοί απαριθμητές βάρους είναι δυνατοί. Επιπλέον, αρκετά είναι γνωστά για τα μεγαλύτερα ελάχιστα βάρη αυτοδυϊκών κωδίκων για αυτά τα σώματα (βλ. [198, Πίνακες X, XII, XIII and XIV]). Επιπρόσθετα t-σχεδιασμοί σχηματίζονται από βέλτιστους αυτοδυϊκούς κώδικες πάνω από τα $GF(2)$, $GF(3)$, ή $GF(4)$ [193] χρησιμοποιώντας το θεώρημα Assmus-Mattson [4]. Αντιστρόφως, αυτοδυϊκοί κώδικες πάνω

από μεγάλα σώματα δεν έχουν διερευνηθεί εκτεταμένα εώς σήμερα [198].

Για το GF(5), αυτοδυϊκοί κώδικες μήκους εώς 12, και για μήκη 14 και 16 έχουν ταξινομηθεί πλήρως, στις [170] και [104]. Τα υψηλότερα δυνατά ελάχιστα βάρη για αυτοδυϊκούς κώδικες πάνω από το GF(5) με μήκη εώς 24 έχουν καθορισθεί πλήρως στην [44]. Για το GF(7) μόνον τα μήκη 4 και 8 έχουν ταξινομηθεί πλήρως στην [195]. Αντίστοιχα τα υψηλότερα ελάχιστα βάρη για αυτοδυϊκούς κώδικες πάνω από το GF(7) για τα μήκη 12 εώς 16 έχουν καθορισθεί πλήρως στην [92]. Πίνακες με τις υψηλότερες γνωστές ελάχιστες αποστάσεις για αυτοδυϊκούς κώδικες πάνω από το GF(5) για μήκη εώς 64 και 70, δίνονται στον ([52, Πίνακα V]) και στους ([54, Πίνακες 9, 10]), αντίστοιχα. Διαθέσιμοι πίνακες στο διαδίκτυο με κατασκευές και τις υψηλότερες γνωστές ελάχιστες αποστάσεις για αυτοδυϊκούς κώδικες πάνω από το GF(5) για μήκη εώς το 70, παραπέμπουμε στην [53]. Κατασκευές για αυτοδυϊκούς κώδικες πάνω από το GF(5) και το GF(7), μπορούν να βρεθούν στις [3, 52, 54, 93, 94, 123, 141, 170] και [52, 59, 92, 170, 195, 141].
Στη συνέχεια θα θεωρήσουμε τους απαριθμητές βάρους των αυτοδυϊκών κωδίκων πάνω από το GF(p).

Θεώρημα 20 (MacWilliams, Mallows and Sloane [175]) *Ο απαριθμητής βάρους ενός αυτοδυϊκού κώδικα πάνω από το* GF(p) *είναι ένα στοιχείο του*

$$\mathbb{C}[(x + (\sqrt{p} - 1)y)^2, y(x - y)].$$

Συνεπώς έχουμε ένα τετριμμένο πάνω φράγμα $d \leq n/2+1$ το οποίο συμπίπτει με το φράγμα του Singleton για έναν $[n, n/2, d]$ κώδικα. Όμως, ο απαριθμητής βάρους $W_p(n)$ ενός αυτοδυϊκού $[n, n/2, n/2 + 1]$ κώδικα πάνω από το GF(p) είναι πλήρως καθορισμένος.

Πρόσφατα, κάποιοι ερευνητές (για παράδειγμα βλ. [123] και [141]) βελτιώσαν τα κάτω και πάνω φράγματα της ελάχιστης απόστασης των αυτοδυϊκών κωδίκων πάνω από το GF(5) για μήκη από 26 εώς 40 και 34, αντίστοιχα. Μια μέθοδος κατασκευής αυτοδυϊκών κωδίκων πάνω από το GF(5) από σχεδιασμούς skew-Hadamard για μήκη από 20 εώς 60 εμφανίστηκε στην [126]. Στην [94], κώδικες πάνω από το GF(5) με παραμέτρους $[36, 18, 12]$, $[48, 24, 15]$, $[60, 30, 18]$, $[64, 32, 18]$ και $[76, 38, 21]$ οι οποίοι βελτιώνουν τα προηγουμένως γνωστά φράγματα στο ελάχιστο βάρος των γραμμικών κωδίκων πάνω από το GF(5) κατασκευάστηκαν από πίνακες συνεδρίου (conference matrices). Στην ίδια εργασία, οι συγγραφείς σημείωνουν ότι είναι υπολογιστικά αδύνατον να καθορίσουν το ελάχιστο βάρος για την επόμενη περίπτωση της μεθόδους τους, εν προκειμένω για το μήκος 84.

Ερευνητικό Πρόβλημα 6 *Η κατασκευή βέλτιστων αυτοδυϊκών κωδίκων πάνω από πεπερασμένα πρώτα σώματα, εν προκειμένω η βελτίωση των πάνω φραγμάτων της υψηλότερης ελάχιστης απόστασης των αυτοδυϊκών (γραμμικών) κωδίκων χρησιμοποιώντας μαθηματικές δομές της Θεωρίας σχεδιασμών.*

§5.2 Μια Νέα Μέθοδος Κατασκευής για Αυτοδυϊκούς Κώδικες πάνω από το GF(p) από Πίνακες skew-Hadamard

Υπενθυμίζουμε ότι, ένας *πίνακας Hadamard* τάξεως n είναι ένας $n \times n$ πίνακας με στοιχεία από το σύνολο $\{1, -1\}$ ο οποίος ικανοποιεί την σχέση $HH^T = nI_n$. Είναι γνωστό ότι αν n είναι η τάξη του πίνακα Hadamard τότε το n είναι απαραίτητα 1, 2 ή πολλαπλάσιο του 4. Ένας πίνακας Hadamard έιναι *κανονικοποιημένος (normalized)* αν όλα τα στοιχεία της πρώτης γραμμής και στήλης είναι ίσα με 1. Δύο πίνακες Hadamard θα λέγονται ισοδύναμοι αν ο ένας μπορεί να μετασχηματισθεί στον άλλον μετά από την εφαρμογή διαδοχικών μεταθέσεων των στηλών ή και των γραμμών του, καθώς και πολλαπλασιασμό αυτών με -1. Ένας πίνακας H με στοιχεία από το σύνολο $\{1, -1\}$, για τον οποίο ισχύει

$$H = C + I_n \tag{5.1}$$

θα λέγεται *skew-Hadamard πίνακας* τάξεως n αν $CC^T = (n-1)I_n$ και $C^T = -C$.

Περισσότερες λεπτομέρειες για την κατασκευή των πινάκων Hadamard και skew-Hadamard μπορούν να βρεθούν στο σύγγραμμα [70]. Στην εργασία [166] μελετάται η ύπαρξη και η ισοδυναμία των πινάκων skew-Hadamard. Στη συνέχεια παραθέτουμε μια γνωστή μέθοδο κατασκευής για αυτοδυϊκούς κώδικες μήκους $2n$ πάνω από το $GF(p)$ χρησιμοποιώντας πίνακες skew-Hadamard τάξεως n.

Θεώρημα 21 (Georgiou, Koukouvinos and Lappas [68]) *Έστω H ένας πίνακας skew-Hadamard τάξεως n και υποθέτουμε ότι υπάρχουν τρία στοιχεία $a \neq 0, b, c$ από το $GF(p)$ τέτοια ώστε $a^2 + b^2 + (n-1)c^2 \equiv 0 \pmod p$. Τότε ο πίνακας $G = [aI_n \; cC + bI_n]$ παράγει έναν αυτοδυϊκό κώδικα μήκους $2n$ και διάστασης n.*

Παρατηρήσαμε ότι, μπορούμε να τροποποιήσουμε την προηγούμενη κατασκευή ως ακολούθως. Θέτουμε $a = s, b = u - t, c = u$ στο προηγούμενο θεώρημα. Τότε η διοφαντική εξίσωση $a^2 + b^2 + (n-1)c^2 \equiv 0 \pmod p$ είναι ισοδύναμη με $s^2 + (u-t)^2 + (n-1)u^2 \equiv 0 \pmod p$, και μετασχηματίζουμε τον γεννήτορα πίνακα στον $G = [aI_n \ cC + bI_n] = [sI_n \ uC + (u-t)I_n] = [sI_n \ u(C + I_n) - tI_n] = [sI_n \ uH - tI_n]$. Συνεπώς, με βάση αυτήν την παρατήρηση είμαστε σε θέση να αποδείξουμε το παρακάτω θεώρημα που θα χρησιμοποιήσουμε στις επόμενες ενότητες του κεφαλαίου.

Θεώρημα 22 *Έστω H ένας πίνακας skew-Hadamard τάξεως n και υποθέτουμε ότι υπάρχουν τρία στοιχεία $a \neq 0, b \neq 0, c \neq 0$ από το $GF(p)$ τέτοια ώστε $a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod p$. Τότε ο πίνακας $G = [aI_n \ cH - bI_n]$ παράγει έναν αυτοδυϊκό κώδικα μήκους $2n$ και διάστασης n.*

Απόδειξη. Επειδή ο H είναι ένας πίνακας skew-Hadamard τάξεως n μπορούμε να τον γράψουμε στη μορφή $H = C + I_n$ όπου ο C ικανοποιεί την σχέση $CC^T = (n-1)I_n$. Επιπλέον, ο C είναι skew-συμμετρικός και ισχύει $C^T = -C$. Συνεπώς έχουμε ότι $H + H^T = 2I_n$. Επιπρόσθετα, υπολογίζουμε το γινόμενο $GG^T = [aI_n \ cH - bI_n][aI_n \ cH - bI_n]^T = a^2I_n + (cH - bI_n)(cH^T - bI_n) = a^2I_n + c^2HH^T - bcH - bcH^T + b^2I_n = a^2I_n + c^2nI_n - bc(H + H^T) + b^2I_n = a^2I_n + b^2I_n - 2bcI_n + c^2I_n + (n-1)c^2I_n = (a^2+(b-c)^2+(n-1)c^2)I_n \equiv 0_n \pmod p$, όπου 0_n είναι ο $n \times n$ μηδενικός πίνακας. Επειδή $a^2+(b-c)^2+(n-1)c^2 \equiv 0 \pmod p$ έχουμε ότι ο κώδικας ο οποίος παράγεται από τον G είναι ένας αυτοδυϊκός κώδικας μήκους $2n$ και διάστασης n. □

Παρατήρηση 13 *Όταν $b = c$ ο προηγούμενος γεννήτορας πίνακας έχει μια πιο απλούστερη μορφή $G = [aI_n \ cC]$, όπου $C = H - I_n$, υπό την προϋπόθεση ότι $a^2 + (n-1)c^2 \equiv 0 \pmod p$.*

Παρατήρηση 14 *Μπορούμε να υποθέσουμε ότι $a = 1$ στις προηγούμενες κατασκευές λαμβάνοντας υπόψιν την ισοδυναμία.*

§5.2.1 Κατασκευή Τριαδικών Αυτοδυϊκών Κωδίκων

Ένας τριαδικός αυτοδϋικός κώδικας C θα καλείται βέλτιστος (optimal) αν είναι ακραίος (extremal), για παράδειγμα αν έχει το μεγαλύτερο δυνατό ελάχιστο βάρος. Τα γνωστά φράγματα της ελάχιστης απόστασης d για το $GF(3)$ δίνονται στις [198] και [226]. Ιδιαίτερα το ακόλουθο θεώρημα είναι γνωστό.

Θεώρημα 23 (Tonchev [226]) *Η ελάχιστη απόσταση* d *ενός τριαδικού αυτοδϋικού* $[2n, n]$ *κώδικα* C *ικανοποιεί την ανισοισότητα*

$$d \leq 3\left[\frac{n}{6}\right] + 3.$$

όπου με $[x]$ *συμβολίζουμε τον πλησιέστερο ακέραιο του* x.

Σε αυτή την ενότητα, θα υπολογίσουμε το ελάχιστο βάρος των αυτοδϋικών κωδίκων που παράγονται από το Θεώρημα 22 για κάθε πιθανή λύση της διοφαντικής εξίσωσης,

$$a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod 3$$

όταν $a, b, c \neq 0$ πάνω από το $GF(3)$. Η διοφαντική εξίσωση έχει λύσεις για $n = 8, 12, 20, 24$. Θα παρουσιάσουμε στη συνέχεια, βέλτιστους (ακραίους) αυτοδυϊκούς κώδικες με μήκη $2n = 16, 24, 40, 48$ οι οποίοι παράγονται από τους μη-ισοδύναμους πίνακες skew-Hadamard τάξεως $n = 8, 12, 20, 24$. Το κίνητρο μας να παρουσιάσουμε μια πλήρη μελέτη για αυτές τις τάξεις των πινάκων skew-Hadamard έγγειται στο γεγονός ότι οι αντίστοιχες τάξεις αυτών των πινάκων είναι πλήρως καθορισμένη για τάξεις εώς 28, και επιπρόσθετα επειδή στην [154] αυτοδυϊκοί κώδικες μόνο πάνω από το $GF(5)$ είχαν παρουσιαστεί. Με N_n θα συμβολίσουμε τον αριθμό των μη-ισοδύναμων πινάκων skew-Hadamard για μια δεδομένη τάξη n. Συνοψίζουμε τα γνωστά αποτελέσματα για N_n στον ακόλουθο πίνακα, τα οποία αναφέρονται στην [166].

n	4	8	12	16	20	24	28
N_n	1	1	1	2	1	16	54

Πίνακας 5.1: Μη-ισοδύναμοι πίνακες skew-Hadamard τάξεως 4 εώς 28

Στον πίνακα 5.2.1, συμβολίζουμε με n την τάξη του πίνακα skew-Hadamard και με N_n τον αριθμό των γνωστών μη-ισοδύναμων πινάκων skew-Hadamard τάξεως n.

Στα αποτελέσματα που ακολουθούν, δίνουμε για κάθε μη-ισοδύναμο πίνακα skew-Hadamard μόνο τους αντίστοιχους μη-ισοδύναμους αυτοδυϊκούς κώδικες που παράγονται, την τάξη των ομάδων αυτομορφισμών αυτών των κωδίκων και τους αντίστοιχους απαριθμητές βάρους. Υπενθυμίζουμε ότι, δύο γραμμικοί κώδικες C_1 και C_2 πάνω από το $GF(p)$ είναι μονώνυμα ισοδύναμοι αν υπάρχει ένας μονώνυμος πίνακας M πάνω από το $GF(p)$ τέτοιος ώστε $C_2 = C_1M = \{cM \mid c \in C_1\}$. Ένας μονώνυμος πίνακας πάνω από το $GF(p)$ ο οποίος απεικονίζει τον C στον εαυτό του θα καλείται ένας αυτομορφισμός του C. Το σύνολο όλων των αυτομορφισμών του C θα καλείται ομάδα αυτομορφισμών $Aut(C)$ του C. Για έναν αυτοδυϊκό κώδικα ο οποίος παράγεται από τον i-ο μη-ισοδύναμο πίνακα skew-Hadamard τάξεως n θα χρησιμοποίήσουμε το συμβολισμό $C_{n,i}$.

[16, 8] **Τριαδικοί Αυτοδυϊκοί Κώδικες** Σε αυτήν την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το $GF(3)$, οι οποίοι προκύπτουν από τον μοναδικό πίνακα skew-Hadamard τάξεως 8. Ο μοναδικός πίνακας skew-Hadamard (λαμβάνοντας υπόψιν την ισοδυναμιά) τάξεως 8 είναι ο

$$H_8 = C + I_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	$Aut(C)$	$W(x, y)$
$C_{8,1}$	1	2	1	6	$43008 = 2^{11} \cdot 3 \cdot 7$	$x^{16} + 224x^{10}y^6 + 2720x^7y^9 + 3360x^4y^{12} + 256xy^{15}$

Πίνακας 5.2: $[16, 8]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 8

Ο κώδικας $C_{8,1}$ είναι ακραίος καθώς το φράγμα για $n = 8$ από το Θεωρήμα 23 είναι 6.

[24, 12] **Τριαδικοί Αυτοδυϊκοί Κώδικες** Σε αυτήν την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(3), οι οποίοι προκύπτουν από το μοναδικό πίνακα skew-Hadamard τάξεως 12. Ο μοναδικός πίνακας skew-Hadamard (λαμβάνοντας υπόψιν την ισοδυναμιά) τάξεως 12 είναι ο

$$H_{12} = C + I_{12} = \begin{pmatrix} 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)	$W(x, y)$
$C_{12,1}$	1	1	1	9	$5280 = 2^5 \cdot 3 \cdot 5 \cdot 11$	$x^{24} + 4048x^{15}y^9 + 61824x^{12}y^{12}$ $+242880x^9y^{15} + 198352x^6y^{18}$ $+24288x^3y^{21} + 48y^{24}$

Πίνακας 5.3: [24, 12] αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 12

Ο κώδικας $C_{12,1}$ είναι ακραίος καθώς το φράγμα για $n = 12$ από το Θεωρήμα 23 είναι 9.

[40, 20] **Τριαδικοί Αυτοδυϊκοί Κώδικες** Σε αυτή την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(3), οι οποίοι προκύπτουν από τον μοναδικό πίνακα skew-Hadamard τάξεως 20. Ο μοναδικός πίνακας skew-Hadamard (λαμβάνοντας υπόψιν την ισοδυναμιά) τάξεως 20 είναι ο

$$H_{20} = C + I_{20} = \begin{pmatrix}
+&-&+&-&+&+&-&-&+&+&-&-&-&+&-&-&-&-&+\\
+&+&-&+&-&-&-&+&+&+&-&-&+&-&-&-&-&+&-\\
-&+&+&-&+&-&+&+&+&-&-&-&+&-&-&-&-&+&-\\
+&-&+&+&-&+&+&+&-&-&-&+&-&-&-&-&+&-&-\\
-&+&-&+&+&+&+&-&-&+&-&-&-&+&-&-&-&-&-\\
-&+&+&-&-&+&-&+&-&+&-&-&-&-&+&+&+&+&-\\
+&+&-&-&-&+&+&-&+&-&-&-&-&+&-&+&+&-&+\\
+&-&-&-&+&-&+&+&-&+&-&-&+&-&-&+&+&-&+\\
-&-&-&+&+&+&-&+&+&-&-&+&-&-&-&+&-&+&+\\
-&-&+&-&-&+&-&-&+&+&+&-&-&-&-&-&+&+&+\\
+&+&+&+&-&+&+&+&-&+&-&+&-&+&+&-&-&+&+\\
+&+&+&-&+&+&+&+&-&+&+&-&+&-&-&-&+&+&+\\
+&+&-&+&+&+&-&+&+&-&+&+&-&+&-&+&+&+&-\\
+&-&+&+&+&-&+&+&+&+&-&+&+&-&+&-&+&+&-\\
-&+&+&+&-&+&+&+&+&-&+&-&+&+&+&+&-&-&+\\
+&+&+&-&-&-&-&+&-&+&+&-&-&+&-&+&-&+&-\\
+&+&+&-&+&-&-&-&+&-&+&+&-&-&+&+&-&+&-\\
+&+&-&+&+&-&-&+&-&+&-&-&-&+&-&+&+&-&+\\
+&-&+&+&+&-&+&-&-&-&-&-&-&+&+&+&-&+&-\\
-&+&+&+&+&+&-&-&-&-&-&-&+&+&-&-&+&-&+
\end{pmatrix}$$

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	$Aut(C)$	$W(x,y)$
$C_{20,1}$	1	2	1	12	$13680 = 2^4 \cdot 3^2 \cdot 5 \cdot 19$	$x^{40} + 19760x^{28}y^{12} + 1138176x^{25}y^{15}$ $+25549680x^{22}y^{18} + 236945280x^{19}y^{21}$ $+907161840x^{16}y^{24} + 1389711680x^{13}y^{27}$ $+783017664x^{10}y^{30} + 137826000x^{7}y^{33}$ $+5394480x^{4}y^{36} + 19840xy^{39}$

Πίνακας 5.4: $[40, 20]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 12

Ο κώδικας $C_{20,1}$ είναι ακραίος καθώς το φράγμα για $n = 20$ από το Θεωρήμα 23 είναι 12.

$[48, 24]$ **Τριαδικοί Αυτοδυϊκοί Κώδικες** Σε αυτή την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το $GF(3)$, οι οποίοι προκύπτουν από τους δεκαέξι μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 24. Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα. Οι πίνακες skew-Hadamard που χρησιμοποιήσαμε μπορούν να βρεθούν στην ιστοσελίδα που δίνεται στην [145]. Σημειώνουμε ότι σε αυτή την περίπτωση, παραθέτουμε μόνον την τάξη των ομάδων αυτομορφισμών των παραγόμενων αυτοδυϊκών κωδίκων, και όχι τους αντίστοιχους απαριθμητές βάρους

λόγω του ότι ο υπολογιστικός χρόνος αυξάνει εκθετικά σε αυτή την περίπτωση.

C	a	b	c	d	$\mathrm{Aut}(C)$	C	a	b	c	d	$\mathrm{Aut}(C)$
$C_{24,1}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,9}$	1	1	1	12	$48 = 2^4 \cdot 3$
$C_{24,2}$	1	1	1	12	$24 = 2^3 \cdot 3$	$C_{24,10}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,3}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,11}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,4}$	1	1	1	12	$80 = 2^4 \cdot 5$	$C_{24,12}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,5}$	1	1	1	12	$32 = 2^5$	$C_{24,13}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,6}$	1	1	1	12	$32 = 2^5$	$C_{24,14}$	1	1	1	15	$48576 = 2^6 \cdot 3 \cdot 11 \cdot 23$
$C_{24,7}$	1	1	1	12	$32 = 2^5$	$C_{24,15}$	1	1	1	12	$80 = 2^4 \cdot 5$
$C_{24,8}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,16}$	1	1	1	12	$24 = 2^3 \cdot 3$

Πίνακας 5.5: $[48, 24]$ αυτοδυϊκοί κώδικες από τους πίνακες skew-Hadamard τάξεως 24

Ο κώδικας $C_{24,14}$ είναι ακραίος καθώς το φράγμα για $n = 24$ από το Θεωρήμα 23 είναι 15.

§5.2.2 Κατασκευή Αυτοδυϊκών Κωδίκων πάνω από το $\mathrm{GF}(5)$

Σε αυτήν την ενότητα, παρουσιάζουμε αυτοδυϊκούς κώδικες με μήκη από 8 εώς 56 πάνω από το $\mathrm{GF}(5)$, οι οποίοι παράγονται από τους μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 4 εώς 28. Το κίνητρο μας να παρουσιάσουμε μια πλήρη μελέτη για αυτές τις τάξεις των πινάκων skew-Hadamard έγγειται στο γεγονός ότι οι αντίστοιχες τάξεις αυτών των πινάκων είναι πλήρως καθορισμένη για τάξεις εώς 28, όπως ήδη αναφέραμε στην περίπτωση των τριαδικών αυτοδυϊκών κωδίκων.

Υπολογίσαμε το ελάχιστο βάρος των παραγόμενων αυτοδυϊκών κωδίκων για κάθε πιθανή λύση της διοφαντικής εξίσωσης του Θεωρήματος 22 πάνω από το $\mathrm{GF}(5)$. Στα αποτέλεσματα που ακολουθούν, δίνουμε για κάθε μη-ισοδύναμο πίνακα skew-Hadamard μόνο τους αντίστοιχους μη-ισοδύναμους αυτοδυϊκούς κώδικες που παράγονται και την τάξη των

ομάδων αυτομορφισμών αυτών των κωδίκων. Όπως και στην περίπτωση των τριαδικών αυτοδυϊκών κωδίκων, για έναν αυτοδυϊκό κώδικα ο οποίος παράγεται από τον i-ο μη-ισοδύναμο πίνακα skew-Hadamard τάξεως n θα χρησιμοποιήσουμε το συμβολισμό $C_{n,i}$.

[8, 4] **Αυτοδυϊκοί Κώδικες πάνω από το** GF(5) Σε αυτή την ενότητα, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(5) οι οποίοι παράγονται από το μοναδικό πίνακα skew-Hadamard τάξεως 4. Τα αποτελέσματα μας παρουσιάζονται στο Παράδειγμα 26.

Στο επόμενο παράδειγμα εφαρμόζουμε το Θεώρημα 22 για να διερευνήσουμε την ύπαρξη υψηλής απόστασης αυτοδυϊκών κωδίκων μήκους 8 και διάστασης 4, που κατασκευάζονται από τον μοναδικό πίνακα skew-Hadamard τάξης 4 (λαμβάνοντας υπόψιν την ισοδυναμία).

Παράδειγμα 26 Ο πίνακας skew-Hadamard τάξης 4 είναι ο $H = C + I_4$, όπου

$$C = \begin{bmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 1 & -1 & 0 \end{bmatrix} \text{ και } I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ορίζουμε $G = [aI\ cH - bI]$ και παράγουμε τον ακόλουθο $[8, 4, d]$ αυτοδυϊκό κώδικα πάνω από το GF(5).

C	a	b	c	d	Aut(C)
$C_{4,1}$	1	2	1	4	$768 = 2^8 \cdot 3$

Πίνακας 5.6: $[8, 4]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 4

[16, 8] **Αυτοδυϊκοί Κώδικες πάνω από το** GF(5) Σε αυτήν την ενότητα, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(5) οι οποίοι παράγονται από το μοναδικό πίνακα skew-Hadamard τάξεως 8, H_8, που δώσαμε σε προηγούμενη ενότητα.

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)
$C_{8,1}$	1	1	2	7	$1344 = 2^6 \cdot 3 \cdot 7$

Πίνακας 5.7: $[16, 8]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 8

$[24, 12]$ **Αυτοδυϊκοί Κώδικες πάνω από το** $GF(5)$ Σε αυτήν την ενότητα, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το $GF(5)$ οι οποίοι παράγονται από το μοναδικό πίνακα skew-Hadamard τάξεως 12, H_{12}, που δώσαμε σε προηγούμενη ενότητα.

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)
$C_{12,1}$	1	2	2	9	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$

Πίνακας 5.8: $[24, 12]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξεως 12

Από τους πίνακες του Gaborit ([53]) το υψηλότερο φράγμα στο ελάχιστο βάρος για τους $[24, 12]$ αυτοδυϊκούς κώδικες εκτείνεται από 9 εώς 10. Πρόσφατα, στην εργασία [103] αποδείχθηκε ότι δεν υπάρχει ένας $[24, 12]$ αυτοδυϊκός κώδικας του οποίου το ελάχιστο βάρος είναι 10 πάνω από το $GF(5)$. Συνεπώς, μπορούμε να αποφανθούμε ότι ο κώδικας $C_{12,1}$ είναι βέλτιστος ανάμεσα στην κλάση των $[24, 12]$ αυτοδυϊκών κωδίκων. Επιπλέον, ο κώδικας $C_{12,1}$ είναι ισοδύναμος με τον τετραγωνικά διπλά κυκλκό κώδικα μήκους 24 (QDC_{24}). Πρόσφατα, ένας ακόμη αυτοδυϊκός κώδικας με παραμέτρους $[24, 12, 9]$ πάνω από το $GF(5)$ κατασκευάστηκε στην [100].

$[32, 16]$ **Αυτοδυϊκοί Κώδικες πάνω από το** $GF(5)$ Σε αυτήν την ενότητα, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το $GF(5)$ οι οποίοι παράγονται από τους δύο μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 16. Οι πίνακες skew-Hadamard που χρησιμοποιήσαμε είναι οι

$$H_{16,1} = \begin{pmatrix}
+&+&+&+&+&+&+&+&+&+&+&+&+&+&+&+\\
-&+&+&-&+&-&+&-&-&+&+&-&+&-&+&-\\
-&-&+&+&-&+&+&-&-&-&+&+&-&+&-&+\\
-&+&-&+&+&+&-&-&-&+&-&+&+&+&-&-\\
-&-&+&-&+&+&-&+&-&-&+&-&+&+&+&-\\
-&+&-&-&-&+&+&+&-&+&-&-&-&+&+&+\\
-&-&-&+&+&-&+&-&-&+&+&+&-&-&+&+\\
-&+&+&-&-&+&-&+&+&+&-&-&-&+&-&+\\
-&+&+&+&+&+&+&+&-&-&-&-&-&-&-&-\\
-&-&+&-&+&-&+&-&+&-&+&-&+&-&+&+\\
-&-&-&+&-&+&+&-&+&+&+&-&+&-&+&+\\
-&+&-&-&+&+&-&-&+&-&+&+&-&+&+&+\\
-&-&+&-&-&+&-&+&+&-&+&+&+&-&+&+\\
-&+&-&-&-&-&+&+&-&+&+&+&+&-&-&-\\
-&-&-&+&+&-&-&+&+&+&+&-&-&+&+&-\\
-&+&+&+&-&-&-&+&-&-&-&+&+&+&+&+
\end{pmatrix}, H_{16,2} = \begin{pmatrix}
+&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-\\
+&+&-&+&-&+&-&+&+&-&-&+&-&+&-&+\\
+&+&+&-&+&-&-&+&+&+&-&-&+&-&-&+\\
+&-&+&+&-&-&+&+&-&+&+&+&-&-&+&+\\
+&+&-&+&+&-&+&-&+&-&+&+&+&-&-&-\\
+&-&+&+&+&+&-&-&+&-&+&+&+&-&-&-\\
+&+&+&-&-&+&+&-&+&+&+&-&-&+&-&-\\
+&-&-&-&+&+&+&+&-&-&-&+&+&+&-&+\\
+&-&-&-&-&-&-&-&+&+&+&+&+&+&+&+\\
+&+&-&+&-&+&-&+&-&+&+&-&+&-&+&-\\
+&+&+&-&+&-&-&+&-&-&+&+&-&+&-&+\\
+&-&+&+&-&-&+&-&+&+&-&+&-&+&+&-\\
+&+&-&+&+&-&+&-&-&+&-&+&+&-&-&-\\
+&-&+&+&+&-&-&+&-&-&-&+&+&+&+&+\\
+&+&+&-&-&+&+&-&-&-&-&+&+&-&+&+\\
+&-&-&-&+&+&+&+&-&+&+&+&-&-&-&+
\end{pmatrix}$$

όπου με '+' και '−' συμβολίζουμε τα στοιχεία 1 και −1, αντίστοιχα.

Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)
$C_{16,1}$	1	1	3	8	$172032 = 2^{13} \cdot 3 \cdot 7$
	1	1	4	10	$1344 = 2^6 \cdot 3 \cdot 7$
$C_{16,2}$	1	1	3	8	$172032 = 2^{13} \cdot 3 \cdot 7$
	1	1	4	10	$1344 = 2^6 \cdot 3 \cdot 7$

Πίνακας 5.9: $[32, 16]$ αυτοδυϊκοί κώδικες από τους πίνακες skew-Hadamard τάξεως 16

$[40, 20]$ **Αυτοδυϊκοί Κώδικες πάνω από το** $\mathsf{GF}(5)$ Σε αυτήν την ενότητα, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το $\mathsf{GF}(5)$ οι οποίοι παράγονται από τον μοναδικό πίνακα skew-Hadamard τάξεως 20, H_{20}, που δώσαμε σε προηγούμενη ενότητα. Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)
$C_{20,1}$	1	1	1	13	$54720 = 2^6 \cdot 3^2 \cdot 5 \cdot 19$

Πίνακας 5.10: $[40, 20]$ αυτοδυϊκός κώδικας από τον πίνακα skew-Hadamard τάξης 20

Σημειώνουμε ότι, ένας αυτοδυϊκός κώδικας με παραμέτρους $[40, 20, 13]$ κατασκευάστηκε στην [170].

[48, 24] **Αυτοδυϊκοί Κώδικες πάνω από το** GF(5) Σε αυτήν την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(5), οι οποίοι προκύπτουν από τους δεκαέξι μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 24. Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα.

C	a	b	c	d	Aut(C)	C	a	b	c	d	Aut(C)
$C_{24,1}$	1	2	1	10	$1536 = 2^9 \cdot 3$	$C_{24,9}$	1	2	1	10	$192 = 2^6 \cdot 3$
$C_{24,2}$	1	2	1	10	$144 = 2^3 \cdot 3^2$	$C_{24,10}$	1	2	1	10	$192 = 2^6 \cdot 3$
$C_{24,3}$	1	2	1	10	$1536 = 2^9 \cdot 3$	$C_{24,11}$	1	2	1	10	$192 = 2^6 \cdot 3$
$C_{24,4}$	1	2	1	10	$160 = 2^5 \cdot 5$	$C_{24,12}$	1	2	1	10	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,5}$	1	2	1	10	$64 = 2^6$	$C_{24,13}$	1	2	1	10	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,6}$	1	2	1	10	$128 = 2^7$	$C_{24,14}$	1	2	1	14	$48576 = 2^6 \cdot 3 \cdot 11 \cdot 23$
$C_{24,7}$	1	2	1	10	$128 = 2^7$	$C_{24,15}$	1	2	1	10	$160 = 2^5 \cdot 5$
$C_{24,8}$	1	2	1	10	$192 = 2^6 \cdot 3$	$C_{24,16}$	1	2	1	10	$144 = 2^3 \cdot 3^2$

Πίνακας 5.11: [48, 24] αυτοδυϊκοί κώδικες από τους πίνακες skew-Hadamard τάξεως 24

Οι πίνακες skew-Hadamard που χρησιμοποιήσαμε μπορούν να βρεθούν στην ιστοσελίδα που δίνεται στην [145].
Από τους πίνακες του Gaborit ([53]) το υψηλότερο φράγμα στο ελάχιστο βάρος για [48, 24] αυτοδυϊκούς κώδικες εκτείνεται από 14 εώς 20. Ο μοναδικός γνωστός αυτοδυϊκός κώδικας που επιτυγχάνει το κάτω φράγμα που ισούται με 14 είναι ο τετραγωνικά διπλά κυκλικός κώδικας μήκους 48 (QDC_{48}). Ελέγξαμε αν ο κώδικας μας $C_{24,14}$ είναι ισοδύναμος με τον προηγούμενο βέλτιστο κώδικα QDC_{48}, και η απάντηση είναι *αρνητική*. Επιπλέον, υπολογίσαμε ότι $\mathtt{Aut}(QDC_{48})$ είναι 192. Συνεπώς, έχουμε τουλάχιστον δύο μη-ισοδυνάμους [48, 24] αυτοδυϊκούς κώδικες πάνω από το GF(5). Σημειώνουμε ότι για την περίπτωση $a = 1, b = 2, c = 1$, ο $cH - bI = C + I - 2I = C - I$ είναι ένας πίνακας Hadamard εφόσον ο πίνακας $C + I$ είναι skew-Hadamard. Αυτοδυϊκοί κώδικες από πίνακες Hadamard τάξεως 24 επίσης έχουν μελετηθεί στην [101].

[56, 28] **Αυτοδυϊκοί Κώδικες πάνω από το** GF(5) Σε αυτήν την παράγραφο, θα μελετήσουμε αυτοδυϊκούς κώδικες πάνω από το GF(5), οι οποίοι προκύπτουν από τους 54 μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 28, οι οποίοι έχουν αναχθεί από τους 65 μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 28 που δίνονται στην [218].

Σημειώνουμε ότι, σε αυτήν την περίπτωση δίνουμε την τάξη της ομάδας αυτομορφισμού μόνο για τον καλύτερο κώδικα που υπολογίσαμε λόγω του ότι ο υπολογιστικός χρόνος αυξάνει εκθετικά σε αυτή την περίπτωση. Τα αποτελέσματα τα οποία παράγαμε εφαρμόζοντας το Θεώρημα 22 παρουσιάζονται στον ακόλουθο πίνακα. Οι πίνακες skew-Hadamard που χρησιμοποιήσαμε μπορούν να βρεθούν στην ιστοσελίδα που δίνεται στην [145].

C	a	b	c	d	C	a	b	c	d	C	a	b	c	d
$C_{28,1}$	1	1	2	12	$C_{28,22}$	1	1	2	12	$C_{28,43}$	1	1	2	14
$C_{28,2}$	1	1	2	12	$C_{28,23}$	1	1	2	12	$C_{28,44}$	1	1	2	12
$C_{28,3}$	1	1	2	12	$C_{28,24}$	1	1	2	12	$C_{28,45}$	1	1	2	12
$C_{28,4}$	1	1	2	12	$C_{28,25}$	1	1	2	14	$C_{28,46}$	1	1	2	12
$C_{28,5}$	1	1	2	12	$C_{28,26}$	1	1	2	12	$C_{28,47}$	1	1	2	12
$C_{28,6}$	1	1	2	12	$C_{28,28}$	1	1	2	12	$C_{28,49}$	1	1	2	14
$C_{28,7}$	1	1	2	12	$C_{28,29}$	1	1	2	12	$C_{28,50}$	1	1	2	12
$C_{28,8}$	1	1	2	12	$C_{28,30}$	1	1	2	12	$C_{28,51}$	1	1	2	12
$C_{28,9}$	1	1	2	12	$C_{28,31}$	1	1	2	12	$C_{28,53}$	1	1	2	12
$C_{28,10}$	1	1	2	12	$C_{28,33}$	1	1	2	12	$C_{28,55}$	1	1	2	12
$C_{28,12}$	1	1	2	12	$C_{28,34}$	1	1	2	12	$C_{28,56}$	1	1	2	12
$C_{28,13}$	1	1	2	12	$C_{28,35}$	1	1	2	12	$C_{28,57}$	1	1	2	12
$C_{28,14}$	1	1	2	12	$C_{28,36}$	1	1	2	12	$C_{28,58}$	1	1	2	12
$C_{28,16}$	1	1	2	12	$C_{28,37}$	1	1	2	12	$C_{28,60}$	1	1	2	14
$C_{28,17}$	1	1	2	12	$C_{28,38}$	1	1	2	12	$C_{28,61}$	1	1	2	12
$C_{28,19}$	1	1	2	12	$C_{28,40}$	1	1	2	14	$C_{28,62}$	1	1	2	14
$C_{28,20}$	1	1	2	12	$C_{28,41}$	1	1	2	12	$C_{28,63}$	1	1	2	16
$C_{28,21}$	1	1	2	12	$C_{28,42}$	1	1	2	14	$C_{28,65}$	1	1	2	12

Πίνακας 5.12: $[56, 28]$ αυτοδυϊκοί κώδικες από τους πίνακες skew-Hadamard τάξεως 28

Από τους πίνακες του Gaborit ([53]) το υψηλότερο φράγμα στο ελάχιστο βάρος για $[56, 28]$ αυτοδυϊκούς κώδικες εκτείνεται από 16 εώς 23. Ο μοναδικός γνωστός αυτοδυϊκός κώδικας που επιτυγχάνει το κάτω φράγμα που ισούται με 16 είναι ο τετραγωνικά διπλά κυκλικός κώδικας μήκους 56 (QDC_{56}), ο οποίος και συμβολίζεται με $C_{5,56}$ στην [53]. Ελέγξαμε αν ο κώδικας μας $C_{28,63}$ είναι ισοδύναμος με τον προηγούμενο βέλτιστο κώδικα $C_{5,56}$, και η απάντηση είναι *αρνητική*. Επιπλέον, υπολογίσαμε ότι $\mathrm{Aut}(C_{28,63})$ είναι $4368 = 2^4 \cdot 3 \cdot 7 \cdot 13$. Συνεπώς, έχου-

με τουλάχιστον δύο μη-ισοδυνάμους $[56, 28]$ αυτοδυϊκούς κώδικες πάνω από το $\mathsf{GF}(5)$.

Ένας $[72, 36]$ **Αυτοδυϊκός Κώδικας πάνω από το** $\mathsf{GF}(5)$ Χρησιμοποιήσαμε έναν από τους δεκαοχτώ μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 36 που δίνονται στην [145] για να σχηματίσουμε ένα γεννήτορα πίνακα G της μορφής $\mathsf{G} = [\mathrm{I}_{36}\ 3\mathsf{H} - \mathrm{I}_{36}]$ για $a = b = 1$, $c = 3$ και $p = 5$ στο Θεώρημα 22. Ο πίνακας G παράγει έναν αυτοδυϊκό κώδικα μήκους 72 και διάστασης 36. Δίνουμε παρακάτω τις γραμμές του υποπίνακα $3\mathsf{H} - \mathrm{I}_{36}$ του γεννήτορα πίνακα G του $[72, 36]$ αυτοδυϊκού κώδικα πάνω από το $\mathsf{GF}(5)$.

222232333333233322223222223232223233
322223233332333223232222232322232332
332222323323333223332222232222323323
333222232233322333222223223223233232
233322223333223332222232232232332322
323332222332233323222322322323323222
232333222322333233223223222233232223
223233322223332333232232222332322232
222323332233323333232232222323222323
222322233222232333323222323333332332
223222332322223233232222323333323323
232223322332222323322232332333233233
322233222333222232222323323332332333
222332223233322223223233232323323333
223322232323332222232332322233233333
233222322223233322232332322233233332
332223222223233322233232223323333323
322232223222323332332322232233333233
332333332232333232222232333233323332
323333323323332322322223233333233322
233333233233323223332222323332333223
333332332333232232333222232323332233
333323323332322323233322223233322333
333233233323223233323332222333223332
332332333232232333232333222332233323
323323333322323332223233322322333233
233233333223233323222323332223332333
323332322222223223322232223222232333
233323223222232232222322233222223233
333232232222322322223222332332222323
332322323223223222232223322332222232
323223233232232222322233222233322223
232223233322322222222332223323332222
322323332223222223223322232232333222
223233323232222232233222322223233322
232333232322222322332223222222323332

Υπολογισμός του Ελαχίστου Βάρους του $[72, 36]$ **Αυτοδυϊκού Κώδικα πάνω από το** $\mathsf{GF}(5)$ Χρησιμοποιήσαμε το Magma, ένα πακέτο υπολογίστικης άλγεβρας εξειδικευμένο για πράξεις που αφορούν συμβολικούς υπολογισμούς το οποίο έχει αναπτυχθεί από το Πανεπιστή-

μιο του Sydney ([15, 83]), για να υπολογίσουμε το ελάχιστο βάρος του $[72, 36]$ αυτοδυϊκού κώδικα που κατασκευάσαμε προηγουμένως. Δίνουμε παρακάτω τις λεπτομέρειες της τελευταίας φάσης αυτού του υπολογισμού για το μήκος 72.

```
Linear Code over GF(5) of length 72 with 36 generators.
Enumerating using 8 generators at a time:
Completed Matrix  1:
lower = 16, upper = 16.
Computation complete
72574065912 vectors enumerated
in total (0.000000% of 72 36 code)
Final Results: lower = 16, upper = 16
IsSelfDual: True
```

Θεώρημα 24 *Υπάρχει ένας* $[72, 36, 16]$ *αυτοδυϊκός κώδικας πάνω από το* $\mathrm{GF}(5)$.

Ένας $[80, 40]$ **Αυτοδυϊκός Κώδικας πάνω από το** $\mathrm{GF}(5)$ Χρησιμοποιήσαμε έναν πίνακα skew-Hadamard τάξης 40 ο οποίος κατασκευάζεται μέσω μιας τεχνικής διπλασιασμού ([205]) του μοναδικού πίνακα skew-Hadamard) τάξης 20 για να σχηματίσουμε έναν γεννήτορα G της μορφής $G = [I_{40}\ H - I_{40}]$ για $a = 1$ πάνω από το $\mathrm{GF}(5)$. Ο πίνακας G παράγει έναν αυτοδυϊκό κώδικα μήκους 80 και διάστασης 40. Δίνουμε παρακάτω τις γραμμές του υποπίνακα $H - I_{40} = C$ του γεννήτορα πίνακα G του $[80, 40]$ αυτοδυϊκού κώδικα πάνω από το $\mathrm{GF}(5)$.

```
0141411111441114411111144141114141141411 4014111111411144111411441411111411414114
1401411111111441114414411111144114141141 4140111111114411144144111111411141411414
1414011111144111441141114114111414114141 4444401414441111144414111444114141114144
4444440141411141444141111441141411441441 4444414014111444441111114411444114114414
4444441401114414411411141114441141444141 4444414140144114114411411144411414141414
1144411444014141111141414141411444144 144411444140141111111414441411111444144
4441144411140141111141441141141144114444 441144411441401111111441441141144144441
4114441144141401111144141114144411144414 114444411144444014141414114141441444144
1444141114444444014141411414114144444411 444111114444444140141411414114144444114
4411411441444444140141141411414444141144 411441441144444141401141411414444141144
4441141444141414141401414111114411411441 441141444441411141444014111111411441411
4114444441141144144114014111111144444111 114444441441141144144140111111144414114
1444144144114144414114140111114441111144 414441114441414414414444401414114411441
1444411441141441414444444401411441114411 444411441141441414414444441401444111441111
```

```
444144411114414144144444441401411144111 4414441114441414414144444141401114411144
141441414414441114111144144111401414111111 414414144144411141111441141144401411111
144141441444114411111441111144414014111111 441414414141144111144111414444141401111111
414144141411444111411111444441114140111111 141444141111411411144411444114444401414
414411411414111111444114441144444444401411 144144111414111111441114441144444444014
441411141411111414411144411444144444441401 414141414111141441114441144144114444414140
```

Υπολογισμός του Ελαχίστου Βάρους του $[80, 40]$ **Αυτοδυϊκού Κώδικα πάνω από το** $\mathrm{GF}(5)$ Χρησιμοποιήσαμε το Magma ([15, 83]), όπως και στην περίπτωση του $[72, 36]$ αυτοδυϊκού κώδικα, για να υπολογίσουμε το ελάχιστο βάρος του $[80, 40]$ αυτοδυϊκού κώδικα που κατασκευάσαμε προηγουμένως. Δίνουμε παρακάτω τις λεπτομέρειες της τελευταίας φάσης αυτού του υπολογισμού για το μήκος 80.

```
Linear Code over GF(5) of length 80 with 40 generators.
Enumerating using 8 generators at a time:
Completed Matrix  1:
lower = 17, upper = 17.
Computation complete
160937966256 vectors enumerated
in total (0.000000% of 80 40 code)
Final Results: lower = 17, upper = 17
IsSelfDual: True
```

Θεώρημα 25 *Υπάρχει ένας* $[80, 40, 17]$ *αυτοδυϊκός κώδικας πάνω από το* $\mathrm{GF}(5)$.

Ένας $[88, 44]$ **Αυτοδυϊκός Κώδικας πάνω από το** $\mathrm{GF}(5)$ Χρησιμοποιήσαμε έναν από τους πέντε μή-ισοδύναμους πίνακες skew-Hadamard τάξεως 44 που δίνονται στην [133] για να σχηματίσουμε έναν γεννήτορα πίνακα G της μορφής $G = [I_{44}\ C + I_{44}]$ για $a = b = c = 1$ και $p = 5$ στην κατασκευή του Θεωρήματος 21. Ο πίνακας G παράγει έναν αυτοδυϊκό κώδικα μήκους 88 και διάστασης 44. Δίνουμε παρακάτω τις γραμμές του υποπίνακα $C + I_{44}$ του γεννήτορα πίνακα G του $[88, 44]$ αυτοδυϊκού κώδικα πάνω από το $\mathrm{GF}(5)$.

```
1444414111114444114444114141141411411441141 1144441411144441144441141411414111414411411
1114444141144411444414411411411411141144114111 1111444414144114444144141141411411441141114
1111144441441144441444411414111141144114111141 4111114444111444414444114141114144411411411
1411111444414444144441141411141411411141144114 4141111144444441444411414111414111411141144
4414111114444414444114141141141141141141111411 4441411111444144441144411141411414111411411
4444141111141444411444111414114141411141144114 4111144111114444141111114114411414414414414
```

```
111144111141144441411114114411411414144144144 111441111411114444141141144114111141441414444
114411141111114444141114411411144144144144441 144111141111111444414144114111411441441444414
441111411114111114444144114111411441414444141 411114111141411114444411411141144144144414144
111141111444141111144411411141144144144144144 111411114414414111114414111411441414444141441
114111144114441411111441114114411144144144144 141111441114444141111111141144114444414144141
441414414144414411441414444141111144444144444 414144141444144114414411444414111444441144441
141441414444144114414441114444414114441144444 414144141444144114414441111144444141441144444
```

```
144141444144114414441411111444414411444414444 441414441411144144414441111114444111444414444
414144414141441444414411411111444414444144441 141444141444414441441141411111444444414444411
414441414414144144414411444141111144444144444114 144414144141444144114444414111114441444411144
444141441414444144114414444414111114144441144444 441441144141141411414141111441111144444141111
414411441441414114141111114411114114444414111 144114414444141141411111144111141111444414411
441144144411411414111411441111411111114444141 411441444144114141114114411114111111111444414
114414444144114141114144411114111141111144441 144144414411414111414141111411114141111144444
441444144114141111414111111411114441411111444 414441441141411141141141141111441144141111144
144414411444111414114111411114411444144141111114 444144114411111414114141411114411144441411111
```

Υπολογισμός του Ελαχίστου Βάρους του $[88, 44]$ **Αυτοδυϊκού Κώδικα πάνω από το** $\mathrm{GF}(5)$ Δίνουμε παρακάτω τις λεπτομέρειες της τελευταίας φάσης του υπολογισμού του ελαχίστου βάρους για το μήκος 88.

```
Linear Code over GF(5) of length 88 with 44 generators.
Enumerating using 9 generators at a time:
Completed Matrix  1:
lower = 19, upper = 19.
Computation complete
52596981369064 vectors enumerated
in total (0.000000% of 88 44 code)
Final Results: lower = 19, upper = 19
IsSelfDual: True
```

Θεώρημα 26 *Υπάρχει ένας* $[88, 44, 19]$ *αυτοδυϊκός κώδικας πάνω από το* $\mathrm{GF}(5)$.

§5.2.3 Βέλτιστες Ελάχιστες Αποστάσεις Αυτοδυϊκών Κωδίκων πάνω από το $\mathrm{GF}(5)$

Σε αυτήν την ενότητα, δίνουμε έναν ανανεωμένο πίνακα με τις καλύτερες εώς σήμερα βέλτιστες ελάχιστες αποστάσεις αυτοδυϊκών κωδίκων πάνω από το GF(5), ο οποίος και συνοψίζει τα αποτελέσματα μας σε σύγκριση με τα υπάρχουσα στην βιβλιογραφία. Η πρώτη και η πέμπτη στήλη του πίνακα δίνει τα μήκη των κωδίκων, η δεύτερη και η έκτη στήλη δίνει τις βέλτιστες ελάχιστες αποστάσεις για αυτοδυϊκούς κώδικες πάνω από το GF(5), ενώ η τρίτη και η έβδομη στήλη δίνει τον αριθμό των μή-ισοδύναμων βέλτιστων αυτοδυϊκών κωδίκων.

Μήκος	d	N	Αναφορά	Μήκος	d	N	Αναφορά
2	2	1	[170]	28	$10-11$	≥ 20	[54, 95, 123]
4	2	1	[170]	30	$10-12$	≥ 204	[54, 95]
6	4	1	[170]	32	$11-12$	≥ 1	[54, 95, 123]
8	4	1	[170]	34	$11-12$	≥ 11	[54, 95, 123]
10	4	3	[170]	36	$12-13$	≥ 1	[54, 123]
12	6	1	[170]	38	$12-14$	≥ 1	[54, 123]
14	6	3	[104, 170]	40	$13-15$	≥ 1	[54, 123, 154]
16	7	1	[104, 170]	48	$14-20$	≥ 2	[54, 154]
18	7	9	[104, 123]	56	$16-23$	≥ 2	[54, 154]
20	8	≥ 8	[123, 170]	72	$16-?$	≥ 1	[155]
22	8	≥ 59	[123]	80	$17-?$	≥ 1	[154]
24	9	≥ 2	[93, 100, 103, 154, 170]	88	$19-?$	≥ 1	[154]
26	$9-10$	≥ 1	[54, 95, 123]				

Πίνακας 5.13: Βέλτιστες ελάχιστες αποστάσεις αυτοδυϊκών κωδίκων πάνω από το GF(5)

§5.2.4 Κατασκευή Αυτοδυϊκών Κωδίκων πάνω από το GF(7)

Για $[56, 28]$ αυτοδυϊκούς κώδικες πάνω από το GF(7), το υψηλότερο ελάχιστο βάρος είναι 16 και προκύπτει από τον τετραγωνικά διπλά κυκλικό κώδικα μήκους 56, ([52],[53]). Πρόσφατα, στην [126] δόθηκαν ακόμα έξι μη-ισοδύναμοι $[56, 28, 16]$ αυτοδυϊκοί κώδικες. Σε αυτή την ενότητα, δίνουμε έναν νέο $[56, 28]$ αυτοδυϊκό κώδικα πάνω από το GF(7),

του οποίου το ελάχιστο βάρος είναι 17, βελτιώνοντας με αυτόν τον τρόπο τα γνωστά κάτω φράγματα στο υψηλότερο γνωστό βάρος ανάμεσα σε όλους τους $[56, 28]$ αυτοδυϊκούς κώδικες.

Ένας $[56, 28]$ **Αυτοδυϊκός κώδικας πάνω από το** $GF(7)$ Χρησιμοποιήσαμε έναν από τους 54 μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 28, οι οποίοι έχουν αναχθεί από τους 65 μη-ισοδύναμους πίνακες skew-Hadamard τάξεως 28 που δίνονται στην [218] για να σχηματίσουμε έναν γεννήτορα πίνακα G της μορφής $G = [I_{28}\ 2H - I_{28}]$ για $a = 1$, $b = 1$ και $c = 2$ πάνω από το $GF(7)$. Σημειώνουμε ότι, ο πίνακας skew-Hadamard που χρησιμοποιήσαμε ήταν ο ίδιος πίνακας που έδωσε το υψηλότερο ελάχιστο βάρος για αυτοδυϊκούς κώδικες με ίδιες παραμέτρους πάνω από το $GF(5)$. Δίνουμε παρακάτω τις γραμμές του υποπίνακα $2H - I_{28}$ του γεννήτορα πίνακα G του $[56, 28]$ αυτοδυϊκού κώδικα πάνω από το $GF(7)$.

$$
\begin{array}{c}
12222222222222222222222222 \\
51222222222222255555555555 \\
55122222255555522222225555 \\
55512222522555522255555222 \\
55551225225225555222555225 \\
55555122552252222522525525 \\
55555512225252252252525225 \\
55552551252522222522555522 \\
55525255152222552255222525 \\
55525522155252255555222255 \\
55252525521522555522222552 \\
55225552522125525252552252 \\
55225225555512252552255222 \\
55222555525251225222525525 \\
55222555252255152525522252 \\
52552525252525215255222255 \\
52552255222252521552225525 \\
52525555252252521222522555 \\
52525525225225522512255555 \\
52525525522555222552152252 \\
52522522555252555552122525 \\
52522252555522555225512222 \\
52255522555222522525522555 \\
52255252252255555522255122 \\
52255225522555525225525252 \\
52252555552252222525525215 \\
52225525252552525252552255 \\
\end{array}
$$

Δίνουμε παρακάτω τις λεπτομέρειες της τελευταίας φάσης του υπολογισμού του ελάχιστου βάρους για το μήκος 56.

```
Linear Code over GF(7) of length 56 with 28 generators.
Enumerating using 8 generators at a time:
Completed Matrix  1:
```

```
lower = 17, upper = 17.
Computation complete
7235498131806 vectors enumerated
in total (0.000000% of 56 28 code)
Final Results: lower = 17, upper = 17
IsSelfDual: True
```

Θεώρημα 27 *Υπάρχει ένας* $[56, 28, 17]$ *αυτοδυϊκός κώδικας πάνω από το* $\mathrm{GF}(7)$.

Επιπλέον, υπολογίσαμε την τάξη της ομάδας αυτομορφισμού αυτού του κώδικα και βρήκαμε ότι είναι ίση με $13104 = 2^4 \cdot 3^2 \cdot 7 \cdot 13$.

§5.3 Κατασκευή Μέγιστης Απόστασης Διαχωρίσιμων (MDS) Αυτοδυϊκών Κωδίκων πάνω από Πρώτα Πεπερασμένα Σώματα

Μέχρι σήμερα, ελάχιστοι ερευνητές [3, 8, 62] έχουν μελετήσει αυτοδυϊκούς κώδικες πάνω από σωματα μεγέθους μεγαλύτερου του 9. Για την ακρίβεια, ο de Boer [13] δίνει $[20, 10, 10]$ αυτοδυϊκούς κώδικες πάνω από τα $\mathrm{GF}(11)$ και $\mathrm{GF}(17)$, και έναν $[18, 9, 9]$ κώδικα πάνω από το $\mathrm{GF}(13)$. Στην [8] έχουν μελετηθεί αυτοδυϊκοί κώδικες πάνω από το $\mathrm{GF}(p)$ για $p = 11, 13, 17, 19, 23$ και 29. Η ταξινόμηση αυτοδυϊκών κωδίκων πάνω από αυτά τα σώματα για μικρά μήκη επίσης παρουσιάστηκε στην ίδια εργασία. Ορισμένοι μικροί αυτοδυϊκοί κώδικες με καλές ιδιότητες πάνω από τα $\mathrm{GF}(31)$ και $\mathrm{GF}(37)$ παρουσιάστηκαν στην [62].

Ένας $[n, k, n-k+1]_p$ γραμμικός κώδικας πάνω από το $\mathrm{GF}(p)$, θα καλείται *μέγιστης απόστασης διαχωρίσιμος (MDS)* αν ικανοποιεί την ισότητα στο φράγμα του Singleton, $d \leq n-k+1$ [215]. Το πεπερασμένο σώμα Galois, $\mathrm{GF}(p)$, θα καλείται πρώτο, αν το p είναι πρώτος. Οι μέγιστης απόστασης διαχωρίσιμοι κώδικες (MDS κώδικες) βρίσκονται στην καρδιά της Συνδυαστικής και των πεπερασμένων γεωμετριών. Στο βιβλίο τους [176] οι Mac Williams και Sloane αναφέρονται στους MDS κώδικες ως "Ένα από τα πιο συναρπαστικά κεφάλαια της Θεωρίας κωδίκων". Αυτοί οι κώδικες μπορούν να είναι γραμμικοί ή μη-γραμμικοί. Σε αυτή την ενότητα, θα εστιάσουμε στη γραμμική περίπτωση. Οι MDS κώδικες έχουν μελετηθεί για τις καθαρά συνδυαστικές τους ιδιότητες. Για

παράδειγμα, συνδέονται με την ύπαρξη συνδυαστικών δομών όπως των αμοιβαία ορθογωνίων Λατινικών τετραγώνων (mutually orthogonal Latin squares) και των ορθογώνιων σχηματισμών (orthogonal arrays) [176], καθώς και με την ύπαρξη γεωμετρικών δομών που καλούνται n-*τόξα (*n-*arcs)* [176]. Ένα από τα κύρια προβλήματα της Θεωρίας κωδίκων είναι να καθορίσει το μέγιστο μήκος ενός MDS κώδικα. Η ακόλουθη είναι μια δίασημη εικασία, γνωστή ως η κύρια εικασία για MDS κώδικες.

Εικασία 3 (Tsfasman και Vladut [228]) *Για έναν μη-τετριμμένο* $[n, k, n-k+1]$ *MDS κώδικα πάνω από το* $GF(q)$ *έχουμε ότι* $n \leq q+2$ *αν το* q *είναι άρτιος και* $k = 3$ *ή* $k = q-1$*, και* $n \leq q+1$ *διαφορετικά.*

Η προηγούμενη εικασία δεν έχει αποδειχθεί στην γενική της περίπτωση. Έχει όμως αποδειχθεί ότι ισχύει σε αρκετές περιπτώσεις, για παράδειγμα για κώδικες πάνω από το $GF(q)$ όπου $q \leq 27$, και για κώδικες με διάσταση $k \leq 5$ (για σχετικές αναφορές βλ. [110, 176] και τις εργασίες [21, 22]). Στην εργασία τους [20] οι Bruen, Thas, και Blokhuis δείξανε ότι η εικασία ισχύει τουλάχιστον ασυμπτωτικά. Μια βιβλιογραφική έρευνα για την κύρια εικασία των MDS κωδίκων δίνεται στην [109]. Η ύπαρξη και η πιθανή δομή μεγάλων MDS κωδίκων ήταν το κεντρικό θέμα της ομιλίας του J. A. Thas στο Διεθνές Συνέδριο Μαθηματικών το 1998 [224]. Προς αυτήν την κατεύθυνση, ο Alderson έδωσε στην εργασία του [1] ένα κριτήριο επεκτασιμότητας για το μήκος των MDS κωδίκων για άρτιο q. Πρόσφατα, βελτιώσεις αυτών των αποτελεσμάτων σχετικά με την επεκτασιμότητα των γραμμικών MDS κωδίκων εμφανίστηκαν στην [2].

Η απόκλιση Singleton για έναν $[n, k, d]$ κώδικα C ορίζεται ως $s(C) = n-k+1-d$ και δείχνει πόσο απέχει ο C από το να είναι MDS. Ένας κώδικας C με απόκλιση Singleton $s(C) = 1$, δηλαδή ένας $[n, k, n-k]$ κώδικας θα καλείται *σχετικά-MDS (almost-MDS)* (AMDS εν συντομία) [13]. Ένας $[n, k, n-k]$ AMDS κώδικας για τον οποίο ο δυϊκός κώδικας είναι επίσης ένας AMDS κώδικας, δηλαδή ισχύει ότι $s(C) = s(C^{\perp}) = 1$, θα καλείται σχεδόν-MDS (near-MDS) κώδικας (NMDS εν συντομία) [42].

Η σπουδαιότητα των NMDS κωδίκων έγγειται στο γεγονός ότι υπάρχουν NMDS κώδικες οι οποίοι είναι αρκετά μεγαλύτεροι από τους μέγιστους δυνατούς MDS κώδικες για δεδομένο μέγεθος του κώδικα και του αλφαβήτου. Επίσης, αυτοί οι κώδικες έχουν καλές δυνατότητες για διόρθωση σφαλμάτων [43] και ορισμένες φορές είναι δυνατό να παράγουν t-σχεδιασμούς (t-designs) [42]. NMDS κώδικες μέγιστου μήκους πάνω από το $GF(q)$, $8 \leq q \leq 11$ έχουν βρεθεί στην [179].

Πρόσφατα, κάποιοι ερευνητές (για παράδειγμα [62] και [124]) κατασκεύασαν MDS αυτοδυϊκούς κώδικες πάνω από μεγάλα πεπερασμένα

σώματα $GF(p)$ για μικρά μήκη. Ιδιαίτερα, MDS αυτοδυϊκοί κώδικες μήκους $4, 8, 12$ για $p = 31$ και MDS αυτοδυϊκοί κώδικες μήκους $2n \leq 14$ για $p = 37$ κατασκευάστηκαν στην [62] και MDS αυτοδυϊκοί κώδικες μήκους $2n \leq 10$ για $p = 41$ κατασκευάστηκαν στην [124]. MDS αυτοδυϊκοί κώδικες με μήκη $8, 10, 12$ και 16 για αρκετά πεπερασμένα σώματα κατασκευάστηκαν μέσω ορθογωνίων σχεδιασμών (orthogonal designs) και γενικευμένων ορθογώνιων σχεδιασμών (generalized orthogonal designs) στην [102]. Μια κατασκευή για MDS αυτοδυϊκούς κώδικες πάνω από δακτυλίους Galois δόθηκε στην [125], όπου παρουσιάζονται MDS και NMDS αυτοδυϊκοί κώδικες μήκους εώς 12.

§5.3.1 Αυτοδυϊκοί Κώδικες Παραγόμενοι από Λύσεις Διοφαντικών Εξισώσεων

Αυτοδυϊκοί κώδικες οι οποίοι παράγονται μέσω λύσεων διοφαντικών εξισώσεων έχουν κατασκευαστεί στις [62, 64, 66]. Υπενθυμίζουμε αυτές τις μεθόδους σε αυτήν την ενότητα, και τις επαναπροσδιόριζουμε κάτω από μια κατάλληλη αλγεβρική μοντελοποιήση. Θα δώσουμε μια μέθοδο κατασκευής αυτοδυϊκών κωδίκων που έχουν για γεννήτορα πίνακα G, έναν $n \times 2n$ πίνακα, της μορφής $G = [cI_n \; M]$ χρησιμοποιώντας έναν, δύο ή τέσσερις κυκλικούς πίνακες με έναν σύστημα διοφαντικών εξισώσεων.

Για να μπορέσουμε να παρουσιάσουμε αυτήν τη μέθοδο κατασκευής κατάλληλων κυκλικών ή block κυκλικών πινάκων M τάξης n με στοιχεία από το $GF(p)$ οι οποίοι ικανοποιούν την σχέση $MM^T = -cI_n$ για κάποιο $c \not\equiv 0 \pmod p$, $c \in GF(p)$, θα χρειάστουμε κάποιους βασικούς ορισμούς από τη Θεωρία σχεδιασμών. Ένας πίνακας M πάνω από το $GF(p)$ ο οποίος ικανοποιεί τη σχέση $MM^T = -c^2 I_n$ για ένα μη-μηδενικό στοιχείο c θα καλείται ένας *ορθογώνιος σχεδιασμός (orthogonal design)* πάνω από το $GF(p)$ [67].

Ορισμός 25 *Έστω* $A = \{A_j : A_j = \{a_{j1}, a_{j2}, \ldots, a_{jn}\},\ j = 1, \ldots, \ell\}$, *ένα σύνολο* ℓ *ακολουθιών μήκους* n. *Η μη-περιοδική συνάρτηση αυτοσυσχετίσης (non-periodic autocorrelation function), πάνω από το* $GF(p)$, $N_A(s)$ *(εν συντομία NPAF) των παραπάνω ακολουθιών ορίζεται ως*

$$N_A(s) = \left(\sum_{j=1}^{\ell} \sum_{i=1}^{n-s} a_{ji} a_{j,i+s} \right) \pmod p, \quad s = 0, 1, \ldots, n-1. \qquad (5.2)$$

Ορισμός 26 *Έστω* $A = \{A_j : A_j = \{a_{j1}, a_{j2}, \ldots, a_{jn}\},\ j = 1, \ldots, \ell\}$, *ένα σύνολο* ℓ *ακολουθιών μήκους* n. *Η περιοδική συνάρτηση αυτοσυσχετίσης (periodic autocorrelation function), πάνω από το* $GF(p)$, $P_A(s)$ *(εν συντομία PAF) των παραπάνω ακολουθιών ορίζεται ως*

$$P_A(s) = \left(\sum_{j=1}^{\ell} \sum_{i=1}^{n} a_{ji} a_{j,i+s} \right) \pmod{p}, \quad s = 0, 1, \ldots, n-1. \tag{5.3}$$

όπου το $i + s$ *υπολογίζεται modulo* n.

Είναι εύκολο να αποδειχθεί ότι $P_A(s) = P_A(n-s)$ και συνεπώς έχουμε να ελέχξουμε την $P_A(s)$ μόνον για όλα τα $s = 0, 1, \ldots, [n/2]$, όπου $[x]$ είναι ο πλησιέστερος ακέραιος του x. Για τα αποτελέσματα αυτής της ενότητας επαρκεί η ισχύς του PAF. Όμως NPAF ακολουθίες σημαίνουν την ύπαρξη PAF ακολουθιών, καθώς στις NPAF ακολουθίες μπορούμε να παραθέσουμε μηδενικά στο τέλος αυτών έτσι ώστε να σχηματίσουμε ακολουθίες μεγαλύτερου μήκους. Συνεπώς η ισχύς του NPAF μπορεί να δώσει γενικότερα αποτελέσματα. Ένας κυκλικός πίνακας E τάξης n με στοιχεία πρώτης γραμμής $e_{11}, e_{12}, \ldots, e_{1n}$ θα συμβολίζεται με $E = \mathrm{circ}(e_{11}, e_{12}, \ldots, e_{1n})$.

Διοφαντικές Εξισώσεις και Κατασκευή με έναν Κυκλικό Πίνακα Έστω $M = \mathrm{circ}(m_1, m_2, \ldots, m_n)$ ένας κυκλικός πίνακας τάξης n με στοιχεία από το $GF(p)$ ο οποίος ικανοποιεί τη σχέση $MM^T = fI_n$ όπου $f \equiv -c^2 \pmod{p}$, και c είναι ένα μη-μηδενικό στοιχείο του $GF(p)$. Για να βρούμε πίνακες τέτοιας μορφής πρέπει να λύσουμε το σύστημα διοφαντικών εξισώσεων που προκύπτει από τη σχέση (5.3). Ορίζουμε το σύστημα των αλγεβρικών εξισώσεων $S^1_{(n,p,c)}$ πάνω από το $GF(p)$ για την κατασκευή με έναν κυκλικό πίνακα ως ακολούθως:

$$S^1_{(n,p,c)} = \begin{cases} P_M(0) + c^2 \equiv 0 \pmod{p}, \\ P_M(s) \equiv 0 \pmod{p}, \quad s = 1, \ldots, [n/2]. \end{cases} \tag{5.4}$$

Το σύστημα $S^1_{(n,p,c)}$ έχει n αγνώστους και $[n/2]+1$ εξισώσεις. Ιδιαίερα, το $S^1_{(n,p,c)}$ ορίζεται ως:

$$S^1_{(n,p,c)} = \begin{cases} \left(\sum_{i=1}^{n} m_i^2 \right) + c^2 \equiv 0 \pmod{p}, \\ \left(\sum_{i=1}^{n} m_i m_{i+s} \right) \equiv 0 \pmod{p}, \quad s = 1, \ldots, [n/2] \\ \text{όπου το } i + s \text{ υπολογίζεται modulo } n, \text{όπου χρείαζεται.} \end{cases}$$

Κάθε λύση του συστήματος $S^1_{(n,p,c)}$ των $[n/2]+1$ διοφαντικών εξισώσεων παράγει έναν γεννήτορα πίνακα G της μορφής $G = [cI_n \ M]$ για έναν $[2n, n]$ αυτοδυϊκό κώδικα πάνω από το $GF(p)$ εφόσον $GG^T = [cI_n \ M][cI_n \ M]^T = c^2 I_n + MM^T$ και $MM^T = -c^2 I_n$.

Παράδειγμα 27 Έστω $M = \mathrm{circ}(m_1, m_2, m_3, m_4, m_5, m_6, m_7)$. Κατασκευάζουμε το σύστημα των διοφαντικών εξισώσεων όπως ορίστηκε στην μέθοδο 5.4 για $c = 1$ και $p = 37$.

$$S^1_{(7,37,1)} = \begin{cases} P_M(0) + 1 \equiv 0 \pmod{37}, \\ P_M(s) \equiv 0 \pmod{37}, \quad s = 1, 2, 3. \end{cases} \Longrightarrow$$

$$S^1_{(7,37,1)} = \begin{cases} \left(\sum_{i=1}^{7} m_i^2 \right) + 1 \equiv 0 \pmod{37}, \\ \left(\sum_{i=1}^{7} m_i m_{i+s} \right) \equiv 0 \pmod{37}, \quad s = 1, 2, 3 \\ \text{όπου το } i+s \text{ υπολογίζεται modulo } 7, \text{όπου χρείαζεται.} \end{cases}$$

Μια λύση αυτού του συστήματος των τεσσάρων διοφαντικών εξισώσεων είναι η $m_1 = 1, m_2 = 1, m_3 = 15, m_4 = 29, m_5 = 10, m_6 = 14, m_7 = 35$. Συνεπώς

$$G = [I_7 \ M] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 15 & 29 & 10 & 14 & 35 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 35 & 1 & 1 & 15 & 29 & 10 & 14 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 14 & 35 & 1 & 1 & 15 & 29 & 10 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 10 & 14 & 35 & 1 & 1 & 15 & 29 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 29 & 10 & 14 & 35 & 1 & 1 & 15 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 15 & 29 & 10 & 14 & 35 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 15 & 29 & 10 & 14 & 35 & 1 \end{pmatrix}.$$

Ο πίνακας G παράγει έναν γραμμικό $[14, 7, 8]$ αυτοδυϊκό MDS κώδικα πάνω από το $GF(37)$ με απαριθμητή βάρους $W(x, y) = x^{14} + 108108\, x^6 y^8 + 2090088\, x^5 y^9 + 38630592\, x^4 y^{10} + 504608832\, x^3 y^{11} + 4542167448\, x^2 y^{12} + 25156386864\, xy^{13} + 64687885200\, y^{14}$.

Στη συνέχεια παρουσιάζουμε ένα θεωρητικό αποτέλεσμα που αφορά τα συστήματα $S^1_{(n,p,1)}$ το οποίο απλουστεύει την σχέση της επιλυσιμότητας αυτών των συστημάτων με τετραγωνικά υπόλοιπα (quadratic residues).

Λήμμα 12 *Έστω* n *ένας θετικός ακέραιος και* $c = 1$*. Τότε για κάθε πρώτο αριθμό* $p \geq 3$ *έχουμε ότι, το* $S^1_{(n,p,1)}$ *έχει λύσεις πάνω από το* $GF(p)$ *αν και μόνον αν* $(p-1) \equiv 0 \pmod 4$.

Απόδειξη. Προσθέτοντας τις $[n/2]$ εξισώσεις του συστήματος $S^1_{(n,p,1)}$ κατά μέλος, παίρνουμε

$$\sum_{s=1}^{[n/2]} P_M(s) \equiv 0 \pmod p,$$

που είναι ισοδύναμο με

$$e_2 \equiv 0 \pmod p,$$

όπου με e_2 συμβολίζουμε την δεύτερη στοιχειώδης συμμετρική συνάρτηση (second elementary symmetric function) σε n μεταβλητές $m_1, \ldots, m_n$. Σημειώνουμε ότι για n άρτιο, n ισοτιμία $P_M(n/2) \equiv 0 \pmod p$ είναι ίση με το

$$2\left(\sum_{i=1}^{n/2} m_i m_{i+n/2}\right) \equiv 0 \pmod p$$

και εφόσον $(2, p) = 1$, μπορούμε να αγνοήσουμε τον παράγοντα του 2.

Ο τύπος Jacobi-Trudi, $e_2 = \frac{1}{2}(p_1^2 - p_2)$ (όπου p_1, p_2 είναι τα δυναμόαθροίσματα στις n μεταβλητές $m_1, \ldots, m_n$) συνεπάγεται ότι

$$p_1^2 - p_2 \equiv 0 \pmod p$$

και χρησιμοποιώντας την πρώτη εξίσωση του $S^1_{(n,p,1)}$, η προηγούμενη σχέση γίνεται

$$p_1^2 \equiv -1 \pmod p.$$

Η παραπάνω ισοτιμία έχει λύσεις αν και μόνον αν $(p-1) \equiv 0 \pmod 4$, δηλαδή όταν το -1 είναι τετραγωνικό υπόλοιπο των πρώτων αριθμών της μορφής $4k+1$ και ενα μη-τετραγωνικό υπόλοιπο των πρώτων αριθμών της μορφής $4k+3$, βλ. για παράδειγμα στο [116].

□

Σε ορισμένες περιπτώσεις, φαίνεται ότι είναι πειραματικά πιθανό να καθορίσουμε έναν τύπο για τον αριθμό των λύσεων του συστήματος $S^1_{(n,p,1)}$, για ένα συγκεκριμένο n και για όλους τους πρώτους αριθμούς p. Αναφέρουμε μια τέτοια περίπτωση στην ακόλουθη παρατήρηση για $n = 4$:

Παρατήρηση 15 *Η ακολουθία των (μη-μηδενικών) αριθμών των λύσεων του συστήματος* $S^{1}_{(4,p,1)}$ *δίνεται από:*

$$|S_{(4,p,1)}| = 4^2 \cdot a_n$$

όπου a_n *είναι η ακολουθία A005098 της Εγκυκλοπαίδειας των Ακεραίων Ακολουθιών του Sloane: για παράδειγμα η ακολουθία* $1, 3, 4, 7, 9, 10, 13, 15, 18, 22, 24, 25, 27, 28, 34, 37, 39, 43, 45, 48, 49, 57, 58, 60, 64, 67, 69, 70, 73, 78, 79, 84, 87, 88, 93, 97, 99, 100, 102, 105, 108, 112, 114, 115, 127, 130, 135, 139, 142, 144, 148, 150, 153, 154, 160, 163, 165, 168, 169, 175, 177, 183 \ldots$ *η οποία ορίζεται από τους*

Αριθμούς n τέτοιους ώστε ο $4n+1$ να είναι πρώτος.

Παρατήρηση 16 *Σημείωνουμε ότι, παρόλο που δεν καταφέραμε να αποδείξουμε την προηγούμενη δήλωση, αυτή προβλέπει ακριβώς τα υπολογιστικά αποτελέσματα που πήραμε για όλους τους περιττούς πρώτους αριθμούς* $p \equiv 1 \pmod 4$*, υπό την προϋπόθεση ότι* $p \leq 541$*.*

Διοφαντικές Εξισώσεις και Κατασκευή με δύο Block Κυκλικούς Πίνακες Έστω M ένας $2n \times 2n$ πίνακας, ο οποίος κατασκευάζεται από δυο κυκλικούς πίνακες $A_1 = \mathrm{circ}(a_{11}, a_{12}, \ldots, a_{1n})$ και $A_2 = \mathrm{circ}(a_{21}, a_{22}, \ldots, a_{2n})$ τάξεως n, της μορφής

$$M = \begin{pmatrix} A_1 & A_2 \\ -A_2^{\mathsf{T}} & A_1^{\mathsf{T}} \end{pmatrix}$$

με στοιχεία από το $\mathrm{GF}(p)$, ο οποίος ικανοποιεί τη σχέση $MM^{\mathsf{T}} = fI_{2n}$ όπου $f \equiv -c^2 \pmod p$, και c είναι ένα μη-μηδενικό στοιχείο του $\mathrm{GF}(p)$. Για να βρούμε πίνακες τέτοιας μορφής πρέπει να λύσουμε το σύστημα διοφαντικών εξισώσεων που προκύπτει από τη σχέση (5.3). Ορίζουμε το σύστημα των αλγεβρικών εξισώσεων $S^{2}_{(n,p,c)}$ πάνω από το $\mathrm{GF}(p)$ για την κατασκευή με δύο block κυκλικούς πίνακες ως ακολούθως:

$$S^{2}_{(n,p,c)} = \begin{cases} P_A(0) + c^2 \equiv 0 \pmod p, \\ P_A(s) \equiv 0 \pmod p, \quad s = 1, \ldots, [n/2]. \end{cases} \tag{5.5}$$

Το σύστημα $S^{2}_{(n,p,c)}$ έχει $2n$ αγνώστους και $[n/2]+1$ εξισώσεις. Ιδιαίτερα, το $S^{2}_{(n,p,c)}$ ορίζεται ως:

$$S^{\,2}_{(n,p,c)} = \begin{cases} \left(\sum_{j=1}^{2}\sum_{i=1}^{n} a_{ji}^2\right) + c^2 \equiv 0 \pmod p, \\ \left(\sum_{j=1}^{2}\sum_{i=1}^{n} a_{ji}a_{j,i+s}\right) \equiv 0 \pmod p, \quad s = 1,\ldots,[n/2] \\ \text{όπου το } i+s \text{ υπολογίζεται modulo } n, \text{όπου χρειάζεται.} \end{cases}$$

Κάθε λύση του συστήματος $S^{\,2}_{(n,p,c)}$ των $[n/2]+1$ διοφαντικών εξισώσεων παράγει έναν γεννήτορα πίνακα G της μορφής $G = [cI_{2n}\ M]$ για έναν $[4n, 2n]$ αυτοδυϊκό κώδικα πάνω από το GF(p) εφόσον $GG^T = [cI_{2n}\ M][cI_{2n}\ M]^T = c^2I_{2n} + MM^T$ και $MM^T = -c^2I_{2n}$.

Παράδειγμα 28 Έστω $A_1 = \mathrm{circ}(a_{11}, a_{12}, a_{13})$ και $A_2 = \mathrm{circ}(a_{21}, a_{22}, a_{23})$. Κατασκευάζουμε το σύστημα των διοφαντικών εξισώσεων όπως ορίστηκε στην μέθοδο 5.5 για $c = 1$ και $p = 41$.

$$S^{\,2}_{(3,41,1)} = \begin{cases} P_A(0) + 1 \equiv 0 \pmod{41}, \\ P_A(s) \equiv 0 \pmod{41}, \quad s = 1. \end{cases} \Longrightarrow$$

$$S^{\,2}_{(3,41,1)} = \begin{cases} \left(\sum_{j=1}^{2}\sum_{i=1}^{3} a_{ji}^2\right) + 1 \equiv 0 \pmod{41}, \\ \left(\sum_{j=1}^{2}\sum_{i=1}^{3} a_{ji}a_{j,i+s}\right) \equiv 0 \pmod{41}, \quad s = 1. \\ \text{όπου το } i+s \text{ υπολογίζεται modulo } 3, \text{όπου χρειάζεται.} \end{cases}$$

Μια λύση αυτού του συστήματος των δύο διοφαντικών εξισώσεων είναι n $a_{11} = 1, a_{12} = 1, a_{13} = 5, a_{21} = 1, a_{22} = 12, a_{23} = 14$. Συνεπώς

$$G = [I_6\ M] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 5 & 1 & 12 & 14 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5 & 1 & 1 & 14 & 1 & 12 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 5 & 1 & 12 & 14 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 40 & 27 & 29 & 1 & 5 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 29 & 40 & 27 & 1 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 27 & 29 & 40 & 5 & 1 & 1 \end{pmatrix}.$$

Ο πίνακας G παράγει έναν γραμμικό $[12, 6, 7]$ αυτοδυϊκό MDS κώδικα πάνω από το GF(41) με απαριθμητή βάρους $W(x, y) = x^{12} + 31680\,x^5y^7 + 673200\,x^4y^8 + 12152800\,x^3y^9 + 145685760\,x^2y^{10} + 1059593280\,xy^{11} + 3531967520\,y^{12}$.

Διοφαντικές Εξισώσεις και Κατασκευή με τέσσερις Block Κυκλικούς Πίνακες Έστω M ένας $4n \times 4n$ πίνακας, ο οποίος κατασκευάζεται από τέσσερις κυκλικούς πίνακες $A_i = \mathrm{circ}(a_{i1}, a_{i2}, \ldots, a_{in})$, $i = 1, 2, 3, 4$ τάξεως n, της μορφής

$$M = \begin{pmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & A_4^TR & -A_3^TR \\ -A_3R & -A_4^TR & A_1 & A_2^TR \\ -A_4R & A_3^TR & -A_2^TR & A_1 \end{pmatrix}$$

όπου $R = (r_{ij})$ είναι ο πίσω διαγώνιος πίνακας με στοιχεία από το $GF(p)$, ο οποίος ικανοποιεί τη σχέση $MM^T = fI_{4n}$ όπου $f \equiv -c^2 \pmod p$, και c είναι ένα μη-μηδενικό στοιχείο του $GF(p)$. Για να βρούμε πίνακες τέτοιας μορφής πρέπει να λύσουμε το σύστημα διοφαντικών εξισώσεων που προκύπτει από τη σχέση (5.3). Ορίζουμε το σύστημα των αλγεβρικών εξισώσεων $S^4_{(n,p,c)}$ πάνω από το $GF(p)$ για την κατασκευή με τέσσερις block κυκλικούς πίνακες ως ακολούθως:

$$S^4_{(n,p,c)} = \begin{cases} P_A(0) + c^2 \equiv 0 \pmod p, \\ P_A(s) \equiv 0 \pmod p, \quad s = 1, \ldots, [n/2]. \end{cases} \tag{5.6}$$

Το σύστημα $S^4_{(n,p,c)}$ έχει $4n$ αγνώστους και $[n/2] + 1$ εξισώσεις. Ιδιαίτερα, το $S^4_{(n,p,c)}$ ορίζεται ως :

$$S^4_{(n,p,c)} = \begin{cases} \left(\sum_{j=1}^{4} \sum_{i=1}^{n} a_{ji}^2 \right) + c^2 \equiv 0 \pmod p, \\ \left(\sum_{j=1}^{4} \sum_{i=1}^{n} a_{ji} a_{j,i+s} \right) \equiv 0 \pmod p, \quad s = 1, \ldots, [n/2] \\ \text{όπου το } i + s \text{ υπολογίζεται modulo } n, \text{όπου χρειάζεται.} \end{cases}$$

Κάθε λύση του συστήματος $S^4_{(n,p,c)}$ των $[n/2] + 1$ διοφαντικών εξισώσεων παράγει έναν γεννήτορα πίνακα G της μορφής $G = [cI_{4n}\ M]$ για έναν $[8n, 4n]$ αυτοδυϊκό κώδικα πάνω από το $GF(p)$ εφόσον $GG^T = [cI_{4n}\ M][cI_{4n}\ M]^T = c^2I_{4n} + MM^T$ και $MM^T = -c^2I_{4n}$.

Παράδειγμα 29 Έστω $A_1 = \mathrm{circ}(a_{11}, a_{12})$, $A_2 = \mathrm{circ}(a_{21}, a_{22})$, $A_3 = \mathrm{circ}(a_{31}, a_{32})$, $A_4 = \mathrm{circ}(a_{41}, a_{42})$. Κατασκευάζουμε το σύστημα των διοφαντικών εξισώσεων όπως ορίστηκε στη μέθοδο 5.6 για $c = 1$ και $p = 17$.

$$S^{\,4}_{(2,17,1)} = \begin{cases} P_A(0) + 1 \equiv 0 \pmod{17}, \\ P_A(s) \equiv 0 \pmod{17}, \quad s = 1. \end{cases} \Longrightarrow$$

$$S^{\,4}_{(2,17,1)} = \begin{cases} \left(\sum_{j=1}^{4} \sum_{i=1}^{2} a_{ji}^2 \right) + 1 \equiv 0 \pmod{17}, \\ \left(\sum_{j=1}^{4} \sum_{i=1}^{2} a_{ji} a_{j,i+s} \right) \equiv 0 \pmod{17}, \quad s = 1. \\ \text{όπου το } i + s \text{ υπολογίζεται modulo } 2, \text{όπου χρειάζεται.} \end{cases}$$

Μια λύση αυτού του συστήματος των δύο διοφαντικών εξισώσεων είναι η $a_{11} = 0, a_{12} = 0, a_{21} = 7, a_{22} = 5, a_{31} = 15, a_{32} = 6, a_{41} = 12, a_{42} = 8$. Συνεπώς

$$G = [I_8 \; M] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 7 & 6 & 15 & 8 & 12 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 5 & 15 & 6 & 12 & 8 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 12 & 10 & 0 & 0 & 8 & 12 & 11 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 10 & 12 & 0 & 0 & 12 & 8 & 2 & 11 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 11 & 2 & 9 & 5 & 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 11 & 5 & 9 & 0 & 0 & 7 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 9 & 5 & 6 & 15 & 12 & 10 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5 & 9 & 15 & 6 & 10 & 12 & 0 & 0 \end{pmatrix}.$$

Ο πίνακας G παράγει έναν γραμμικό $[16, 8, 7]$ αυτοδυϊκό κώδικα πάνω από το $GF(17)$ με απαριθμητή βάρους $W(x, y) = x^{16} + 3072\,x^9y^7 + 5440\,x^8y^8 + 81152\,x^7y^9 + 1327872\,x^6y^{10} + 11092480\,x^5y^{11} + 73017728\,x^4y^{12} + 362163200\,x^3y^{13} + 1239102208\,x^2y^{14} + 2644584960\,xy^{15} + 2644379328\,y^{16}$.

§5.3.2 Νέοι MDS Αυτοδυϊκοί Κώδικες

Σε αυτήν την ενότητα, παρουσιάζουμε τα αποτελέσματα τα οποία παράγαμε με υπολογιστική μελέτη. Συνολικά κατασκευάσαμε πάνω από 3 εκατομμύρια αυτοδυϊκούς κώδικες χρησιμοποιώντας τις μεθόδους 5.4, 5.5 και 5.6. Όπως και στην περίπτωση των αυτοδυικών κωδίκων πάνω από μικρά πεπερασμένα σώματα, χρησιμοποιήσαμε το Magma,

για να υπολογίσουμε την ελάχιστη απόσταση των παραγόμενων αυτοδυϊκών κωδίκων [15, 83].

Αποτελέσματα από την Κατασκευή με έναν Κυκλικό Πίνακα

Λήμμα 13 *Υπάρχουν* $[2n, n, n+1]$ *MDS αυτοδυϊκοί κώδικες, χρησιμοποιώντας την κατασκευή με έναν κυκλικό πίνακα, πάνω από το* $\mathsf{GF}(p)$ *για:*

(i) Μήκη $2n = 10$ *και* $p = 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197$.

(ii) Μήκη $2n = 14$ *και* $p = 13, 29, 37, 41$.

Δίνουμε ένα παρόμοιο Λήμμα για σχεδόν-MDS αυτοδυϊκούς κώδικες, για εκείνες τις περιπτώσεις για τις οποίες δεν βρήκαμε MDS αυτοδυϊκούς κώδικες.

Λήμμα 14 *Υπάρχουν* $[2n, n, n]$ *σχεδόν-MDS αυτοδυϊκοί κώδικες, χρησιμοποιώντας την κατασκευή με έναν κυκλικό πίνακα, πάνω από το* $\mathsf{GF}(p)$ *για:*

(i) Μήκη $2n = 8$ *και* $p = 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197$.

(ii) Μήκη $2n = 12$ *και* $p = 13, 17, 29, 37, 41, 53, 61$.

(iii) Μήκη $2n = 14$ *και* $p = 17, 41, 53, 61$.

(iv) Μήκη $2n = 16$ *και* $p = 13, 19, 29$.

Αποτελέσματα από την Κατασκευή με δύο Block Κυκλικούς Πίνακες

Λήμμα 15 *Υπάρχουν* $[4n, 2n, 2n+1]$ *MDS αυτοδυϊκοί κώδικες, χρησιμοποιώντας την κατασκευή με δύο block κυκλικούς πίνακες, πάνω από το* $\mathsf{GF}(p)$ *για:*

(i) Μήκη $4n = 12$ *και* $p = 11, 19, 23, 29, 31, 37, 41$.

Δίνουμε ένα παρόμοιο Λήμμα για σχεδόν-MDS αυτοδυϊκούς κώδικες, για εκείνες τις περιπτώσεις για τις οποίες δεν βρήκαμε MDS αυτοδυϊκούς κώδικες.

Λήμμα 16 *Υπάρχουν* $[4n, 2n, 2n]$ *σχεδόν-MDS αυτοδυϊκοί κώδικες, χρησιμοποιώντας την κατασκευή με δύο block κυκλικούς πίνακες, πάνω από το* $\mathsf{GF}(p)$ *για:*

(i) Μήκη $4n = 12$ *και* $p = 3, 5, 7, 13, 17$.

(ii) Μήκη $4n = 16$ *και* $p = 11, 13, 17, 19$.

Αποτελέσματα από την Κατασκευή με τέσσερις Block Κυκλικούς Πίνακες

Λήμμα 17 *Υπάρχουν* $[8n, 4n, 4n]$ *σχεδόν-MDS αυτοδυϊκοί κώδικες, χρησιμοποιώντας την κατασκευή με τέσσερις block κυκλικούς πίνακες, πάνω από το* $\mathsf{GF}(p)$ *για:*

(i) Μήκη $8n = 16$ *και* $p = 17, 29$.

Παρατήρηση 17 *Από τα αποτελέσματα που παρουσιάστηκαν σε αυτή την ενότητα, φαίνεται ότι η κύρια εικασία για* $[n, k, n - k + 1]$ *MDS κώδικες πάνω από το* $\mathsf{GF}(p)$ *(βλ. Εικασία 3) είναι αληθής για αυτοδυϊκούς κώδικες.*

§5.3.3 Βέλτιστοι Αυτοδυϊκοί Κώδικες πάνω από Μικρά Πρώτα Σώματα

Υπενθυμίζουμε ότι ένας αυτοδυϊκός κώδικας C καλείται *βέλτιστος ή ακραίος* αν ο C έχει το μεγαλύτερο ελάχιστο βάρος.

Ακραίοι Τριαδικοί Κώδικες από Διοφαντικές Εξισώσεις Επίσης, υπενθυμίζουμε ότι τα γνωστά φράγματα για την ελάχιστη απόσταση για το $\mathsf{GF}(3)$ δίνονται στις [198] και [226], μέσω του Θεωρήματος 23.

Σημειώνουμε ότι, πάνω από το $\mathsf{GF}(3)$ κατασκευάσαμε όλους τους ακραίους (βέλτιστους) $[n, n/2]$ τριαδικούς αυτοδυϊκούς κώδικες για μήκη $12 \leq n \leq 40$ μέσω λύσεων συστημάτων που προέρχονται από διοφαντικές εξισώσεις. Ιδιαίτερα, βρήκαμε τους ακόλουθους κώδικες.

Βέλτιστοι Αυτοδυϊκοί Κώδικες από Διοφαντικές Εξισώσεις πάνω από τα Πρώτα Σώματα $\mathsf{GF}(5)$ **και** $\mathsf{GF}(7)$ Στη συνέχεια, δίνουμε αποτελέσματα για $[n, n/2]$ αυτοδυϊκούς κώδικες για άλλα πρώτα σώματα

n	12	16	20	24	28	32	36	40
d	6	6	6	9	9	9	12	12

Πίνακας 5.14: Ακραίοι τριαδικοί αυτοδυϊκοί κώδικες για μήκη $12 \leq n \leq 40$.

συγκρίνοντας τα με τα καλύτερα διαθέσιμα γνωστά φράγματα χρησιμοποιώντας τους Πίνακες του Brouwer [19] και του Grassl [85]. Τα φράγματα σε αυτούς τους πίνακες δίνονται σε ένα εύρος κάτω-πάνω φράγματος. Τα κάτω φράγματα είναι κατασκευαστικά ενώ τα πάνω φράγματα έχουν βρεθεί μέσω γραμμικού προγραμματισμού (lienar programming) ή με διαγραφή (shortening) και επιμήκυνση (truncating) υπάρχουσων κωδίκων. Συνεπώς, θεωρούμε ότι ένας κώδικας είναι βέλτιστος αν επιτυγχάνει το μέγιστα δυνατό ελάχιστο βάρος ανάμεσα στους αυτοδυϊκούς κώδικες, δηλαδή επιτυγχάνει το κάτω (κατασκευαστικό) φράγμα αυτών των πινάκων.

Σημειώνουμε ότι, NMDS ή MDS κώδικες μηκρότερου μήκους πάνω από μεγάλα πρώτα σώματα δεν παρατίθενται στους ακόλουθους Πίνακες, καθώς τους παρουσιασάμε νωρίτερα σε προηγούμενη ενότητα. Επιπλέον, αν ένας κώδικας δεν αναφέρεται σε αυτούς τους πίνακες τότε αυτό σημαίνει ότι δεν υπήρχε επιτρεπτή τιμή στο αντίστοιχο σύστημα των διοφαντικών εξισώσεων, και συνεπώς δεν είχαμε λύσεις για αυτήν την περίπτωση.

Συμβολισμός 3 Στους ακόλουθους Πίνακες συμβολίζουμε με n το μήκος των αυτοδυϊκών κωδίκων, ενώ με $d_{max}(n)$ συμβολίζουμε το μέγιστο ελάχιστο βάρος που έχουμε βρεί. Τα κάτω και πάνω φράγματα σε αυτούς τους πίνακες προέρχονται από τους Πίνακες που βρίσκονται στις [19, 85] και συμβολίζονται με $[Lb, Ub]$.

Στην συνέχεια, δίνουμε αυτοδυϊκούς κώδικες μεγαλύτερου μήκους πάνω από το $GF(5)$ με καλές ιδιότητες ως προς το ελάχιστο βάρος.

§5.3.4 Βελτίωση του Pless-Pierce Φράγματος στο Ελάχιστο Βάρος των Αυτοδυϊκών Κωδίκων

Μήκος	$p = 5$		$p = 7$	
n	$d_{max}(n)$	$[Lb, Ub]$	$d_{max}(n)$	$[Lb, Ub]$
14	6	6	-	7
16	-	7	7	7
18	7	7-8	-	8
20	8	8-9	9	9
22	8	8-10	-	9-10
24	9	9-10	10	10-11

Πίνακας 5.15: Βέλτιστοι αυτοδυϊκοί κώδικες με μήκη $20 \leq n \leq 24$.

Μήκος	$p = 5$	
n	$d_{max}(n)$	$[Lb, Ub]$
26	9	10-11
28	10	11-12
30	10	12
32	10	11-13
34	10	11-14

Πίνακας 5.16: Καλοί αυτοδυϊκοί κώδικες με μήκη $26 \leq n \leq 34$.

Πρόσφατα, οι Kim και Lee [124] χρησιμοποίησαν το Pless-Pierce φράγμα [194] στο ελάχιστο βάρος των αυτοδυϊκών κωδίκων ως ένα κριτήριο για να εκτιμήσουν τα αποτελέσματα τους στους αυτοδυϊκούς (σχεδόν) MDS κώδικες πάνω από μεγάλα πεπερασμένα σώματα και κατάφεραν να το βελτιώσουν σε ορισμένες περιπτώσεις (βλ. [124, Πίνακας 1]).

Σε αυτήν την ένοτητα, τα αποτελέσματά μας (τα οποία εμφανίζονται με έντονη γραμματοσειρά) στο ελάχιστο βάρος των $[n, n/2]$ βέλτιστων ή MDS αυτοδυϊκών κωδίκων πάνω από πρώτα σώματα δίνουν ένα καλύτερο φράγμα από αυτό των Pless-Pierce (το οποίο εμφανίζεται στην παρένθεση) και το οποίο παράγεται από το τροποποιημένο Gilbert-Varshamov φράγμα.

n	$p = 5$
14	**6** (4)
16	**6** (5)
18	**7** (6)
20	**8** (6)
22	**8** (6)
24	**9** (7)
26	**9** (7)
28	**10** (8)
30	**10** (8)
32	**10** (8)
34	**10** (9)

Πίνακας 5.17: Ελάχιστα βάρη αυτοδυϊκών κωδίκων με μήκη $14 \leq n \leq 34$ πάνω από το $GF(5)$.

n	$p = 7$
16	**7** (6)
20	**9** (7)
24	**10** (8)

Πίνακας 5.18: Ελάχιστα βάρη βέλτιστων αυτοδυϊκών κωδίκων με μήκη $n \leq 24$ πάνω από το $GF(7)$.

n	$p = 41$
12	**7** (6)

Πίνακας 5.19: Ελάχιστο βάρος του $[12, 6]$ MDS κώδικα πάνω από το $GF(41)$.

In Galois fields,
full of flowers
primitive elements
dance for hours.

S. B. Weinstein (1970)

6

Πολυκυκλικοί Κώδικες

Στο έκτο αυτό κεφάλαιο, μελετούνται δυαδικοί πολυκυκλικοί (quasi-cyclic) κώδικες χρησιμοποιώντας στατιστικά εργαλεία από τους πειραματικούς σχεδιασμούς. Επιτυγχάνεται μια σύνδεση μεταξύ μιας δομημένης κυκλικής κλάσης στατιστικών σχεδιασμών, των k*-κυκλικών υπερκορεσμένων σχεδιασμών, και των πολυκυκλικών κωδίκων. Η μαθηματική δομή των παραγόμενων κωδίκων ερευνάται σε βάθος και επιτυγχάνεται η αντιστοιχία μεταξύ των συμπληρωματικά δυϊκών δυαδικών πολυκυκλικών (complementary dual binary quasi-cyclic) κωδίκων και* $\mathsf{E}(s^2)$*-βέλτιστων* k*-κυκλικών υπερκορεσμένων σχεδιασμών.*

Επιπλέον, διερευνώνται όλες οι περιπτώσεις οι οποίες δεν καλύπτονται από τη μέθοδό μας αλλά με κατάλληλη μοντελοποίηση μπορούν να ερευνηθούν με ευρετικές μεθόδους (heuristic methods). Η προσέγγιση μας βασίζεται στην εύρεση κωδίκων με καλές ιδιότητες που επιτυγχάνουν τα γνωστά κάτω φράγματα στην ελάχιστη απόσταση των γραμμικών κωδίκων, και η οποία μοντελοποιείται ως ένα πρόβλημα συνδυαστικής βελτιστοποίησης (combinatorial optimization). Ιδιαίτερα, δυαδικοί πολυκυκλικοί κώδικες με ρυθμούς 1/3, 1/4, 1/5, 1/6 *και* 1/7 *βρίσκονται υλοποιώντας έναν γενετικό αλγόριθμο (genetic algorithm).*

Ερευνώντας προηγούμενα αποτελέσματα, δείχνουμε ότι οι κώδικες που παράγονται από τη δοθείσα μέθοδο επιτυγχάνουν τα τωρινά καλύτερα γνωστά κάτω φράγματα στην απόσταση των γραμμικών κωδίκων με ίδιες παραμέτρους. Στο τέλος, παρουσιάζεται και μια σύνδεση των πολυκυκλικών κωδίκων με οπτικά ορθογώνιους κώδικες (optical orthogonal codes).

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στην επιστημονική εργασία [162].

§6.1 Εισαγωγή και Προηγούμενη Συνεισφορά

Υπενθυμίζουμε ότι, με $GF(q)$ θα συμβολίζουμε το σώμα Galois με q στοιχεία και ένας γραμμικός κώδικας C πανω από το $GF(q)$ μήκους n, διάστασης k, και ελάχιστης απόστασης Hamming d θα καλείται ένας $[n, k, d]_q$ κώδικας. Σε αυτό το κεφάλαιο, θα θεωρήσουμε το σώμα Galois με δύο στοιχεία, $GF(2)$. Ο ρυθμός (rate) ενός κώδικα ορίζεται ως το πηλίκο

$$r = \frac{k}{n}$$

είναι δηλαδή ο αριθμός των συμβόλων πληροφορίας ανά κωδικολέξη.

Ένας κώδικας C θα καλείται *πολυκυκλικός (quasi-cyclic)* (QC ή p-QC ή QC με δείκτη p) αν από μια κυκλική μετάθεση μιας κωδικολέξης κατά p θέσεις προκύπτει μια άλλη κωδικολέξη. Μια κυκλική μετάθεση μιας m-άδας $(x_0, x_1, \ldots, x_{m-1})$ είναι η m-άδα $(x_{m-1}, x_0, \ldots, x_{m-2})$. Ο ορισμός αυτός των πολυκυκλικών κωδίκων, είναι η γενίκευση των γνωστών κυκλικών κωδίκων, που είναι στην ουσία QC κώδικες για $p = 1$.

Το block μήκος n ενός p-QC κώδικα είναι ένα πολλαπλάσιο του p έτσι ώστε $n = pm$ (βλ. [88]). Ένας πίνακας B της μορφής

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \ldots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \ldots & b_{m-3} & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \ldots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ b_1 & b_2 & b_3 & \ldots & b_{m-1} & b_0 \end{bmatrix} \tag{6.1}$$

θα καλείται κυκλικός πίνακας (circulant matrix). Ένας κυκλικός πίνακας με πρώτη γραμμή $(b_0, b_1, \ldots, b_{m-1})$ θα συμβολίζεται με $\mathrm{circ}(b_0, b_1, \ldots, b_{m-1})$ ή απλούστερα με τη διατεταγμένη λίστα $[b_0, b_1, \ldots, b_{m-1}]$. Μια κλάση των QC κωδίκων μπορεί να κατασκευαστεί από $m \times m$ κυκλικούς πίνακες (με μια κατάλληλη μετάθεση των συντεταγμένων τους [131]). Σε αυτήν την περίπτωση, ο γεννήτορας πίνακας G του p-QC κώδικα μπορεί να αναπαρασταθεί ως

$$G = [B_1 \; B_2 \; \ldots \; B_p]. \tag{6.2}$$

όπου B_i, $i = 1, \ldots, p$ είναι ένας κυκλικός πίνακας ([211]).
Η άλγεβρα των $m \times m$ κυκλικών πινάκων πάνω από το $GF(p)$ είναι ισομορφική με την άλγεβρα των πολυωνύμων στο δακτύλιο $GF(q)[x]/(x^m - 1)$

έαν ο B απεικονιστεί στο πολυώνυμο $b(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{m-1}x^{m-1}$, το οποίο έχει τον λιγότερα σημαντικό συντελεστή στα αριστερά, και σχηματίζεται από τα στοιχεία της πρώτης γραμμής του B. Τα πολυώνυμα $b_i(x)$, $i = 1, \ldots, p$ που συσχετίζονται με έναν p-QC κώδικα καλούνται τα οριστικά πολυώνυμα (defining polynomials) του κώδικα [88]. Επιπλέον, ένας p-QC κώδικας πάνω από το $GF(q)$ μήκους $n = pm$ μπορεί να θεωρηθεί ως ένα υποπρότυπο (submodule) $GF(q)[x]/(x^m - 1)$ του $(GF(q)[x]/(x^m - 1))^p$ ([211]). Τότε ένας QC κώδικας με s-γεννήτορες παράγεται από s στοιχεία του $(GF(q)[x]/(x^m - 1))^p$. Η αλγεβρική δομή ενός QC κώδικα πάνω από ένα πεπερασμένο σώμα και των αντίστοιχων γεννητόρων του, μελετήθηκε διεξοδικά στην [171]. Σε αυτό το κεφάλαιο, θα θεωρήσουμε QC κώδικες που έχουν μόνον ένα γεννήτορα.

Οι πολυκυκλικοί κώδικες σχηματίζουν μια σημαντική κλάση των γραμμικών κωδίκων, η οποία εμπεριέχει την γνώστη κλάση των κυκλικών κωδίκων. Αυτοί οι κώδικες είναι μια φυσική γενίκευση των γνωστών κυκλικών κωδίκων. Συνεπώς, οι πολυκυκλικοί κώδικες είναι δομημένοι κώδικες που μπορούν να παραχθούν, κωδικοποιηθούν και αποκωδικοποιηθούν ευκολότερα και ταχύτερα από τυχαίους ή μη-δομημένους κώδικες. Οι πολυκυκλικοί κώδικες ερευνήθηκαν πρώτα από τους Townsend και Weldon [227], Karlin [119] και Chen et al. [23]. Η πανέμορφη δομή και απλότητα τους προσέλκυσε αρκετούς ερευνητές σε αυτό το πεδίο έρευνας, δες για παράδειγμα [9, 24] και τις αναφορές μέσα σε αυτές τις εργασίες.

Η μελέτη των QC κωδίκων έχει ως κίνητρο τα ακόλουθα γεγονότα: οι QC επιτυγχάνουν το τροποποιήμενο Gilbert-Varshamov φράγμα [120], μερικοί από τους καλύτερους τετραγωνικούς κώδικες υπολοίπων (quadratic residue codes) και Pless συμμετρικούς κώδικες είναι QC κώδικες [176], ένας μεγάλων αριθμός βέλτιστων κωδίκων είναι QC κώδικες [85], και υπάρχει μια αντιστοιχία μεταξύ QC κωδίκων και συνελικτικών (convolutional) κωδίκων [47]. Επιπρόσθετα, οι QC κώδικες είναι γνωστοί ως καλοί κώδικες [233]. Η πολυπλοκότητα αποκωδικοποίησης είναι διαχειρίσιμη [119], και πολλοί QC κώδικες είναι λογικά αποκωδικοποιήσιμοι [89]. Ο Chen συντηρεί μια βάση δεδομένων με δυαδικούς QC κώδικες που μπορεί να βρεθεί στην [25].

Ένας συμπληρωματικά δυϊκός γραμμικός κώδικας (linear code with a complementary dual) (εν συντομία LCD κώδικας) ορίστηκε στην [180] ως ένας γραμμικός κώδικας C του οποίου ο δυϊκός κώδικας $C^\perp$ ικανοποιεί τη σχέση $C \cap C^\perp = \{0\}$. Αποδείχθηκε στην [180] ότι ασυμπτωτικά καλοί γραμμικοί LCD κώδικες υπάρχουν και ότι οι LCD κώδικες διέπονται από άλλες ελκυστικές ιδιότητες. Στην [212], ο Sendrier υποδεικνύει ότι οι συμπληρωματικά δυϊκοί γραμμικοί κώδικες επιτυγχάνουν το ασυμπτω-

τικό Gilbert-Varshamov φράγμα. Περαιτέρω, η πρακτική χρησιμότητα των LCD κωδίκων επιδεικνύεται στην [181]. Πρόσφατα, οι Esmaeilli και Yari αναγνώρισαν ορισμένες κλάσεις LCD πολυκυκλικών κωδίκων στην [46].

Ερευνητικό Πρόβλημα 7 *Η κατασκευή δυαδικών πολυκυκλικών κωδίκων που διέπονται από καλές ιδιότητες και η πιθανή αλληλεπίδραση τους με μαθηματικές δομές που προέρχονται από την Θεωρία σχεδιασμών. Η κατάλληλη μοντελοποίηση της εύρεσης της ελάχιστης απόστασης των πολυκυκλικών κωδίκων ως ένα πρόβλημα συνδυαστικής βελτιστοποίησης και η υλοποίηση σχετικών ευρετικών αλγορίθμων.*

§6.2 Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων και Πειραματικών Σχεδιασμών

Στη συνέχεια, θα αναπτύξουμε τα απαραίτητα εργαλεία που χρησιμοποίησαμε για την κατασκευή μας από τους χώρους της αλγεβρικής Θεωρίας κωδίκων και των πειραματικών σχεδιασμών (experimental designs).

§6.2.1 Δυαδικοί Συμπληρωματικά Δυϊκοί Πολυκυκλικοί Κώδικες

Σε αυτήν την ενότητα, εξερευνούμε τους δυαδικούς LCD QC κώδικες από την αλγεβρική τους σκοπιά. Παραθέτουμε ένα αποτέλεσμα του Massey [181], το οποίο χαρακτηρίζει πλήρως τους LCD κώδικες, και θα παίξει καθοριστικό ρόλο στην αναζήτηση LCD QC κωδίκων με καλές ιδιότητες από κυκλικά-δομημένους σχεδιασμούς.

Πρόταση 14 (Massey [181]) *Αν* G *είναι ο γεννήτορας πίνακας για έναν* $[n, k]$ *γραμμικό κώδικα* C*, τότε ο* C *είναι ένας LCD κώδικας αν και μόνον αν ο* $k \times k$ *πίνακας* GG^T *είναι μη-ιδιάζων (δηλ. αντιστρέψιμος).*

Κάποιος θα πρέπει να ειναι ιδιαίτερα προσεχτικός, όταν υπολογίζει τον GG^T πάνω από ένα πεπερασμένο σώμα. Στην περίπτωση μας, ο

πολλαπλασιασμός των πινάκων γίνεται χρησιμοποιώντας την αριθμητική του GF(2) καθώς διερευνούμε δυαδικούς γραμμικούς κώδικες. Πάνω από ένα πεπερασμένο σώμα, ο πίνακας GG^T είναι μη-ιδιάζων αν και μόνον αν η αντίστοιχη τιμή της ορίζουσας (η οποία και είναι ένα στοιχείο του σώματος) είναι μη-μηδενική. Αν περιοριστούμε στη περίπτωση των QC κωδίκων έχουμε τη δυνατότητα να εκμεταλλευτούμε την ειδική δομή του G για να βρούμε κατάλληλες συνθήκες έτσι ώστε ο GG^T να είναι μη-ιδιάζων πάνω από το GF(2).

Σε αυτήν την ενότητα θεωρούμε συστηματικούς κώδικες ρυθμού $1/p$ καθώς έχουν ιδιαίτερη πρακτική χρησιμότητα, ενώ αντιθέτως οι μη-συστηματικοί κώδικες δεν αποκωδικοποιούνται εύκολα καθώς ορισμένοι κυκλικοί πίνακες δεν έχουν αντίστροφο. Επίσης, ένας κώδικας ρυθμού $1/p$ μπορεί να γραφεί στην συστηματική μορφή του αν ένας από τους κυκλικούς πίνακες του γεννήτορα πίνακα είναι αντιστρέψιμος. Αυτό μπορεί να συμβεί όταν ένας από τους κυκλικούς πίνακες της σχέσης (6.2) έχει πλήρη βαθμό m, συνεπώς μπορεί να μετασχηματιστεί στον μοναδιαίο πίνακα I_m με στοιχειώδεις μετασχηματισμούς γραμμών. Επιπλέον μεταθέσεις των κυκλικών πινάκων μπορούν να μετατοπίσουν τον μοναδιαίο πίνακα στο αριστερό block του G. Αυτό δεν είναι δυνατό μόνον όταν όλοι οι πίνακες είναι μη-αντιστρέψιμοι. Ευτυχώς, κώδικες οι οποίοι αποτελούνται αποκλειστικά από μη-αντιστρέψιμους κυκλικούς πίνακες είναι ένα μικρό υποσύνολο των δυνατών QC κωδίκων [7], και σπάνια περιέχονται στους βέλτιστους κώδικες. Συνεπώς, για ένα μικρό υπολογιστικό πλεονέκτημα θα υποθέσουμε ότι $B_1 = I_m$ έτσι ώστε ένας συστηματικός QC κώδικας ρυθμού $1/p$ να έχει έναν $m \times pm$ γεννήτορα πίνακα της μορφής

$$G = [I_m \; B_2 \; \ldots \; B_p]. \tag{6.3}$$

με πλήρη δίασταση m.

Ένας $[pm, m]$ QC κώδικας για να είναι LCD θα πρέπει να υπολογίσουμε την μορφή του ακόλουθου $m \times m$ πίνακα, καθώς ο G είναι ένας διαχωρισμένος (partitioned) πίνακας,

$$GG^T = I_m + \sum_{i=2}^{m} B_i B_i^T \tag{6.4}$$

Λαμβάνοντας υπόψιν ότι οι κυκλικοί πίνακες σχηματίζουν μια μεταθετική άλγεβρα καθώς για οποιουσδήποτε δύο κυκλικούς πίνακες A και B, το άθροισμα $A + B$ είναι κυκλικός πίνακας, το γινόμενο AB είναι επίσης κυκλικός πίνακας και $AB = BA$, και επιπλέον ο ανάστροφος

ενός κυκλικού πίνακα είναι επίσης κυκλικός πίνακας. Συνεπώς μπορούμε να αποφανθούμε ότι ο GG^T είναι ένας κυκλικός πίνακας. Επειδή $(B_i B_i^T)^T = B_i^T B_i = B_i B_i^T$ τότε ο GG^T είναι στην πραγματικότητα ένας κυκλικός συμμετρικός πίνακας πάνω από το $GF(2)$. Άρα ενδιαφέρομαστε για την περίπτωση όπου ένας $(0,1)$ κυκλικός συμμετρικός πίνακας πάνω από το $GF(2)$ είναι μη-ιδιάζων. Συνθήκες που αφορούν την ορίζουσα πινάκων αυτής της μορφής μπορούν να βρεθούν στην [202]. Καθώς η τιμή της ορίζουσας στο $GF(2)$ μπορεί να πάρει μόνο τις τιμές 0 ή 1, εστιάζουμε στην περίπτωση των αντιστρέψιμων πινάκων που έχουν ορίζουσα ίση με 1. Στη θεωρία ομάδων, αυτοί οι πίνακες σχηματίζουν την ειδική γραμμική ομάδα (special linear group), η οποία συμβολίζεται με $SL(m, GF(2))$ και η οποία είναι υποομάδα της γενικής γραμμικής ομάδας (general linear group) $GL(m, GF(2))$ με τις πράξεις του πολλαπλασιασμού και αντιστροφής πινάκων. Επειδή, πάνω από πεπερασμένα σώματα οι ιδιοτιμές ενός πίνακα έχουν περιορισμένη χρησιμότητα, επικεντρώνουμε το ενδιαφέρον μας στην εύρεση γεννητόρων πινάκων G απο τους οποίους μπορούμε να υπολογίσουμε την ορίζουσα του GG^T με μικρό κόστος.

§6.2.2 Υπερκορεσμένοι Σχεδιασμοί

Ένας σχεδιασμός δύο επιπέδων θα καλείται κορεσμένος όταν ο αριθμός m των παραγόντων (στηλών) ισούται με $n-1$, όπου n είναι ο αριθμός των πειραματικών εκτελέσεων (γραμμών). Ένας υπερκορεσμένος σχεδιασμός (supersaturated design) είναι ένας παραγοντικός σχεδιασμός (factorial design) δύο επιπέδων, στον οποίο ο αριθμός των πειραματικών εκτελέσεων n είναι μικρότερος του αριθμού των παραγόντων m, δηλαδή ισχύει ότι $n < m$. Για κάθε παράγοντα ενός σχεδιασμού δυο επιπέδων υπάρχουν δύο δυνατές επιλογές τιμών που είναι γνωστές ως επίπεδα (levels), και μπορούν να κωδικοποιηθούν ως ± 1. Κάθε συνδυασμός των επιπέδων όλων των παραγόντων καλείται συνδυασμός αγωγών (treatment combination). Έστω $\mathbf{X} = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m]$ να είναι ο πίνακας σχεδιασμού (design matrix) του πειράματος στο οποίο, κάθε γραμμή αναπαριστά τους n συνδυασμούς αγωγών και κάθε στήλη δίνει την ακολουθία των επιπέδων των παραγόντων. Για κάθε παράγοντα, και οι δυό τιμές των επιπέδων έχουν το ίδιο ενδιαφέρον και κάθε πειραματικό αποτέλεσμα θα πρέπει να ασκεί την ίδια επιρροή. Συνεπώς θεωρούμε σχεδιασμούς με την ιδιότητα ίσων εμφανίσεων (equal occu-

rrence property), όπου όλες οι στήλες αποτελούνται από $\frac{n}{2}$ στοιχεία ίσα με 1 και $\frac{n}{2}$ στοιχεία ίσα με -1, όταν το n είναι άρτιο. Οι σχεδιασμοί με την ιδιότητα ίσων εμφανίσεων θα καλούνται ισσοροπημένοι σχεδιασμοί (balanced designs).

k-**Κυκλικοί Υπερκορεσμένοι Σχεδιασμοί** Για να κατασκευάσουν τον μεγάλο αριθμό παραγόντων που απαιτείται για έναν υπερκορεσμένο σχεδιασμό, οι Liu και Dean στην [173] πρότειναν την κυκλική μετάθεση των στοιχείων ενός γεννήτορα, k στοιχείων την φορά. Ονόμασαν έναν τέτοιο σχεδιασμό ως k-κυκλικό υπερκορεσμένο σχεδιασμό. Αυτοι οι σχεδιασμοί είναι μια γενίκευση των Plackett και Burman σχεδιασμών ([192]), που είναι 1-κυκλικοί κορεσμένοι σχεδιασμοί. Γενικότερα, ο γεννήτορας ενός k-κυκλικού υπερκορεσμένου σχεδιασμού παρέχει την πρώτη γραμμή του πίνακα σχεδιασμού $\mathbf{X}$. Κάθε επόμενη γραμμή του $\mathbf{X}$ παράγεται από την προηγούμενη γραμμή μετακινόντας τα τελευταία k στοιχεία στις k πρώτες γραμμές και μεταθέτοντας τα υπόλοιπα k στοιχεία στα δεξιά. Εναλλακτικά, ένας k-κυκλικός υπερκορεσμένος σχεδιασμός μπορεί να παραχθεί από τον πίνακα 1-κυκλικού σχεδιασμού, επιλέγοντας τις γραμμές $1, k+1, \ldots, m-k+1$. Και στις δύο περιπτώσεις μια γραμμή με μονάδες επισυνάπτεται στον σχεδιασμό.

Το επόμενο θεώρημα, το οποίο αποδείχθηκε από τους Liu και Dean στην [173], δηλώνει τις ικανές και αναγκαίες συνθήκες για την ύπαρξη δύο επιπέδων k-κυκλικών υπερκορεσμένων σχεδιασμών με την ιδιότητα ίσων εμφανίσεων.

Θεώρημα 28 (Liu and Dean [173]) *Έστω* D *ένας* k*-κυκλικός υπερκορεσμένος σχεδιασμός σε* n *εκτελέσεις και* m *παράγοντες, ο καθένας από τους οποίους έχει δύο επίπεδα κωδικοποιημένα ως* $+1$ *και* -1*. Υποθέτουμε ότι, οι γραμμές του σχεδιασμού* D *παράγονται από τον γεννήτορα* $(g_1, g_2, \ldots, g_m)$ *με κυκλική εναλλαγή* k*-στοιχείων σε κάθε βήμα και προσθέτοντας μια γραμμή από* $+1$*. Ικανές και αναγκαίες συνθήκες έτσι ώστε ο* D *να είναι ισσοροπημένος είναι οι ακόλουθες:*

1. $n = 2t$, $m = (2t-1)k$, *για κάποιο θετικό ακέραιο* t.
2. *ο γεννήτορας περιέχει ακριβώς* kt *στοιχεία ίσα με* -1 *και* $(kt-k)$ *στοιχεία ίσα με* $+1$.
3. $\sum_{u=0}^{2t-2} g_{uk+j} + 1 = 0,\ i = 1, \ldots, k.$

Παράδειγμα 30 Ένας 2-κυκλικός σχεδιασμός για $m = 22$ παράγοντες σε $n = 12$ εκτελέσεις μπορεί να παραχθεί από τον ακόλουθο γεννήτορα,

$$(-+--+-+++---++--+--+-+)$$

με επαναλαμβανομένη κυκλική εναλλαγή 2 θέσεων προς τα δεξιά και μετακινώντας τα τελευταία δύο στοιχεία στις πρώτες δύο θέσεις. Αυτή η διαδικασία παράγει τις πρώτες έντεκα γραμμές του πίνακα σχεδιασμού $\mathbf{X}$. Η δωδέκατη γραμμή με τις μονάδες τότε προστίθεται στο τέλος για να παραχθεί ένας ισσοροπημένος σχεδιασμός, με τον ακόλουθο πίνακα σχεδιασμού $\mathbf{X}$.

$$\mathbf{X} = \left[\begin{array}{c} -+--+-+++---++--+--+-+ \\ \hline -+-+--+-+++---++--+--+- \\ -+-+-+--+-+++---++--+-- \\ +--+-+-+--+-+++---++--+- \\ --+--+-+-+--+-+++---++-- \\ ++--+--+-+-+--+-+++---+- \\ --++--+--+-+-+--+-+++--+ \\ +--+--+-+--+-+-+--+--++ \\ ++++---++--+-+-+--+---+- \\ +-++++--++--+-+-+--+--+- \\ --+-+++--++--+-+-+--+-+- \\ ++++++++++++++++++++++++ \end{array}\right]$$

§6.3 Κατασκευή Δυαδικών Πολυκυκλικών Κωδίκων από k-Κυκλικούς Υπερκορεσμένους Σχεδιασμούς

Σε αυτήν την ενότητα, παρουσιάζουμε μια μοντελοποίηση που μας επιτρέπει να θεωρήσουμε k-κυκλικούς υπερκορεσμένους σχεδιασμούς ως k κυκλικούς πίνακες κατάλληλους ώστε να σχηματίσουν γεννήτορες πίνακες για QC κώδικες. Το πρώτο βήμα στην προσέγγιση μας είναι να μετασχηματίσουμε το πίνακα σχδιασμού $\mathbf{X}$ ο οποίος έχει στοιχεία $\{-1, 1\}$, και θα συμβολίζεται εφεξής με$\mathbf{X}_{(-1,1)}$, σε ένα υποπίνακα του γεννήτορα πίνακα ενός δυαδικού κώδικα. Από το Θεώρημα 28 ο γεννήτορας ενός k-κυκλικού υπερκορεσμένου σχεδιασμού έχει kt στοιχεία ίσα με -1 και

$(kt - k)$ στοιχεία ίσα με $+1$ και κάθε στήλη του σχεδιασμού έχει τον ίδιο αριθμό από -1 και 1. Συνεπώς, θεωρώντας αυτή τη δομή ως μέρος ενός γεννήτορα πίνακα είναι επιθυμητό να έχουμε όσο το δυνατόν περισσότερα μη-μηδενικά στοιχεία ανά γραμμή. Αν $g = (g_1, g_2, \ldots, g_m)$ είναι ο γεννήτορας ενός k-κυκλικού υπερκορεσμένου σχεδιασμού, τότε μπορούμε να σχηματίσουμε το γεννήτορα $g' = (g'_1, g'_2, \ldots, g'_m)$ θεωρώντας $g'_i = (1 - g_i)/2$, για $i = 1, \ldots, m$. Ο πίνακας σχεδιασμού που σχηματίζεται από τον g' θα συμβολίζεται με $\mathbf{X}_{(1,0)}$.

Το δεύτερο βήμα είναι η αναγνώριση των εμφωλιασμένων (embedded) κυκλικών πινάκων στους k-κυκλικούς υπερκορεσμένους σχεδιασμούς. θεωρώντας τον υπερκορεσμένο σχεδιασμό που δόθηκε στο Παράδειγμα 30 σε $(0, 1)$ μορφή, επιλέγοντας ξεχωριστά τις περιττές και άρτιες στήλες του πίνακα σχεδιασμού $\mathbf{X}_{(1,0)}$ μπορούμε να σχηματίσουμε κυκλικούς πίνακες B_1 και B_2 ως ακολούθως,

$$B_1 = \mathrm{circ}(1,1,0,0,0,1,0,1,0,1,1) \text{ και } B_2 = \mathrm{circ}(0,1,1,0,1,1,0,1,1,0,0).$$

Για έναν δυαδικό QC κώδικα θεωρούμε modulo 2 τα στοιχεία (επίπεδα) του πίνακα σχεδιασμού $\mathbf{X}_{(1,0)}$. Συνεπώς, ένας υπερκορεσμένος σχεδιασμός του οποίου τα στοιχεία θεωρούνται modulo 2, θα καλείται ένας *υπερκορεσμένος σχεδιασμός πάνω από το* $\mathrm{GF}(2)$. Η παράθεση των πινάκων B_1 και B_2 παράγει έναν πίνακα σχεδιασμού $\overline{\mathbf{X}}_{(1,0)}$ ισοδύναμο με τον $\mathbf{X}_{(1,0)}$ (καθώς μεταθέσεις στηλών σε ένα γεννήτορα πίνακα παράγουν ισοδύναμο γεννήτορα πίνακα).

Ένας γεννήτορας πίνακας G ενός QC κώδικα μπορεί να κατασκευαστεί ως $G = [I_{11}\ B_1\ B_2]$ ή $G = [I_{11}\ \overline{\mathbf{X}}_{(1,0)}]$ όπου με I_{11} συμβολίζουμε το μοναδιαίο πίνακα τάξης 11 και ο $\overline{\mathbf{X}}_{(1,0)}$ θεωρείται πάνω από το $\mathrm{GF}(2)$. Για τον σχεδιασμό του Παραδείγματος 30, αυτή η μοντελοποίηση παράγει ένα γεννήτορα πίνακα G ενός QC κώδικα ρυθμού 1/3 ως ακολούθως

$$G = [\ I_{11}\ \mathrm{circ}(1,1,0,0,0,1,0,1,0,1,1)\ \mathrm{circ}(0,1,1,0,1,1,0,1,1,0,0)].$$

Με τον υπολογισμό της ελάχιστης απόστασης του 3-QC κώδικα μήκους 33 και διάστασης 11 στο υπολογιστικό πακέτο, Magma [15], παίρνουμε ότι ο κώδικας έχει ελάχιστη απόσταση d ίση με 11, και επιπλέον ο κώδικας είναι καλός ανάμεσα στους QC κώδικες με ίδιες παραμέτρους [25]. Επιπλέον, ισχύει $GG^T = I_{11}$ και ο πίνακας GG^T είναι μη-ιδιάζων πάνω από το $\mathrm{GF}(2)$ λόγω της Πρότασης 14, συνεπώς ο κώδικας είναι επίσης LCD. Στη συνέχεια, δίνουμε με μαθηματικούς όρους την προηγούμενη μοντελοποίηση επιτυγχάνοντας έτσι μια μέθοδο κατασκευής για πολυκυκλικούς κώδικες.

Θεώρημα 29 *Έστω $\boldsymbol{X}_{(-1,1)}$ ένας k-κυκλικός υπερκορεσμένος σχεδιασμός με n εκτελέσεις (γραμμές) σε $m = k(n-1)$ παράγοντες (στήλες). Τότε, υπάρχει ένας δυαδικός QC κώδικας ρυθμού $1/(k+1)$ με παραμέτρους $[m+(n-1), n-1]$ ή ισοδύναμα $[(k+1)(n-1), n-1]$.*

Απόδειξη. Προφανώς, το block μήκος του κώδικα $(k+1)(n-1)$ είναι πολλαπλάσιο του $k+1$ (όσον αφορά τον $(k+1)$-QC κώδικα). Έστω $g = (g_1, g_2, \ldots, g_m)$ ο γεννήτορας του k-κυκλικού υπερκορεσμένου σχεδιασμού με πίνακα σχεδιασμού $\mathbf{X}_{(-1,1)}$. Θεωρώντας τα $g'_i = (1-g_i)/2$ για $i = 1, \ldots, m$, σχηματίσουμε ένα γεννήτορα $g' = (g'_1, g'_2, \ldots, g'_m)$ για έναν k-κυκλικό υπερκορεσμένο σχεδιασμό με πίνακα σχεδιασμού $\mathbf{X}_{(1,0)}$.

Σχηματίζουμε B_1, B_2,..., B_k $(n-1)\times(n-1)$ κυκλικούς πίνακες επιλέγοντας τα στοιχεία των αντίστοιχων γεννητόρων τους απο τα στοιχεία του g' ως ακολούθως.

$$B_j = \mathrm{circ}\Big(\bigcup_{l=0}^{n-2}\{g'_{kl+j}\}\Big),\ j = 1, \ldots, k \tag{6.5}$$

Έπειτα, θεωρούμε τον υπερκορεσμένο σχεδιασμό πάνω από το GF(2) που δίνεται από τον πίνακα σχεδιασμού $\overline{\mathbf{X}}_{(1,0)} = [B_1\ B_2\ \ldots\ B_k]$, και ο γεννήτορας πίνακας

$$G = [I_{n-1}\ \overline{\mathbf{X}}_{(1,0)}] \tag{6.6}$$

παράγει ένα δυαδικό QC κώδικα ρυθμού $1/(k+1)$, μήκους $(k+1)(n-1)$ και διάστασης $(n-1)$. □

Παρατήρηση 18 *Η επιλογή γεννητόρων για κυκλικούς πίνακες B_j στη σχέση (6.5) διασφαλίζει ότι κάθε πίνακας B_j έχει ακριβώς $n/2$ μη μηδενικά στοιχεία ανά γραμμή. Αυτό κάποιος μπόρει να το δει και από το Θεώρημα 28.*

Η δομή του γεννήτορα πίνακα στη σχέση (6.6) μας επιτρέπει να αντλήσουμε ένα γενικό άνω φράγμα στην ελάχιστη απόσταση των παραγόμενων QC κωδίκων.

Πρόταση 15 *Έστω ένας δυαδικός $[(k+1)(n-1), n-1]$ QC κώδικας κατασκευασμένος όπως στο Θεώρημα 29. Τότε η ελάχιστη απόσταση του d είναι άνω φραγμένη από $\frac{kn}{2}+1$, δηλαδή ισχύει $d \le \frac{kn}{2}+1$.*

Απόδειξη. Κάθε γραμμή του πίνακα σχεδιασμού $\overline{\mathbf{X}}_{(1,0)}$ στη σχέση (6.6) έχει ακριβώς $kt = \frac{kn}{2}$ μη μηδενικά στοιχεία από το Θεώρημα 28. Συνεπώς, κάθε γραμμή του γεννήτορα πίνακα στη σχέση (6.6) έχει ακριβώς

$d_0 = \frac{kn}{2} + 1$ μη μηδενικά στοιχεία και n ελάχιστη απόσταση d είναι φραγμένη από d_0. □

Είναι άξιον αναφοράς να διερευνήσουμε αν ισοδύναμοι υπερκορεσμένοι σχεδιασμοί καταλήγουν σε ισοδύναμους QC κώδικες μέσω του Θεωρήματος 29. Δύο υπερκορεσμένοι σχεδιασμοί θα καλούνται ισοδύναμοι αν μπορούμε να μετασχηματίσουμε τους αντίστοιχους πίνακες σχεδιασμών τον έναν στον άλλον εφαρμόζοντας διαδοχικά μεταθέσεις γραμμών, στηλών και πολλαπλασιασμούς με -1.

Λήμμα 18 *Ισοδύναμοι* k*-κυκλικοί υπερκορεσμένοι σχεδιασμοί παράγουν ισοδύναμους δυαδικούς QC κώδικες μέσω του Θεωρήματος 29.*

Απόδειξη. Ο γεννήτορας πίνακας ενός γραμμικού κώδικα είναι αναλλοίωτος ως προς μετασχηματισμούς γραμμών και στηλών. Οι πολλαπλασιασμοί με -1 στον k-κυκλικό υπερκορεσμένο σχεδιασμό είναι ισοδύναμοι με τους πολλαπλασιασμούς με 1 στο γεννήτορα πίνακα του Θεωρήματος 29 πάνω από το $\mathsf{GF}(2)$ και συνεπώς καταλήγουμε σε ισοδύναμο κώδικα. □

§6.3.1 Σύνδεση $\mathsf{E}(s^2)$-Βέλτιστων Υπερκορεσμένων Σχεδιασμών και LCD QC Κωδίκων

Σε αυτήν την ενότητα, θα εδραιώσουμε μια σύνδεση μεταξύ μιας ειδικής κλάσης βέλτιστων υπερκορεσμένων σχεδιασμών και LCD QC κωδίκων. Η εφαρμογή αυτή είναι ένα ακόμη παράδειγμα αλληλεπίδρασης μεταξύ κλάδων των μαθηματικών, της Θεωρίας κωδίκων και των πειραματικών σχεδιασμών.

Θεωρούμε έναν υπερκορεσμένο σχεδιασμό με πίνακα σχεδιασμού έναν $n \times m$ πίνακα $\mathbf{X}_{(-1,1)}$. Η ορθογωνιότητα μεταξύ όλων των ζευγών των στηλών του πίνακα του μοντέλου, που σχηματίζεται από τον πίνακα σχεδιασμού επισυνάπτοντας μια στήλη από μονάδες ως πρώτη στήλη, απαιτείται έτσι ώστε να εκτιμήσουμε όλες τις αλληλεπιδράσεις παραγόντων. Αυτή η συνθήκη δεν είναι δυνατόν να ικανοποιηθεί για

όλα τα ζεύγη στηλών σε έναν υπερκορεσμένο σχεδιασμό καθώς $m \geq n$. Συνεπώς, ένας πειραματιστής ενδιαφέρεται να βρει σχεδιασμούς που είναι όσο το δυνατόν σχεδόν ορθογώνιοι. Στη συνέχεια, αναφέρουμε το πιο κοινό κριτήριο βελτιστοποίησης για υπερκορεσμένους σχεδιασμούς.

$E(s^2)$–Κριτήριο Έστω s_{ij} ένα στοιχείο της i γραμμής και j στήλης του πίνακα $\mathbf{X}_{(-1,1)}^{T}\mathbf{X}_{(-1,1)}$. Οι Booth και Cox ([14]) πρότειναν ως κριτήριο σύγκρισης σχεδιασμών την ελαχιστοποίση του μέσου των s_{ij}^2, το οποίο και συμβολίζεται με $ave(s^2)$ ή $E(s^2)$, όπου

$$E(s^2) = \sum_{1\leq i<j\leq m} s_{ij}^2 / \left(\begin{array}{c} m \\ 2 \end{array} \right). \qquad (6.7)$$

Ο όρος s_{ij} μετρά τον βαθμό μη-ορθογωνιότητας μεταξύ των παραγόντων i και j. Αν $s_{ij} = 0$, οι παράγοντες i και j είναι ορθογώνιοι. Αν το n είναι άρτιος αλλά όχι ένα πολλαπλάσιο του 4 (δηλαδή $n \equiv 2 \pmod 4$) τότε το s_{ij} δεν μπορεί να ισούται με 0. Σε αυτές τις περιπτώσεις, οι παράγοντες i και j καλούνται σχεδόν ορθογώνιοι αν το s_{ij} είναι κοντά στο 0. Όταν $s_{ij} = \pm n$ τότε $c_i = \pm c_j$ και τα c_i και c_j είναι πλήρως εξαρτημένα. Σχεδιασμοί με πλήρως εξαρτημένους παράγοντες συνήθως απορρίπτονται.

Ειναι γνωστό (Nguyen, [188], Nguyen και Cheng, [189]) ότι το άθροισμα των τετραγώνων των στοιχείων των πινάκων $\mathbf{X}_{(-1,1)}\mathbf{X}_{(-1,1)}^{T}$ και $\mathbf{X}_{(-1,1)}^{T}\mathbf{X}_{(-1,1)}$ είναι ελάχιστο αν και μόνον αν ο πίνακας $\mathbf{X}_{(-1,1)}\mathbf{X}_{(-1,1)}^{T}$ γράφεται στη μορφή $(m-x)\mathbf{I}_n + x\mathbf{J}_n$, όπου $x = -m/(n-1)$ για άρτιο n και $-m/n$ για περιττό n, όπου $\mathbf{I}_n$ είναι ο $n \times n$ μοναδιαίος πίνακας και $\mathbf{J}_n$ είναι ο $n \times n$ πίνακας με όλα του τα στοιχεία ίσα με 1.

Σε αυτή την περίπτωση, οι Nguyen [188], Tang και Wu [223] ανεξάρτητα απέδειξαν ένα κάτω φράγμα για το $E(s^2)$-κριτήριο, και σχεδιασμοί οι οποίοι επιτυγχάνουν αυτό το κάτω φράγμα θα καλούνται $E(s^2)$-βέλτιστοι. Ιδιαίτερα, στην περίπτωση των k-κυκλικών υπερκορεσμένων σχεδιασμών αυτό το κάτω φράγμα επιτυγχάνεται όταν $nk \equiv 0 \pmod 4$ ή $n \equiv 2 \pmod 4$ και το k είναι περιττός [173].

Με όρους Θεωρίας κωδικών, ενδιαφερόμαστε για τη μορφή του $(n-1) \times (n-1)$ πίνακα $D = \mathbf{X}_{(1,0)}\mathbf{X}_{(1,0)}^{T}$, όπου θεωρούμε τον πίνακα $\mathbf{X}_{(1,0)}$ όπως ορίστηκε στην προηγούμενη ενότητα. Το $E(s^2)$-κριτήριο ως μέτρο βελτιστοποίησης είναι ανεξάρτητο από την κωδικοποίηση των επιπέδων των υπερκορεσμένων σχεδιασμών και υπενθυμίζουμε ότι από την Ενότητα 6.2.1 ο D είναι ένας κυκλικός συμμετρικός πίνακας. Επιπλέον, τα διαγώνια στοιχεία του D προκύπτουν από το εσωτερικό γινόμενο των γραμμών του $\mathbf{X}_{(1,0)}$ και είναι ίσα με $kt = kn/2$ καθώς κάθε γραμμή

του $\mathbf{X}_{(1,0)}$ έχει βάρος $kn/2$ από το Θεώρημα 28. Στην περίπτωση των k-κυκλικών υπερκορεσμένων σχεδιασμών, έχουμε την ακόλουθη περιγραφή του D όταν ο πίνακας σχεδιασμού βρίσκεται σε $(0,1)$ μορφή.

Πρόταση 16 *Έστω ένας* k*-κυκλικός υπερκορεσμένος σχεδιασμός με* $(n-1)$ *γραμμές και* $k(n-1)$ *στήλες, με πίνακα σχεδιασμού* $\boldsymbol{X}_{(1,0)}$*. Τότε, είναι* $E(s^2)$*-βέλτιστον αν* $D = \boldsymbol{X}_{(1,0)}\boldsymbol{X}_{(1,0)}^{\mathsf{T}} = \frac{kn}{4}\boldsymbol{I}_{n-1} + \frac{kn}{4}\boldsymbol{J}_{n-1}$*.*

Απόδειξη. Για να επιτυγχάνει το άθροισμα των τετραγώνων του πίνακα D το ελάχιστο, και συνεπώς ο σχεδιασμός θα είναι $E(s^2)$-βέλτιστος στη $(0,1)$ μορφή του, θα πρέπει τα μη-διαγώνια στοιχεία του να είναι ίσα. Αυτό επιτυγχάνεται όταν η απόσταση hamming κάθε δύο διαφορετικών γραμμών του $\mathbf{X}_{(1,0)}$ είναι σταθερή και ίση με $\frac{kn}{2}$. Επομένως, ο αριθμός των εμφανίσεων μεταξύ κάθε ζεύγους δύο διαφορετικών γραμμών είναι ίσος με $\frac{kn}{2} - k$. Αυτο μπορεί μόνο να επιτευχθεί, όταν οι δυάδες $(0,0)$ και $(1,1)$ εμφανίζονται ως διανύσματα στήλη σε κάθε ζεύγος δύο διαφορετικών γραμμών. Από το Θεώρημα 28, ο αριθμός των δυάδων $(1,1)$ είναι ίσος με $\frac{kn}{4}$ και συνεισφέρει στο εσωτερικό γινόμενο δύο διαφορετικών γραμμών. Συνεπώς, όλα τα μη-διαγώνια στοιχεία είναι ίσα με $\frac{kn}{4}$ και ο D είναι ένας πίνακας της μορφής:

$$D = \mathbf{X}_{(1,0)}\mathbf{X}_{(1,0)}^{\mathsf{T}} = \begin{bmatrix} \frac{kn}{2} & \frac{kn}{4} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \frac{kn}{4} & \frac{kn}{2} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \frac{kn}{4} & \frac{kn}{4} & \frac{kn}{2} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \frac{kn}{4} & \frac{kn}{4} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{2} \end{bmatrix} = \frac{kn}{4}\mathbf{I}_{n-1} + \frac{kn}{4}\mathbf{J}_{n-1}. \quad (6.8)$$

□

Παρατήρηση 19 *Προφανώς, μια απαραίτητη συνθήκη έτσι ώστε ένας* k*-κυκλικός υπερκορεσμένος σχεδιασμός με* $(n-1)$ *γραμμές,* $k(n-1)$ *στήλες και πίνακα σχεδιασμού* $\boldsymbol{X}_{(1,0)}$ *να είναι* $E(s^2)$*-βέλτιστος είναι ότι το* kn *πρέπει να διαιρείται από το* 4*, δηλαδή* $kn \equiv 0 \pmod 4$*.*

Θεωρώντας στη συνέχεια τον υπερκορεσμένο σχεδιασμό πάνω από το GF(2), θεωρούμε GF(2) αριθμητική για τα στοιχεία του D. Θυμίζουμε ότι, από τη σχέση (6.6) ένας γεννήτορας πίνακας για έναν QC κώδικα δίνεται στη μορφή $G = [I_{n-1}\ \overline{\mathbf{X}}_{(1,0)}]$. Σημειώνουμε ότι, ο $\overline{\mathbf{X}}_{(1,0)}\overline{\mathbf{X}}_{(1,0)}^{\mathsf{T}}$ θα έχει την ίδια μορφή με τον D, καθώς μια μετάθεση των στοιχείων του γεννήτορα του $\mathbf{X}_{(1,0)}$ δεν αλλάζει τις τιμές του εσωτερικού γινομένου των

γραμμών. Πλέον είμαστε σε θέση να αναγνωρίσουμε ακριβώς εκείνες τις κλάσεις των υπερκορεσμένων σχεδιασμών που παράγουν LCD QC κώδικες μέσω του Θεωρήματος 29.

Θεώρημα 30 *Έστω ένας* $\mathsf{E}(s^2)$ *βέλτιστος* k*-κυκλικός υπερκορεσμένος σχεδιασμός με* n *εκτελέσεις (γραμμές) σε* $k(n-1)$ *παράγοντες (στήλες), με πίνακα σχεδιασμού* $\boldsymbol{X}_{(-1,1)}$*. Τότε ο δυαδικός* $[(k+1)(n-1), n-1]$ *QC κώδικας που παράγεται από το Θεώρημα 29 είναι LCD σε καθεμία από τις ακόλουθες περιπτώσεις:*

(i) $n \equiv 0 \pmod 4$ *και το* k *είναι άρτιος.*

(ii) $n \equiv 0 \pmod 8$ *και το* k *είναι περιττός.*

(iii) $n \equiv 2 \pmod 4$ *και* $k \equiv 0 \pmod 4$.

Απόδειξη. Θεωρούμε τον υπερκορεσμένο σχεδιασμό πάνω από το $\mathsf{GF}(2)$ μετά την εφαρμογή του Θεωρήματος 29. Διακρίνουμε τις ακόλουθες περιπτώσεις για $GG^T = I_{n-1} + D$, όπου $D = \overline{\mathbf{X}}_{(1,0)}\overline{\mathbf{X}}_{(1,0)}^T$.

- Όταν $n \equiv 0 \pmod 4$ έχουμε τις ακόλουθες περιπτώσεις:

  (i) Αν $k \equiv 0 \pmod 2$, τότε $\frac{kn}{2} = \frac{kn}{4} \equiv 0 \pmod 2$ και ο D είναι ο μηδενικός πίνακας τάξης $n-1$. Επομένως, $GG^T = I_{n-1}$ και ο πίνακας GG^T είναι μη-ιδιάζων. Άρα από την Πρόταση 14, ο παραγόμενος κώδικας είναι LCD.

  (ii) Αν $k \equiv 1 \pmod 2$ και επιπρόσθετα $n \equiv 0 \pmod 8$ τότε $\frac{kn}{2} = \frac{kn}{4} \equiv 0 \pmod 2$ και ο D είναι ο μηδενικός πίνακας τάξης $n-1$. Επομένως, $GG^T = I_{n-1}$ και ο πίνακας GG^T είναι μη-ιδιάζων. Άρα από την Πρόταση 14, ο παραγόμενος κώδικας είναι LCD.

  (iii) Αν $k \equiv 1 \pmod 2$ και επιπρόσθετα $n \equiv 4 \pmod 8$ τότε $\frac{kn}{2} \equiv 0 \pmod 2$ και $\frac{kn}{4} \equiv 1 \pmod 2$. Επομένως, $GG^T = J_{n-1}$ και ο πίνακας GG^T είναι ιδιάζων. Άρα από την Πρόταση 14, ο παραγόμενος κώδικας δεν είναι LCD.

- Όταν $n \equiv 2 \pmod 4$ οι ακόλουθες περιπτώσεις είναι επιτρεπτές λόγω της Παρατήρησης 19:

  (i) Αν $k \equiv 0 \pmod 4$, τότε $\frac{kn}{2} = \frac{kn}{4} \equiv 0 \pmod 2$ και ο D είναι ο μηδενικός πίνακας τάξης $n-1$. Επομένως, $GG^T = I_{n-1}$ και ο πίνακας GG^T είναι μη-ιδιάζων. Άρα από την Πρόταση 14, ο παραγόμενος κώδικας είναι LCD.

(ii) Αν $k \equiv 2 \pmod 4$ τότε $\frac{kn}{2} \equiv 0 \pmod 2$ και $\frac{kn}{4} \equiv 1 \pmod 2$. Επομένως, $GG^T = J_{n-1}$ και ο πίνακας GG^T είναι ιδιάζων. Άρα από την Πρόταση 14, ο παραγόμενος κώδικας δεν είναι LCD.

□

Μέχρι σήμερα, ελάχιστοι LCD QC κώδικες είναι γνωστοί, [46]. Η σύνδεση μεταξύ των $E(s^2)$-βέλτιστων υπερκορεσμένων σχεδιασμών και των LCD QC κωδίκων μας επιτρέπει να χρησιμοποιήσουμε γνωστούς υπερκορεσμένους σχεδιασμούς από τις [173] και [149], για τους οποίους ισχύουν οι συνθήκες του προηγούμενου θεωρήματος, έτσι ώστε να παράγουμε νέους QC κώδικες στην κλάση των LCD QC κωδίκων. Ιδιαίτερα, έχουμε το ακόλουθο πόρισμα.

Πόρισμα 24 *Υπάρχουν LCD QC κώδικες με παραμέτρους,*

(i) $[21, 7], [33, 11], [45, 15], [57, 19]$ *ρυθμού* $1/3$.

(ii) $[28, 7], [60, 15]$ *ρυθμού* $1/4$.

(iii) $[35, 7], [45, 9], [55, 11], [65, 13], [75, 15]$ *ρυθμού* $1/5$.

(iv) $[42, 7], [90, 15]$ *ρυθμού* $1/6$.

(v) $[77, 11]$ *ρυθμού* $1/7$.

(vi) $[99, 11]$ *ρυθμού* $1/9$.

Απόδειξη. Υπάρχουν $E(s^2)$-βέλτιστοι k-κυκλικοί υπερκορεσμένοι σχεδιασμοί με n εκτελέσεις σε $m = k(n-1)$ παράγοντες για $(n, m) \in M$ όπου $M = \{(8, 14), (8, 21), (8, 28), (8, 35), (10, 36), (12, 22), (12, 44), (12, 66), (12, 88), (14, 52), (16, 30), (16, 45), (16, 60), (16, 75), (20, 38)\}$ από τις [173] και [149]. Οι παράμετροι των παραγόμενων LCD QC κωδίκων απορρέουν από το Θεώρημα 30. □

§6.4 Γενετικοί Αλγόριθμοι για Πολυκυκλικούς Κώδικες

Η εύρεση ενός $[n, k]$ γραμμικού κώδικα με μεγάλη ελάχιστη απόσταση d απαιτεί έναν σχεδόν εξαντλητικό έλεγχο (exhaustive search), ο οποίος είναι απρόσιτος (υπολογιστικά) για όλες τις διαστασείς ενός κώδικα (εκτός από τις πιο μικρές και ορισμένων περιορισμένων κλάσεων κωδίκων) καθώς ο υπολογισμός της ελάχιστης απόστασης d ενός δυαδικού γραμμικού κώδικα είναι NP-hard πρόβλημα, και το αντίστοιχο πρόβλημα απόφασης είναι NP-complete ([230]). Στην πραγματικότητα, αυτό το πρόβλημα έγγειται στην κλάση των NP-hard προβλημάτων συνδυαστικής βελτιστοποίησης.

Το πεδίο της συνδυαστικής βελτιστοποίησης παρέχει μια πληθώρα ευρετικών αλγορίθμων (heuristic algorithms), πολλοί από τους οποίους προσεγγίζουν την απόδοση βέλτιστων μεθόδων. Αρκετά γνωστοί αλγόριθμοι που ανήκουν σε αυτή την κλάση αλγορίθμων είναι η προσομοιωμένη ανόπτηση (Simulated Annealing), η μέθοδος Tabu (Tabu Search) και οι γενετικοί αλγόριθμοι (Genetic Algorithms). Διάφοροι ερευνητές έχουν επικεντρωθεί στην κατασκευή καλών QC κωδίκων εφαρμόζοντας ευρετικές μεθόδους, δες για παράδειγμα [24, 107]. Εν προκειμένω, εμείς υλοποιήσαμε ένα γενετικό local search αλγόριθμο.

§6.4.1 Μοντελοποίηση του Γενετικού Αλγορίθμου

Οι γενετικοί αλγόριθμοι αποτελούν μια ισχυρή μεταευρετική (metaheuristic) μέθοδο, η οποία μιμείται διαδικάσιες από την Θεωρία της Εξέλιξης έτσι ώστε να εδραιώσει αλγόριθμους αναζήτησης ορίζοντας τις αλγοριθμικές έννοιες που αντιστοιχούν σε θέματα της Βιολογίας όπως είναι η αναπαραγωγή (reproduction), η διασταύρωση (crossover) και η μετάλλαξη (mutation). Οι γενετικοί αλγόριθμοι εισήχθησαν το 1970 από τον John Holland [111] με σκοπό το σχεδιασμό ενός συστήματος τεχνητής νοημοσύνης που θα είχε ιδιότητες παρόμοιες με εκείνες των φυσικών συστημάτων. Σε αυτή την ενότητα, υποθέτουμε κάποια βασική εξοικείωση με θέματα γενετικών αλγορίθμων. Μια καλή εισαγωγή σε θέματα που αφορούν τον απλό γενετικό αλγόριθμο (εν συντομία SGA) μπορεί να βρεθεί στο σύγγραμμα του Goldberg [74], στο άρθρο της Stefanie Forrest [51] και στο Εγχειρίδιο των γενετικών αλγορίθμων (Handbook of Genetic Algorithms) που έχει επεξεργασθεί ο Davis [40].

Με την επιβολή μιας δομής για τους κωδικούς που αναζητάμε, έ-

χουμε ένα χώρο αναζήτησης που είναι μικρότερος σε σύγκριση με το αρχικό, γενικό πρόβλημα. Όσο ισχυρότερη είναι η δομή, τόσο μικρότερος είναι ο χώρος αναζήτησης. Υπάρχει μια ανταλλαγή εδώ, αφού θα μπορούσαμε να χάσουμε καλούς κωδικούς αν επιβάλουμε πάρα πολύ τη δομή. Ωστόσο, συναντάται συχνά η περίπτωση οι καλοί κώδικες να έχουν αρκετή δομη. Αυτό το γεγονός, εξηγεί εν μέρει γιατί η προσέγγιση μας που παρουσιάζεται σε αυτήν την ενότητα λειτουργεί ιδιαίτερα αποδοτικα.

Αναπαράσταση Χρωμοσωμάτων Μια αναπαράσταση για τα χρωμοσώματα (chromosomes) στο γενετικό αλγόριθμο προκύπτει με φυσικό τρόπο από τη συστηματική μορφή του γεννήτορα πίνακα της σχέσης (6.3). Εφόσον μπορούμε να αναπαραστήσουμε ένα κυκλικό πίνακα με την πρώτη του γραμμή, μια δυαδική συμβολοσειρά θα περιέχει την πρώτη γραμμή του G και θα αντιστοιχεί στο γεννήτορα πίνακα του QC κώδικα. Είναι προφανές ότι το μήκος του χρωμοσώματος θα είναι ίσο με το μήκος pm του QC κώδικα. Αυτή η μέθοδος κωδικοποίησης ενισχύει την συμπάγεια του GA, καθώς χρειάζεται ένα μικρό μέγεθος αποθηκευτικού χώρου στην μνήμη ενός υπολογιστή έτσι ώστε να καταστεί δυνατή η αναπαράσταση ενός συστηματικού QC κώδικα ρυθμού $1/p$ από τον SGA. Ιδιαίτερα, για έναν $[pm, m]$ QC κώδικα που έχει έναν $m \times pm$ γεννήτορα πίνακα χρειάζεται να δεσμευτούν pm bits στη μνήμη. Αντίθετα, αν έπρεπε να αναπαραστήσουμε όλο το γεννήτορα πίνακα θα έπρεπε να δεσμεύσουμε pm^2 bits. Επομένως, η χωρική πολυπλοκότητα μειώνεται από $\mathcal{O}(t^3)$ σε $\mathcal{O}(t^2)$ για $t = \max\{p, m\}$ (αν και στις περισσότερες περιπτώσεις που θεωρήσαμε ισχύει $p < m$).

Αρχικός Πληθυσμός θεωρήσαμε χρήσιμο να παράγουμε αυτά τα χρωμοσώματα ανακτώντας τυχαία δείγματα k-κυκλικών υπερκορεσμένων σχεδιασμών. Στο Θεώρημα 29, δυαδικοί QC κώδικες ρυθμού $1/(k+1)$ με παραμέτρους $[(k+1)(n-1), n-1]$ κατασκευάζονται από k-κυκλικούς υπερκορεσμένους σχεδιασμούς με n γραμμές και $k(n-1)$ στήλες. Ένα δείγμα χρωμοσώματος από την προηγούμενη κατασκευή κατάλληλο για την κωδικοποίηση του GA θα ήταν η παράθεση των ακολούθων δυαδικών συμβολοσειρών $100000000000000; 110010001111010; 110101111000100$, όπου η πρώτη συμβολοσειρά αντιστοιχεί στο μοναδιαίο πίνακα τάξης 15. Αυτό το χρωμόσωμα παράγει έναν δυαδικό QC κώδικα ρυθμού $1/3$ με παραμέτρους $[45, 15]$.

Αντικειμενικές Συναρτήσεις για Συστηματικούς QC Κώδικες Γενικά, ο δυϊκός ενός καλού κώδικα με ρυθμό $1/p$ δεν είναι ένας καλός κώδικας ρυθμού $(p-1)/p$ (παρόλο που αυτό αληθεύει σε ορισμένες περιπτώσεις) [90]. Λαμβάνοντας υπόψιν, αυτό το γεγονός θεωρήσαμε ως αντικειμενική συνάρτηση (objective function), εν συντομία OF, την ακόλουθη σχέση που πρόκειται να μεγιστοποιηθεί από τον GA

$$OF_1 = \frac{d_C + (p-1)\cdot d_{C^\perp}}{p} \tag{6.9}$$

όπου με d_C συμβολίζουμε την ελάχιστη απόσταση του QC κώδικα, C, και με $d_{C^\perp}$ αντίστοιχα συμβολίζουμε την ελάχιστη απόσταση του δυϊκού του κώδικα. Θεωρούμε ότι έχουμε βρεί μια βέλτιστη λύση μέσω τουGA, όταν ανιχνεύσουμε έναν QC κώδικα του οποίου η d_C επιτυγχάνει τα τωρινά κάτω φράγματα στην ελάχιστη απόσταση των γραμμικών κωδίκων.

Κάποιος μπορεί να παρατηρήσει ότι δίνοντας τόση βαρύτητα στην ελάχιστη απόσταση του δυϊκού κώδικα, αυτό μπορεί να περιορίσει σημαντικά τον χώρο αναζήτησης όταν ψάχνουμε καλούς κώδικες. Επομένως, χρησιμοποιήσαμε μια δεύτερη αντικειμενική συνάρτηση $OF_2 = d_C$ όπου σε αυτή τη περίπτωση χρησιμοποιήσαμε έναν ιδιαίτερα αποδοτικό αλγόριθμο για να υπολογίσουμε την ελάχιστη απόσταση του κώδικα όπως αυτός περιγράφεται στην [86]. Είχαμε ως κίνητρο να χρησιμοποιήσουμε αυτή τη μοντελοποίηση για τον υπολογισμό της OF_2 καθώς από τον αλγόριθμο που δίνεται στην [86] μπορούμε να αντλήσουμε κάτω και πάνω φράγματα για την d_C. Συνεπώς, συγκρίνοντας αυτά τα φράγματα κατά τη διάρκεια εκτέλεσης του αλγορίθμου με τα τωρινά κάτω φράγματα στην ελάχιστη απόσταση των καλύτερων γραμμικών κωδίκων, μπορούμε εύκολα να αποφανθούμε αν μια λύση βελτιώνεται κατά τον κύκλο επαναλήψεων του GA.

Στην ενότητα 6.4.3, οι QC κώδικες ρυθμού 1/4, 1/5, 1/6 και 1/3, 1/7 βρέθηκαν με τη χρήση των OF_1 και OF_2, αντίστοιχα.

§6.4.2 Υλοποίηση του Γενετικού Αλγορίθμου

Πλέον, είμαστε σε θέση να περιγράψουμε τους τρεις γενετικούς τελεστές (genetic operators) της αναπαραγωγής, διασταύρωσης και μετάλλαξης όπως ακριβώς τους εφαρμόσαμε με τη χρήση του απλού γενετικού αλγορίθμου.

Αναπαραγωγή ορίζει ότι στα χρωμοσώματα του πληθυσμού με υψηλές τιμές στην OF (στην περίπτωση που θέλουμε να μεγιστοποιήσουμε την OF), πρέπει να τους ανατεθούν υψηλές πιθανότητες συνεισφοράς απογόνων στην επόμενη γενιά. Η πιθανότητα κάθε συμβολοσειράς να εισέλθει στο χώρο ζευγαρώματος (mating pool) είναι ανάλογη της τιμής της αντικειμενικής της συνάρτησης. Αυτός ο γενετικός τελεστής είναι η αλγοριθμική αντιστοιχία της φυσικής επιλογής της Θεωρίας της Εξέλιξης. Αν και πάντα χρωμοσώματα με υψηλές τιμές στην αντικειμενική συνάρτηση θα επιλεχθούν να εισέλθουν στο χώρο ζευγαρώματος σε κάθε γενιά, αυτό δεν διασφαλίζει ότι αυτά τα χρωμοσώματα θα είναι καλύτερα από εκείνα τα οποία πρόκειται να αντικατασταθούν. Ο τελεστής αναπαραγωγής που υλοποιήσαμε στον υπολογιστή, και συμπεριφέρεται ως μιας μεροληπτική ρουλέτα (biased roulette), βασίστηκε στην ομοιόμορφη κατανομή και τελικώς καθορίσαμε το ποσοστό των χρωμοσωμάτων που πρόκειται να αντικατασταθούν. Σύμφωνα με τις τιμές των αντικειμενικών τους συναρτήσεων, τα καλύτερα χρωμοσώματα επιλέγονται και οι γενετικοί τελεστές εφαρμόζονται σε αυτά. Το αποτέλεσμα του τελεστή της αναπαραγωγής είναι ένας χώρος ζευγαρώματος, που περιέχει τα χρωμοσώματα της νέας γενιάς. Σημειώνουμε ότι, δεν αντιστοιχούν όλα τα χρωμοσώματα που παρήχθησαν μέσω του GA σε LCD QC κώδικες, επιτρέποντας με αυτό τον τρόπο την αναζήτηση QC κωδίκων που δεν είναι απαραίτητα συμπληρωματικά δυϊκοί.

Διασταύρωση επιδρά στα χρωμοσώματα του χώρου ζευγαρώματος (της νέας γενιάς) σε δύο βήματα. Αρχικά, αυτά τα χρωμοσώματα επιλέγονται τυχαία και σχηματίζουν ζεύγη (pairs). Στη συνέχεια, το κάθε ζεύγος διασταυρώνεται επιλέγοντας ένα σημείο διασταύρωσης k τυχαία. Αυτό σημαίνει ότι τα στοιχεία πριν και μετά αυτού του σημείου διασταύρωσης k ανταλλάσονται αμοιβαία. Εφαρμόσαμε επίσης αλλή μια εκδοχή αυτου του γενετικού τελεστή. Για παράδειγμα μπορούμε να έχουμε δύο σημεία διασταύρωσης. Διασταύρωση δύο σημείων σημαίνει ότι θα επιλεχθούν αρχικά δύο τέτοια σημεία στις αρχικές συμβολοσειρές. Περισσότερες λεπτομέρειες για αυτούς τους γενετικούς τελεστές μπορούν να βρεθούν στο Εγχειρίδιο του Davis [40]. Η επιλογή του σημείου διασταύρωσης k περιορίστηκε με τέτοιο τρόπο έτσι ώστε να μην είναι δυνατό να επιλεχθεί ως ένα σημείο πολλαπλάσιο της τάξης m των κυκλικών πινάκων που αποτελούν το γεννήτορα πίνακα του QC κώδικα, καθώς τότε θα παράγαμε ισοδύναμους QC κώδικες. Αυτό είναι το γνωστό φαινόμενο παραγωγής διδύμων χρωμοσωμάτων (twin chromosomes) σε ένα GA ([40]). Επιπρόσθετα, θα μπορούσαμε να έχουμε πολλαπλά σημεία δια-

σταύρωσης όποτε σε αυτή την περίπτωση το πρόβλημα της επιλογής αυτών των σημείων είναι ισοδύναμο με την κατάλληλη επιλογή πινάκων πλήρους βαθμού, B_i.

Μετάλλαξη αλλάζει τυχαία ένα bit από 0 σε 1 ή από 1 σε 0, σύμφωνα με μια προκαθορισμένη πιθανότητα που αντλείται από την ομοιόμορφη κατανομή. Αυτή η πιθανότητα μετάλλαξης είναι συνήθως σχετικά μικρή.

§6.4.3 Καλοί Δυαδικοί Πολυκυκλικοί Κώδικες Ρυθμού $1/p$

Σε αυτήν την ενότητα, ένας βέλτιστος κώδικας ορίζεται ως εκείνος που επιτυγχάνει την μέγιστη δυνατή ελάχιστη απόσταση για δοθείσα κλάση γραμμικών κωδίκων. Ένας καλός κώδικας ορίζεται ως εκείνος που έχει την μέγιστη γνωστή ελάχιστη απόσταση για δεδομένα n και k, δηλαδή επιτυγχάνει το γνωστό κατώ φράγμα στην ελάχιστη απόσταση ενός γραμμικού κώδικα.

Παρουσιάζονται τα διανύσματα γραμμών των κυκλικών πινάκων B_i, $i = 2, \ldots, p$ για συστηματικούς δυαδικούς QC κώδικες ρυθμού $1/p$ που βρέθηκαν εφαρμόζοντας τον GA. Για καθένα από τους κώδικες που δίνονται στη συνέχεια συγκρίνουμε την ελάχιστη απόσταση που υπολογίσαμε με τα τωρινά καλυτερα κάτω φράγματα στης ελάχιστη απόσταση (d_{Lb}) των καλύτερων γνωστών QC και γραμμικών κωδίκων όπως αυτά έχουν ανακτηθεί από τους Πίνακες του Chen [25] και του Grassl [85], αντίστοιχα. Για κάθε βέλτιστο ή καλό κώδικα που βρήκαμε, εκτελούμε επιπλέον έναν επιπλέον έλεγχο ισοδυναμίας με γνωστούς κώδικες και αποφαινόμαστε ότι όλοι οι κώδικες που δίνονται σε αυτήν την ενότητα είναι μη-ισοδύναμοι όταν συγκρίνονται με τους αντίστοιχους QC ή γραμμικούς κώδικες ίδιων παραμέτρων, εκτός από την περίπτωση των $[25, 5, 12]$ και $[30, 5, 15]$ κωδίκων. Επιπλέον, πολλοί από τους κώδικες που παρατίθενται είναι κοντά στα άνω φράγματα, τα οποία συμβολίζονται με d_{Ub}, και έτσι αναμένεται ότι ορισμένοι από αυτούς τους κώδικες θα είναι βέλτιστοι όταν αυτά τα πάνω φράγματα βελτιωθούν.

Όπως και στην περίπτωση των αυτοδυϊκών κωδίκων χρησιμοποιήσαμε το Magma [15, 83], για να υπολογίσουμε την ελάχιστη απόσταση d_{QC} όλων των QC κωδίκων που δίνονται παρακάτω. Προηγούμενα αποτελέσματα σε QC κώδικες μπορούν να βρεθούν στις [107, 24, 90, 91].

Δυαδικοί QC Κώδικες Ρυθμού 1/3

- Ένας βέλτιστος $[21, 7, 8]$ κώδικας:

```
[ 1, 0, 1, 0, 1, 1, 0 ]
[ 1, 0, 1, 1, 0, 0, 0 ]
```

- Ένας βέλτιστος $[27, 9, 10]$ κώδικας:

```
[ 0, 0, 1, 1, 0, 0, 1, 0, 0 ]
[ 0, 1, 1, 0, 1, 1, 1, 0, 1 ]
```

- Ένας $[33, 11, 11]$ LCD κώδικας (καλός ανάμεσα στους QC κώδικες):

```
[ 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0 ]
[ 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1 ]
```

- Ένας καλός $[39, 13, 12]$ LCD κώδικας:

```
[ 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0 ]
[ 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 ]
```

- Ένας καλός $[45, 15, 14]$ κώδικας:

```
[ 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0 ]
[ 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0 ]
```

- Ένας $[51, 17, 15]$ κώδικας:

```
[ 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1 ]
[ 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1 ]
```

- Ένας καλός $[57, 19, 16]$ LCD κώδικας:

```
[ 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1 ]
[ 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0 ]
```

- Ένας $[63, 21, 17]$ LCD κώδικας:

```
[ 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0 ]
[ 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0 ]
```

Από τις συγκρίσεις που γίνονται παρακάτω, συμπεραίνουμε ότι οι $[21, 7, 8]$ και $[27, 9, 10]$ κώδικες είναι βέλτιστοι ανάμεσα στους γραμμικούς κώδικες με τις ίδιες παραμέτρους. Επιπλέον, οι $[33, 11, 11]$, $[39, 13, 12]$, $[45, 15, 14]$ και $[57, 19, 16]$ κώδικες επιτυγχάνουν το τωρινό κάτω φράγμα στην ελάχιστη απόσταση των QC κωδίκων ([25]). Επίσης, οι $[33, 11, 11]$, $[39, 13, 12]$, $[57, 19, 16]$ και $[63, 21, 17]$ κώδικες είναι νέοι στη κλάση των δυαδικών QC LCD κωδίκων, [46]. Επιπρόσθετα, επιμηκύνοντας τους $[33, 11, 11]$, $[51, 17, 15]$ και $[63, 21, 17]$ κώδικες προσθέτοντας μια στήλη στο γεννήτορα πίνακα ([84]), παράγουμε $[34, 11, 12]$, $[52, 17, 16]$ και $[63, 21, 18]$ κώδικες που είναι καλοί ανάμεσα στην κλάση των γραμμικών κωδίκων, [85].

Κώδικας	d_{QC}	$[d_{Lb}, d_{Ub}]$	Αναφορά
$[21, 7]$	8	8	[225, 91]
$[27, 9]$	10	10	[91]
$[33, 11]$	11	12	[9, 85]
$[39, 13]$	12	12-13	[9, 90]
$[45, 15]$	14	14-15	[90]
$[51, 17]$	15	16-17	[9]
$[57, 19]$	16	16-19	[9]
$[63, 21]$	17	18-20	[107]

Πίνακας 6.1: Ελάχιστες αποστάσεις δυαδικών QC κωδίκων ρυθμού 1/3

Δυαδικοί QC Κώδικες Ρυθμού 1/4

- Ένας βέλτιστος $[20, 5, 9]$ LCD κώδικας:

```
[ 1, 0, 1, 0, 0 ]
[ 1, 1, 0, 0, 1 ]
[ 0, 1, 1, 0, 1 ]
```

- Ένας βέλτιστος $[28, 7, 12]$ κώδικας:

```
[ 0, 1, 1, 1, 0, 0, 0 ]
[ 0, 1, 1, 0, 1, 0, 0 ]
[ 0, 1, 0, 1, 1, 1, 1 ]
```

- Ένας βέλτιστος $[36, 9, 14]$ κώδικας:

```
[ 0, 0, 0, 0, 1, 1, 0, 0, 1 ]
[ 0, 1, 0, 0, 1, 0, 1, 0, 1 ]
[ 1, 1, 1, 0, 1, 0, 1, 1, 0 ]
```

- Ένας καλός $[44, 11, 16]$ LCD κώδικας:

```
[ 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1 ]
[ 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1 ]
[ 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0 ]
```

- Ένας καλός $[52, 13, 19]$ κώδικας:

```
[ 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0 ]
[ 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1 ]
[ 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0 ]
```

- Ένας καλός $[76, 19, 24]$ κώδικας:

```
[ 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1 ]
[ 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0 ]
[ 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0 ]
```

Από τις συγκρίσεις που γίνονται παρακάτω, συμπεραίνουμε ότι οι $[20, 5, 9]$, $[28, 7, 12]$ και $[36, 9, 14]$ κώδικες είναι βέλτιστοι ανάμεσα στους γραμμικούς κώδικες με τις ίδιες παραμέτρους. Επιπλέον, οι $[44, 11, 16]$, $[52, 13, 19]$ και $[76, 19, 24]$ κώδικες επιτυγχάνουν το τωρινό κάτω φράγμα στην ελάχιστη απόσταση των QC και των γραμμικών κωδίκων ([25, 85]). Επιπρόσθετα, οι $[20, 5, 9]$ και $[44, 11, 16]$ κώδικες είναι νέοι στην κλάση των δυαδικών QC LCD κωδίκων, [46].

Κώδικας	d_{QC}	$[d_{Lb}, d_{Ub}]$	Αναφορά
$[20, 5]$	9	9	[91, 12]
$[28, 7]$	12	12	[225, 91]
$[36, 9]$	14	14	[91, 12, 117]
$[44, 11]$	16	16-17	[12]
$[52, 13]$	19	19-20	[12]
$[76, 19]$	24	24-28	[90, 117]

Πίνακας 6.2: Ελάχιστες αποστάσεις δυαδικών QC κωδίκων ρυθμού 1/4

Δυαδικοί QC Κώδικες Ρυθμού 1/5

- Ένας βέλτιστος $[25, 5, 12]$ κώδικας:

```
[ 0, 1, 0, 1, 1 ]
[ 1, 1, 1, 0, 0 ]
[ 1, 0, 0, 1, 1 ]
[ 0, 0, 1, 1, 0 ]
```

- Ένας βέλτιστος $[35, 7, 16]$ κώδικας:

```
[ 0, 0, 0, 0, 1, 1, 1 ]
[ 1, 0, 1, 1, 1, 0, 1 ]
[ 1, 0, 1, 1, 1, 1, 0 ]
[ 0, 0, 1, 0, 0, 1, 0 ]
```

- Ένας καλός $[45, 9, 18]$ LCD κώδικας:

```
[ 1, 0, 0, 1, 0, 1, 0, 1, 0 ]
[ 1, 0, 1, 0, 1, 0, 0, 0, 1 ]
[ 0, 0, 1, 1, 0, 1, 1, 0, 1 ]
[ 0, 1, 1, 1, 1, 1, 0, 0, 0 ]
```

- Ένας $[55, 11, 21]$ LCD κώδικας (καλός ανάμεσα στους QC κώδικες):

```
[ 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0 ]
[ 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1 ]
[ 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1 ]
[ 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0 ]
```

Από τις συγκρίσεις που γίνονται παρακάτω, συμπεραίνουμε ότι οι $[25, 5, 12]$ και $[35, 7, 12]$ κώδικες είναι βέλτιστοι ανάμεσα στους γραμμικούς κώδικες με τις ίδιες παραμέτρους. Επιπλέον, οι $[45, 9, 18]$ και $[55, 11, 21]$ κώδικες επιτυγχάνουν το τωρινό κάτω φράγμα στην ελάχιστη απόσταση των QC κωδίκων ([25]). Επιπρόσθετα, οι τελευταίοι κώδικες είναι νέοι στην κλάση των δυαδικών QC LCD κωδίκων, [46].

Κώδικας	d_{QC}	$[d_{Lb}, d_{Ub}]$	Αναφορά
$[25, 5]$	12	12	[91]
$[35, 7]$	16	16	[225, 91]
$[45, 9]$	18	18-19	[91]
$[55, 11]$	21	22-23	[91]

Πίνακας 6.3: Ελάχιστες αποστάσεις δυαδικών QC κωδίκων ρυθμού 1/5

Δυαδικοί QC Κώδικες Ρυθμού 1/6

- Ένας βέλτιστος $[30, 5, 15]$ κώδικας:

```
[ 1, 1, 0, 0, 0 ]
[ 0, 1, 1, 0, 1 ]
[ 1, 0, 0, 1, 1 ]
[ 0, 1, 0, 1, 0 ]
[ 1, 1, 1, 0, 1 ]
```

- Ένας βέλτιστος $[42, 7, 19]$ κώδικας:

```
[ 0, 1, 0, 0, 1, 0, 1 ]
[ 0, 0, 1, 0, 1, 1, 0 ]
[ 0, 1, 1, 0, 0, 1, 1 ]
[ 1, 0, 0, 0, 1, 1, 0 ]
[ 1, 1, 1, 0, 1, 0, 1 ]
```

- Ένας καλός $[54, 9, 23]$ κώδικας:

```
[ 1, 0, 0, 0, 1, 0, 0, 1, 1 ]
[ 0, 1, 1, 0, 1, 0, 0, 0, 0 ]
[ 0, 0, 1, 0, 0, 1, 0, 1, 1 ]
[ 1, 0, 1, 1, 1, 1, 0, 1, 0 ]
[ 1, 0, 0, 1, 0, 1, 1, 1, 0 ]
```

Από τις συγκρίσεις που γίνονται παρακάτω, συμπεραίνουμε ότι οι $[30, 5, 15]$ και $[42, 7, 19]$ κώδικες είναι βέλτιστοι ανάμεσα στους γραμμικούς κώδικες με τις ίδιες παραμέτρους. Επιπλέον, ο $[54, 9, 23]$ κώδικας επιτυγχάνει το τωρινό κάτω φράγμα στην ελάχιστη απόσταση των QC και γραμμικών κωδίκων ([25, 85]).

Κώδικας	d_{QC}	$[d_{Lb}, d_{Ub}]$	Αναφορά
$[30, 5]$	15	15	[91]
$[42, 7]$	19	19	[225, 91]
$[54, 9]$	23	23-24	[91]

Πίνακας 6.4: Ελάχιστες αποστάσεις δυαδικών QC κωδίκων ρυθμού 1/6

Δυαδικοί QC Κώδικες Ρυθμού 1/7

- Ένας βέλτιστος $[35, 5, 16]$ κώδικας:

```
[ 0, 1, 0, 0, 1 ]
[ 0, 1, 1, 0, 0 ]
[ 1, 1, 1, 0, 0 ]
[ 1, 1, 1, 0, 0 ]
[ 1, 1, 1, 1, 0 ]
[ 0, 1, 0, 0, 0 ]
```

- Ένας καλός $[77, 11, 32]$ κώδικας:

```
[ 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1 ]
[ 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0 ]
[ 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1 ]
[ 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0 ]
[ 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0 ]
[ 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1 ]
```

Από τις συγκρίσεις που γίνονται παρακάτω, συμπεραίνουμε ότι ο $[35, 5, 16]$ κώδικας είναι βέλτιστος ανάμεσα στους γραμμικούς κώδικες με τις ίδιες παραμέτρους. Επιπλέον, ο $[77, 11, 32]$ κώδικας επιτυγχάνει το τωρινό κάτω φράγμα στην ελάχιστη απόσταση των QC και γραμμικών κωδίκων ([25, 85]).

Κώδικας	d_{QC}	$[d_{Lb}, d_{Ub}]$	Αναφορά
$[35, 5]$	16	16	[91]
$[77, 11]$	32	32-33	[91]

Πίνακας 6.5: Ελάχιστες αποστάσεις δυαδικών QC κωδίκων ρυθμού 1/7

Παρατήρηση 20 *Σημειώνουμε ότι, τα κατασκευαστικά κάτω φράγματα και τα θεωρητικά πάνω φράγματα στην ελάχιστη απόσταση των γραμμικών κωδίκων που δίνονται στους Πίνακες 6.4.3, 6.4.3, 6.4.3, 6.4.3 και 6.4.3 ενδέχεται να μην έχουν προκύψει απευθείας από τους αντίστοιχους κώδικες, αλλά να έχουν παραχθεί με τεχνικές της Θεωρίας κωδίκων, γραμμικό προγραμματισμό και μη-υπαρξιακά αποτελέσματα ([117]). Για ένα λεπτομερή υπολογισμό αυτών των φραγμάτων, παραπέμπουμε στην [85].*

§6.5 Σύνδεση Οπτικών Ορθογώνιων Κωδίκων και QC Κωδίκων

Σε αυτήν την τελευταία ενότητα, εξερευνούμε πιθανές αλληλεπιδράσεις μεταξύ QC κωδίκων και μιας κλάσης κώδικων που προέρχεται από μια εφαρμογή σε διαύλους οπτικών ινών [27].

Ένας (n, w, λ) οπτικός ορθογώνιος κώδικας (optical orthogonal code), εν συντομία OOC, C, $1 \leq \lambda \leq w \leq n$, είναι μια οικογένεια από $\{0, 1\}$ ακολουθίες μήκους n και βάρους Hamming w που ικανοποιούν:

$$C_{x,y}(\tau) = \sum_{k=0}^{n-1} x(k)y(k \oplus_n \tau) \leq \lambda$$

όταν $x \neq y$ ή $\tau \neq 0$ και το σύμβολο $\oplus_n$ σημαίνει πρόσθεση $(\mathrm{mod}\ n)$. Οι OOC είναι στένα συνδεδεμένοι με διάφορες συνδυαστικές δομές. Μια ωραία βιβλιογραφική αναδρομή του θέματος με σύνδεση στους σχεδιασμούς δίνεται στην [28]. Το μέγεθος Φ του κώδικα είναι απλά ο αρθμός των κωδικολέξεων που εμπεριέχονται σε αυτόν. Στην [186] δόθηκε ο ακόλουθος ορισμός για συγχρονισμένους OOC.

Ορισμός 27 *Ένας* (n, w, λ) *συγχρονισμένος (synchronous) OOC, εν συντομία SOOC, είναι μια οικογένεια από* $\{0,1\}$ *ακολουθίες μήκους* n *και βάρους Hamming* w *που ικανοποιούν:*

$$C_{x,y}(0) \leq \lambda \quad \forall\, x \neq y.$$

Ένας (n, w, λ) κυκλικός (cyclic) SOOC, εν συντομία CSOOC, είναι ένας SOOC για τον οποίο ολές οι n κυκλικές μεταθέσεις κάθε κωδικολέξης είναι διακριτές κωδικολέξεις μέσα στον κώδικα. Αυτή η παρατήρηση οδήγησε στο ακόλουθο θεώρημα, [186].

Θεώρημα 31 (Moreno et al. [186]) *Κάθε* (n, w, λ) *OOC μεγέθους* Φ *παράγει έναν* (n, w, λ) *CSOOC μεγέθους* $n\Phi$.

Πλέον, είμαστε σε θέση να αναγνωρίσουμε την αλληλεπίδραση μεταξύ των OOC και QC κωδίκων χρησιμοποιώντας την κυκλική δομή των CSOOC.

Πόρισμα 25 *Κάθε* (n, w, λ) *OOC μεγέθους* Φ *είναι ισοδύναμος με έναν QC κώδικα μήκους* $n\Phi$*, διάστασης* n *και δείκτη* Φ.

Απόδειξη. Παράγουμε τον CSOOC μεγέθους $n\Phi$ από το Θεώρημα 31 και στη συνέχεια θεωρούμε την παράθεση των Φ κυκλικών πινάκων τάξεως n ως ένα γεννήτορα πίνακα του QC κώδικα. □

Μέρος ΙΙΙ

Κρυπτογραφία

A security system is only as strong as its weakest link.

Ferguson and Schneier (2003)

7

Κρυπτοσυστήματα Ιδιωτικού Κλειδιού

Στο έβδομο αυτό κεφάλαιο, προτείνονται δυο κρυπτογραφικά σχήματα (encryption schemes) τα οποία βασίζονται σε πίνακες Hadamard με έναν και δύο κυκλικούς πυρήνες, που είναι κλάσεις συνδυαστικών σχεδιασμών. Η μαθηματική δομή των προηγούμενων πινάκων επιτρέπει το σχεδιασμό κατάλληλων κρυπτογραφικών αλγορίθμων για την κρυπτογράφηση (encryption) και αποκρυπτογράφηση (decryption) του μηνύματος. Συγκεκριμένα, προτείνεται συμμετρική μέθοδος κρυπτογράφησης και κατα συνέπεια τα κρυπτογραφικά σχήματα από πίνακες Hadamard με κυκλικούς πυρήνες ανήκουν στην κατηγορία των κρυποσυστημάτων ιδιωτικού κλειδιού (private-key cryptosystems). Παρουσιάζεται μια εκτεταμένη κρυπτανάλυση (cryptanalysis) των προτεινόμενων κρυπτογραφικών σχημάτων ενάντια στους πιο δημοφιλείς τύπους επιθέσεων (σε κρυπτοσυστήματα), όπως είναι για παράδειγμα οι επιθέσεις εξαντλητικών υπολογισμών (brute force attacks) και οι επιθέσεις γνωστού αρχικού και κρυπτογραφημένου κειμένου (known-plaintext and ciphertext attacks). Αποδεικνύεται ότι, αυτοί οι τύποι των επιθέσεων δεν παραβιάζουν την ασφάλεια των εν λόγω κρυπτογραφικών σχημάτων, κάτω από συγκεκριμένες προϋποθέσεις. Επιπλέον, γίνεται χρήση του γινομένου Kronecker για να ενισχύσουμε την άσφαλεια των κρυπτογραφικών σχημάτων ενώ παράλληλα διατηρούμε το μέγεθος του ιδιωτικού κλειδιού σε λογικά μεγέθη.

Στο δεύτερο μέρος του κεφαλαίου προτείνουμε ένα κρυπτογραφικό σχήμα, παρόμοιο με το One Time Pad και το κρυπτογράφημα (cipher) του Hill, το οποίο βασίζεται σε μια μέθοδο κωδικοποίησης σχηματισμών Plotkin. Η διαδικασία κρυπτογράφησης είναι μια προσέγγιση του One Time Pad κρυπτογραφικού σχήματος. Επιπλέον, παρουσιάζουμε πειραματικά αποτελέσματα τα οποία υποδεικνύουν οτι μια επίθεση εξαντλητικών υπολογισμών στο προτεινόμενο κρυπτογραφικό σχήμα δεν

είναι ένας εφικτός τρόπος παραβίασης της ασφάλειας αυτού του κρυπτοσυστήματος.

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στις επιστημονικές εργασίες [164] και [160].

§7.1 Συμμετρικά Κρυπτοσυστήματα από Πίνακες Hadamard με Κυκλικούς Πυρήνες

Σε αυτήν την ενότητα, προτείνουμε κρυποσυστήματα ιδιωτικού κλειδιού ή απλούστερα συμμετρικά κρυπτογραφικά σχήματα τα οποία προέρχονται από δυαδικούς σχηματισμούς συνδυαστικών σχεδιασμών. Τα κρυπτοσυστήματα είναι συμμετρικά, υπό την έννοια οτι χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Οι αντίστοιχοι κρυπτογραφικοί αλγόριθμοι για τις διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης, καλούνται συμμετρικοί κρυπτογραφικοί αλγόριθμοι δέσμης (symmetric key block ciphers), και τεμαχίζουν σε τμήματα (blocks) το αρχικό κείμενο που πρόκειται να κρυπτογραφηθεί και κρυπτογραφούν κάθε τμήμα ξεχωριστά. Αυτού του είδους οι αλγόριθμοι, καλούνται και συμμετρικά κρυπτογραφήματα. Όταν δεν θα υπάρχει κίνδυνος σύγχυσης της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης θα αναφερόμαστε σε αυτές τις έννοιες χωρίς διάκριση.

Για μεθόδους κρυπτογράφησης από συνδυαστικούς σχεδιασμούς παραπέμπουμε τον αναγνώστη στην [201]. Εφαρμογές των συνδυαστικών σχεδιασμών στις τηλεπικοινωνίες, την κρυπτογραφία και τα δίκτυα μπορούν να βρεθούν στη βιβλιογραφική εργασία, [28].

§7.1.1 Προδιαγραφές

Είχαμε ως κίνητρο να χρησιμοποιήσουμε τους πίνακες Hadamard για τον σχεδιασμό των κρυπτογραφικών σχημάτων αυτής της ενότητας, καθώς αυτοί είναι μέρος της ευρύτερης κλάσης των συνδυαστικών σχεδιασμών και η μαθηματική τους δομή επιτρέπει την υλοποίηση αποδοτικών κρυπτογραφικών αλγορίθμων.

Το προτεινόμενο κρυπτογράφημα έχει ομοιότητες με το κρυπτογράφημα του Hill, δηλαδή την χρησιμοποίηση του πίνακα πρόσπτωσης για κρυπτογράφηση και αποκρυπτογράφηση. Για περαιτέρω λεπτομέρειες σχετικά με τη μέθοδο κρυπτογράφησης του Hill, βλ. [219]. Μια εκτενής αναφορά σε επιθέσεις που αναφέρονται σε κρυπτοσυστήματα, και περιγραφή των πιο σημαντικών κρυπτογραφικών πρωτοκόλλων μπορεί

να βρεθεί στις [49] και [18], αντίστοιχα. Στη συνέχεια, θέτουμε τις προδιαγραφές με βάση τις οποίες σχεδιάσαμε τα κρυπτογραφικά σχήματα από πίνακες Hadamard με κυκλικούς πυρήνες.

Ερευνητικό Πρόβλημα 8 *Ο σχεδιασμός κρυπτοσυστημάτων ιδιωτικού κλειδιού από συνδυαστικές δομές όπου,*

1. *Το συμμετρικό κλειδί (κρυπτογράφησης και αποκρυπτογράφησης) μοιράζεται μόνον μια φορά*
2. *Το μέγεθος του κλειδιού είναι σχετικά μικρό*
3. *Οι αντίστοιχοι κρυπτογραφικοί αλγόριθοι είναι υπολογιστικά γρήγοροι*
4. *Δεν παραβιάζεται η ασφάλεια των κρυπτοσυστημάτων από διαφόρους τύπους κρυπτογραφικών επιθέσεων*

Τα κρυπτογραφικά σχήματα αυτής της ενότητας κάνουν χρήση των προηγούμενων προδιαγραφών, και επιπλέον μπορούν να θεωρηθούν και ως η γενίκευση εκείνων που παρουσιάστηκαν στην [150].

§7.1.2 Σχεδιασμός Κρυπτογραφικών Αλγορίθμων

Υποθέτουμε ότι, το αρχικό μήνυμα το οποίο πρόκειται να μεταδοθεί με τη μορφή κειμένου (plaintext) περιέχει n χαρακτήρες, και αναπαριστάται από ένα διάνυσμα μήκους n, όπου n κάθε συντεταγμένη του διανύσματος είναι μια αριθμητική τιμή που αντιστοιχεί σε ένα συγεκριμένο χαρακτήρα στο αρχικό κείμενο (κώδικας ASCII). Σημειώνουμε ότι, ο σχεδιασμός των κρυπτογραφικών αλγορίθμων που δίνεται σε αυτήν την ενότητα είναι μια γενίκευση εκείνων που δίνονται στην [150], καθώς εδώ μελετούμε ορθογώνιους πίνακες αντί για ορθογώνιους σχηματισμούς.

Αν το μήνυμα έχει περισσότερους από n χαρακτήρες τότε η διαδικασία κρυπτογράφησης που περιγράφεται παρακάτω, επαναλαμβάνεται όσες φορές χρειάζεται. Αν έχει λιγότερους από n χαρακτήρες τότε συμπληρώνουμε το αρχικό κείμενο με τον χαρακτήρα "κενό" όσες φορές χρειάζεται. Για τις απαιτήσεις της προτεινόμενης μεθόδου κρυπτογράφησης θα κάνουμε χρήση ενός πίνακα A τάξης $n \times n$, ειδικής δομής, με

στοιχεία $\{\pm 1\}$ όπου ο πίνακας A ικανοποιεί την σχέση $AA^T = kI_n$ για κάποια σταθερά $k \in \mathbb{N}$, και I_n είναι ο μοναδιαίος πίνακας τάξης n. Η Θεωρία σχεδιασμών είναι πλούσια σε περιεχομένο από τέτοιους πίνακες ειδικής δομής, που έχουν καλές συνδυαστικές ιδιότητες, για παράδειγμα οι πίνακες Hadamard. Για περισσότερες λεπτομέρειες στην εφαρμογή των συνδυαστικών σχεδιασμών στην κρυπτογραφία παραπέμπουμε στις [28, 201].

Αν το μήνυμα το οποίο επιθυμούμε να μεταδώσουμε έχει μετατραπεί σε ένα αριθμητικό διάνυσμα $\overline{m}$, τότε το κρυπτογραφημένο μήνυμα που πρόκειται να μεταδοθεί μέσα από ένα δίαυλο επικοινωνίας είναι

$$\overline{c} = \overline{m}A + d\overline{e}_n$$

όπου d είναι μια κατάλληλη σταθερά και $\overline{e}_n = (1, \ldots, 1)$ είναι ένα $1 \times n$ διάνυσμα μονάδων. Ο παραλήπτης για να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα, θα πρέπει να κάνει χρήση της συνάρτησης $\overline{m} = 1/k(\overline{c} - d\overline{e}_n)A^T$, όπου A^T είναι ο ανάστροφος του πίνακα A που χρησιμοποιήθηκε κατά την διαδικασία κρυπτογράφησης. Αυτή η μέθοδος κρυπτογράφησης μπορεί να υλοποιηθεί με τον παρακάτω κρυπτογραφικό αλγόριθμο.

Algorithm 20 ENCRYPTION ALGORITHM

```
  function EncrAlg(msg)
Require: msg in ASCII code          ▷ Encode a sample plaintext, msg
    Select(A, d)                    ▷ Choose appropriate A and d
    k ← (A, d)                      ▷ Form private key k
    Transmit(k)                     ▷ Transmit securely the private key
    m̄ ← Convert(msg)                ▷ Convert original msg
    c̄ ← m̄A + de_n                   ▷ Encrypted msg is c̄
    return (Transmit(c̄))
  end function
```

Για να είναι η μέθοδος κρυπτογράφησης συνεπής με τις βασικές κρυπτογραφικές αρχές, θα πρέπει το κρυπτογραφημένο μήνυμα $\overline{c}$ να αποκρυπτογραφείται μοναδικά. Αυτή η απαίτηση ικανοποιείται από το παρακάτω θεώρημα.

Θεώρημα 32 *Το κρυπτογραφημένο μήνυμα $\overline{c}$ που μεταδίδεται μέσω του αλγορίθμου κρυπτογράφησης, αποκρυπτογραφείται μοναδικά ως $\overline{w} = 1/k(\overline{c} - d\overline{e}_n)A^T$ και $\overline{w} \equiv \overline{m}$.*

Απόδειξη. $\overline{c} = \overline{m}A + d\overline{e}_n \Rightarrow \overline{c} - d\overline{e}_n = \overline{m}A \Rightarrow 1/k(\overline{c} - d\overline{e}_n)A^T = 1/k(\overline{m}AA^T) \Rightarrow 1/k(\overline{c} - d\overline{e}_n)A^T = \overline{m}I_q \Rightarrow \overline{m} = 1/k(\overline{c} - d\overline{e}_n)A^T$. □

Η διαδικάσια αποκρυπτογράφησης που περιγράφεται από το προηγούμενο θεώρημα υλοποιείται με τον ακόλουθο κρυπτογραφικό αλγόριθμο.

Algorithm 21 DECRYPTION ALGORITHM

function DECRALG($\overline{c}$)
Require: given ciphertext $\overline{c}$ ▷ Decode a given ciphertext
RECEIVE(A, d) ▷ Receive the securely transmitted private key
$k \leftarrow (A, d)$ ▷ Set private key k
$\overline{m} \leftarrow 1/k(\overline{c} - d\overline{e}_n)A^T$ ▷ Decrypt ciphertext $\overline{c}$
$msg \leftarrow$ CONVERT($\overline{m}$) ▷ Original plaintext is msg
return (msg)
end function

§7.1.3 Κρυπτογραφικά Σχήματα από Πίνακες Hadamard

Σε αυτήν την ενότητα, δίνουμε αρκετές κατασκευές κρυπτογραφικών σχημάτων χρησιμοποιώντας ένα σχηματισμό ειδικής δομής. Δίνουμε επιπλέον κάποιους απαραίτητους ορισμούς και συμβολισμούς που θα κάνουμε χρήση κατά τη διάρκεια αυτής της ενότητας. Σημειώνουμε ότι, όλοι οι σχηματισμοί που ακολουθούν μπορούν να θεωρηθούν ως δυαδικοί σχηματισμοί με τη βοήθεια του παρακάτω $\{1, -1\}$-bit συμβολισμού [174].

Συμβολισμός 4 Ορισμένες φορές είναι βολικό να θεωρήσουμε ότι τα bits έχουν $\{1, -1\}$-τιμές αντί για $\{0, 1\}$-τιμές. Αν $b \in \{0, 1\}$ τότε το $\overline{b} \in \{1, -1\}$ ορίζεται ως $\overline{b} = (-1)^b$. Αν $x \in \{0, 1\}^n$ τότε το $\overline{x} \in \{1, -1\}^n$, ορίζεται ως εκείνη η συμβολοσειρά όπου το i bit της είναι $\overline{x}_i$.

Η ισχύς ενός κρυπτογραφήματος καθορίζεται από τους υπολογιστικούς πόρους που απαιτούνται για την παραβίαση της ασφάλειας του. Η υπολογιστική πολυπλοκότητα ενός αλγορίθμου είναι μετρήσιμη από δυο μεταβλητές: T για τη χρονική πολυπλοκότητα (time complexity)

που καθορίζει με ποιο τρόπο ο χρόνος εκτέλεσης μεταβάλλεται σε σχέση με το μέγεθος της εισόδου, και S για τη χωρική πολυπλοκότητα (space complexity) δηλαδή της μνήμης που απαιτείται για αποθήκευση των δεδομένων εισόδου. Οι δυο μεταβλητές T και S συνήθως εκφράζονται ως συναρτήσεις του n, όπου n είναι το μέγεθος της εισόδου (του αλγορίθμου).
Γενικότερα, η υπολογιστική πολυπλοκότητα ενός αλγορίθμου εκφράζεται από το λεγόμενο ασυμπτωτικό συμβολισμό (" big $\mathcal{O}$ " notation), που είναι ο ρυθμός αύξησης της υπολογιστικής πολυπλοκότητας. Θα χρησιμοποιήσουμε αυτόν το συμβολισμό (που περιγράφεται παρακάτω) για να δώσουμε ένα άνω φράγμα στην τάξη μεγέθους της συνάρτησης πολυπλοκότητας [30].

Συμβολισμός 5 *Για δοθείσα συνάρτηση* $g(n)$ *θα συμβολίζουμε με* $\mathcal{O}(g(n))$ *το σύνολο των συναρτήσεων* $\mathcal{O}(g(n)) = \{f(n) :$ *υπάρχουν θετικές σταθερές* c *και* n_0 *τέτοιες ώστε* $0 \leq f(n) \leq cg(n)$ *για κάθε* $n \geq n_0\}$.

Δίνουμε τον ορισμό ενός κρυπτογραφικού σχήματος από την [18].

Ορισμός 28 *Ένα κρυπτογραφικό σχήμα αποτελείται από τα ακόλουθα τρια σύνολα: ένα σύνολο κλειδιών* K*, ένα σύνολο μηνυμάτων* M*, και το κρυπτογραφημένο κείμενο* C *μαζί με τους παρακάτω τρεις αλγορίθμους.*

1. *Έναν αλγόριθμο παραγωγής κλειδιών, που παράγει ένα έγκυρο κλειδί κρυπτογράφησης* $k \in K$ *και ένα έγκυρο κλειδί αποκρυπτογράφησης* $k^{-1} \in K$*.*

2. *Έναν αλγόριθμο κρυπτογράφησης, που έχει ως είσοδο ένα μήνυμα* $m \in M$ *και ένα κλειδί κρυπτογράφησης* $k \in K$ *και δίνει ως έξοδο ένα κρυπτογραφημένο κείμενο* $c \in C$ *που ορίζεται ως* $c = E_k(m)$*.*

3. *Έναν αλγόριθμο αποκρυπτογράφησης, που έχει ως είσοδο ένα κρυπτογραφημένο μήνυμα* $c \in C$ *και ένα κλειδί αποκρυπτογράφησης* $k^{-1} \in K$ *και δίνει ως έξοδο το αρχίκο μήνυμα* $m \in M$ *που ορίζεται ως* $m = D_k^{-1}(c)$*. Απαιτούμε να ισχύει* $D_k^{-1}(E_k(m)) = m$*.*

Παρατήρηση 21 *Σημειώνουμε ότι, ενώ έχουμε χρησιμοποιήσει ως ιδιωτικό κλειδί το ζεύγος* (A, d)*, σε όρους υπολογιστικής πολυπλοκότητας μπορούμε εφεξής να αναφερομάστε στο ιδιωτικό κλειδί χρησιμοποιώντας μόνο τον πίνακα κρυπτογράφησης* A *καθώς* n d *είναι τάξης μεγέθους* $\mathcal{O}(1)$*.*

Υπενθυμίζουμε παρακάτω τον ορισμό ενός πίνακα Hadamard.

Ορισμός 29 *Ένας πίνακας Hadamard τάξης* n *είναι ένας τετραγωνικός* $n \times n$ *πίνακας* H *όπου τα στοιχεία του είναι* $+1$ *και* -1*, με την ιδιότητα*

$$HH^T = nI_n.$$

Η ιδιότητα αυτή διασφαλίζει ότι οι γραμμές (αλλά και στήλες) του πίνακα Hadamard είναι αμοιβαία ορθογώνιες. Είναι γνωστό ότι αν n είναι η τάξη ενός πίνακα Hadamard τότε αυτή είναι απαραίτητα $1, 2$ ή ένα πολλαπλάσιο του 4. Οι πίνακες Hadamard έχουν χρησιμοποιηθεί στη Συνδυαστική, τη Στατιστική, τη Θεωρία κωδίκων και στις τηλεπικοινωνίες και σε διάφορες άλλες περιοχές. Περαιτέρω λεπτομέρειες για αυτούς τους πίνακες μπορούν να βρεθούν στις [32, 206].

Ως πίνακα κρυπτογράφησης για το προτεινόμενο σχήμα θα χρησιμοποιήσουμε έναν πίνακα Hadamard τάξης n. Σε αυτή την περίπτωση είναι προφανές ότι η χρήση δυο διαφορετικών πινάκων Hadamard ίδιας τάξης θα παράγει δυο διαφορετικά κρυπτογραφημένα κείμενα, λόγω της ύπαρξης της ιδιότητας της H-ισοδυναμίας που περιγράφεται παρακάτω (βλ. και δεύτερο κεφάλαιο).

Δυο πίνακες Hadamard θα καλούνται ισοδύναμοι ή H-ισοδύναμοι αν ο ένας μπορεί να μετασχηματιστεί στον άλλον εφαρμόζοντας διαδοχικά τους ακόλουθους μετασχηματισμούς:

- Πολλαπλασιασμούς γραμμών και στηλών με -1
- Εναλλαγές γραμμών και στηλών

Δύο πίνακες Hadamard θα καλούνται μη-ισοδύναμοι, αν αυτοί δεν είναι ισοδύναμοι. Επομένως, η επιλογή μη-ισοδύναμων πινάκων Hadamard ως πινάκων κρυπτογράφησης διασφαλίζει ότι θα παραχθούν διαφορετικά κρυπτογραγημένα κείμενα. Σε αντίθετη περίπτωση, κάποιος θα μπορούσε να μετασχηματίσει τον έναν πίνακα κρυπτογράφησης στον άλλον, ακολουθώντας τους μετασχηματισμούς που αναφέρθηκαν προηγουμένως.

Ειναι ζωτικής σημασίας για την εφαρμογή μας να έχουμε στη διάθεση μας μεγάλες βάσεις δεδομένων από μη-ισοδύναμους πίνακες Hadamard. Το υπολογιστικό πακέτο Magma, στην έκδοση 2.13, περιέχει μια βάση δεδομένων από μη-ισοδύναμους πίνακες Hadamard. Υπάρχουν αρκετές χιλιάδες μη-ισοδύναμοι πίνακες Hadamard για ορισμένες τάξεις. Για παράδειγμα, στην τάξη 32 που είναι ένα λογικό μέγεθος για τη διαδικασία κρυπτογράφησης υπάρχουν περισσότεροι από $3,578,006$ μη-ισοδύναμοι πίνακες Hadamard [190].

Το ιδιωτικό κλειδί k που χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης, θα είναι ένας πίνακας Hadamard τάξης n, $A = H_n$, και αποτελείται από $n \times n$ bits. Σε όρους υπολογιστικής πολυπλοκότητας, n τάξη μεγέθους του κλειδιού είναι $\mathcal{O}(n^2)$.

Πρόταση 17 *Υπάρχει μια οικογένεια κρυπτογραφικών σχημάτων, που θα καλούμε* Hadamard Ciphers, *η οποία παράγεται από πίνακες Hadamard τάξεως* n.

Απόδειξη. Ένα κρυπτογραφικό σχήμα αυτής της οικογένειας θα χρησιμοποιεί ένα πίνακα Hadamard A τάξης n, και ένα κλειδί k με τάξη μεγέθους $\mathcal{O}(n^2)$, όπως περιγράφηκε προηγούμενως, και μπορεί να κρυπτογραφηθεί – αποκρυπτογραφηθεί χρησιμοποιώντας τους Αλγορίθμους 20 και 21 καθώς ισχύει $AA^T = nI_n$. □

Υπάρχουν ορισμένες ειδικές κατασκευές πινάκων Hadamard που μας επιτρέπουν να μειώσουμε την τάξη μεγέθους του ιδιωτικού κλειδιού, όπως θα δούμε στη συνέχεια αυτής της ενότητας.

Σχήματα από πίνακες Hadamard με έναν Κυκλικό Πυρήνα Ένας πίνακας Hadamard τάξης $p+1$, ο οποίος μπορεί να γραφτεί σε μια από τις δυο παρακάτω ισοδύναμες μορφές

$$\left[\begin{array}{c|c} 1 & 1\cdots 1 \\ \hline 1 & \\ \vdots & C \\ 1 & \end{array}\right] \quad \text{ή} \quad \left[\begin{array}{c|c} 1 & \\ \vdots & C \\ 1 & \\ \hline 1 & -1\cdots -1 \end{array}\right]$$

όπου ο $C = (c_{ij})$ είναι ένας κυκλικός πίνακας τάξης p, δηλαδή $c_{ij} = c_{1,j-i+1 \pmod p}$, θα λέμε ότι έχει έναν κυκλικό πυρήνα (circulant core). Οι παρακάτω πίνακες είναι παραδείγματα τέτοιων πινάκων τάξεως 12.

1	1	1	1	1	1	1	1	1	1	1
1	-	1	-	1	1	1	-	-	-	1	-
1	-	-	1	-	1	1	1	-	-	-	1
1	1	-	-	1	-	1	1	1	-	-	-
1	-	1	-	-	1	-	1	1	1	-	-
1	-	-	1	-	-	1	-	1	1	1	-
1	-	-	-	1	-	-	1	-	1	1	1
1	1	-	-	-	1	-	-	1	-	1	1
1	1	1	-	-	-	1	-	-	1	-	1
1	1	1	1	-	-	-	1	-	-	1	-
1	-	1	1	1	-	-	-	1	-	-	1
1	1	-	1	1	1	-	-	-	1	-	-

1	1	-	1	-	-	-	1	1	1	-	1
1	1	1	-	1	-	-	-	1	1	1	-
1	-	1	1	-	1	-	-	-	1	1	1
1	1	-	1	1	-	1	-	-	-	1	1
1	1	1	-	1	1	-	1	-	-	-	1
1	1	1	1	-	1	1	-	1	-	-	-
1	-	1	1	1	-	1	1	-	1	-	-
1	-	-	1	1	1	-	1	1	-	1	-
1	-	-	-	1	1	1	-	1	1	-	1
1	1	-	-	-	1	1	1	-	1	1	-
1	-	1	-	-	-	1	1	1	-	1	1
1	-	-	-	-	-	-	-	-	-	-	-

όπου με $-$ συμβολίζουμε το στοιχείο -1.

Το κρυπτογραφικό σχήμα κατασκευάζεται θεωρώντας τον προηγούμενο πίνακα Hadamard $A = H_n$ τάξης $n = 4m = p + 1$ ως πίνακα κρυπτογράφησης. Όμως σε αυτή την περίπτωση, η κυκλική δομή του πίνακα Hadamard μας παρέχει τη δυνάτοτητα να χρησιμοποιήσουμε ένα κλειδί αρκετά μικρότερου μεγέθους από οτι στην περίπτωση των Hadamard Ciphers.

Με $A_c = [a_1, a_2, \ldots, a_p]$ ας συμβολίσουμε την πρώτη γραμμή του κυκλικού πίνακα, C, που χρησιμοποιήθηκε στην προηγούμενη κατασκεύη. Το ιδιωτικό κλειδί k για αυτό το κρυπτογραφικό σχήμα είναι το δυαδικό διάνυσμα, A_c το οποίο αποτελείται από p bits. Συνεπώς, όταν κάνουμε χρήση ενός πίνακα Hadamard τάξης $n = p + 1$ της παραπάνω μορφής, η τάξη μεγέθους του κλειδιού είναι $\mathcal{O}(n)$, καθώς αυτό αποτελείται από $p = n - 1$ bits.

Πρόταση 18 *Υπάρχει μια οικογένεια κρυπτογραφικών σχημάτων, που θα καλούμε* Hadamard Core Ciphers, *η οποία παράγεται από πίνακες Hadamard με έναν κυκλικό πυρήνα τάξεως* $n = p + 1$.

Απόδειξη. Ένα κρυπτογραφικό σχήμα αυτής της οικογένειας θα χρησιμοποιεί ένα πίνακα Hadamard A με έναν κυκλικό πυρήνα τάξης $n = p + 1$, και ένα κλειδί $k = A_c$ με τάξη μεγέθους $\mathcal{O}(n)$, όπως περιγράφηκε προηγούμενως, και μπορεί να κρυπτογραφηθεί – αποκρυπτογραφηθεί χρησιμοποιώντας τους Αλγορίθμους 20 και 21 καθώς ισχύει $AA^T = nI_n$. □

Τέσσερις οικογένειες πινάκων Hadamard αυτής της μορφής έχουν βρεθεί από τους Paley [191], Stanton, Sprott και Whiteman [220, 234], Singer [214] και Marshall Hall Jr. [98], και οι οποίοι μπορούν να χρησιμοποιηθούν στην προηγούμενη πρόταση για να παράγουν άπειρες οικογένειες από Hadamard Core Ciphers. Το παρακάτω θεώρημα δόθηκε στην [135].

Θεώρημα 33 (Circulant Core Hadamard Construction Theorem) *Ένας πίνακας Hadamard τάξης* $p + 1$ *με έναν κυκλικό πυρήνα μπορεί να κατασκευαστεί αν*

1. $p \equiv 3 \pmod 4$ *είναι πρώτος [191].*
2. $p = q(q + 2)$ *όπου* q *και* $q + 2$ *είναι και οι δυο πρώτοι [220, 234].*
3. $p = 2^t - 1$ *όπου* t *είναι ένας θετικός ακέραιος [214].*
4. $p = 4x^2 + 27$ *όπου* p *είναι πρώτος και* x *ένας θετικός ακέραιος [98].*

Σχήματα από πίνακες Hadamard με Δυο Κυκλικούς Πυρήνες Ένας πίνακα Hadamard τάξης $2\ell + 2$ (για ℓ περιττό), ο οποίος μπορεί να γραφεί σε μια από τις δύο παρακάτων ισοδύναμες μορφές (όπου με $-$ συμβολίζουμε το -1 και με $+$ το $+1$)

$$\left[\begin{array}{cc|ccc} - & - & + & \cdots & + \\ - & + & + & \cdots & - \\ \hline + & + & & & \\ \vdots & \vdots & & A & \\ + & + & & & \\ \hline + & - & & & \\ \vdots & \vdots & & B^T & \\ + & - & & & \end{array}\right.\quad \left.\begin{array}{ccc} + & \cdots & + \\ - & \cdots & - \\ \hline & & \\ & B & \\ & & \\ \hline & & \\ & -A^T & \\ & & \end{array}\right] \quad \text{ή} \quad \left[\begin{array}{cc|cc} + & + & & \\ \vdots & & A & B \\ + & + & & \\ \hline + & - & & \\ \vdots & & B^T & -A^T \\ + & - & & \\ \hline - & - & + \cdots + & + \cdots + \\ - & + & + \cdots + & - \cdots - \end{array}\right]$$

όπου $A = (a_{ij})$, $B = (b_{ij})$ είναι δυο κυκλικοί πίνακες (με στοιχεία ± 1) τάξεως ℓ, δηλαδή $a_{ij} = a_{1,j-i+1 \pmod{\ell}}$, $b_{ij} = b_{1,j-i+1 \pmod{\ell}}$, θα λέμε ότι έχει δυο κυκλικούς πυρήνες.

Όπως και προηγουμένως, το κρυπτογραφικό σχήμα κατασκευάζεται χρησιμοποιώντας ως πίνακα κρυπτογράφησης τον προηγούμενο πίνακα Hadamard $A = H_n$ τάξης $n = 2\ell+2$. Επίσης, και σε αυτήν την περίπτωση η κυκλική δομή του πίνακα Hadamard μας παρέχει τη δυνατότητα να χρησιμοποιήσουμε ένα κλειδί αρκετά μικρότερου μεγέθους από οτι στην περίπτωση των Hadamard Ciphers, ως ακολούθως.

Με $A_c = [a_1, a_2, \ldots, a_\ell]$ και $B_c = [b_1, b_2, \ldots, b_\ell]$, ας συμβολίσουμε τις πρώτες γραμμές των κυκλικών πινάκων, A και B που χρησιμοποιήθηκαν στην προηγούμενη κατασκεύη, αντίστοιχα. Το ιδιωτικό κλειδί k για αυτό το κρυπτογραφικό σχήμα είναι η παράθεση των δυο διανυσμάτων, A_c και B_c, που συμβολίζουμε με $A_c \oplus B_c$ και αποτελείται από $\ell + \ell$ bits. Συνεπώς, όταν κάνουμε χρήση ενός πίνακα Hadamard τάξης $n = 2\ell + 2$ ως πίνακα κρυπτογράφησης η τάξη μεγέθους του κλειδιού είναι $\mathcal{O}(n)$, καθώς αυτό αποτελείται από $2\ell = n - 2$ bits.

Πρόταση 19 *Υπάρχει μια οικογένεια κρυπτογραφικών σχημάτων, που θα καλούμε* Hadamard Cores Ciphers, *η οποία παράγεται από πίνακες Hadamard με δύο κυκλικούς πυρήνες τάξεως* $n = 2\ell + 2$.

Απόδειξη. Ένα κρυπτογραφικό σχήμα αυτής της οικογένειας θα χρησιμοποιεί ένα πίνακα Hadamard A με δύο κυκλικούς πυρήνες τάξης $n = 2\ell + 2$, και ένα κλειδί $k = A_c \oplus B_c$ με τάξη μεγέθους $\mathcal{O}(n)$, όπως περιγράφηκε προηγούμενως, και μπορεί να κρυπτογραφηθεί – αποκρυπτογραφηθεί χρησιμοποιώντας τους Αλγορίθμους 20 και 21 καθώς ισχύει $AA^T = nI_n$. □

Επειδή το $2\ell + 2$ πρέπει να ισούται με ένα πολλαπλάσιο του 4, έχουμε ότι το ℓ πρέπει να είναι ένας περιττός ακεράιος έτσι ώστε αυτή η κατασκευή να παράγει πίνακες Hadamard.

Στην [69] αναφέρεται ότι τα γενικευμένα ζεύγη Legendre (Generalized Legendre, GL, pairs), τα οποία μπορούν να χρησιμοποιηθούν για να κατασκευάσουν πίνακες Hadamard τάξεως $2\ell+2$ με δυο κυκλικούς πυρήνες, υπάρχουν για αρκετές περιπτώσεις. Αυτοί οι πίνακες μπορούν να χρησιμοποιηθούν στην προηγούμενη πρόταση για να παράγουν άπειρες οικογένειες από Hadamard Cores Ciphers. Το παρακάτω θεώρημα δόθηκε στην [136].

Θεώρημα 34 (Two Circulant Cores Hadamard Construction Theorem) *Ένας πίνακας Hadamard τάξης $2\ell+2$ με δυο κυκλικούς πυρήνες μπορεί να κατασκευαστεί αν*

1. *ℓ είναι πρώτος (βλ. για παράδειγμα [50]).*
2. *$2\ell+1$ είναι δύναμη πρώτου (που προκύπτει από Szekeres σύνολα διαφορών, βλ. για παράδειγμα [50] ή [70]).*
3. *$\ell = 2^k - 1$, $k \geq 2$ (δύο ακολουθίες Galois είναι ένα GL-ζεύγος, βλ. για παράδειγμα [204]).*
4. *$\ell = p(p+2)$ όπου τα p και $p+2$ είναι και οι δυο πρώτοι (δύο τέτοιες ακολουθίες είναι ένα GL-ζεύγος, βλ. για παράδειγμα [220, 234]).*
5. *$\ell = 49, 57$ (αυτοί βρέθηκαν χρησιμοποιώντας γενικευμένη κυκλοτομία, βλ. [70, 96]).*
6. *$\ell = 3, 5, \ldots, 45$ (αυτοί βρέθηκαν και ταξινομήθηκαν με εξαντλητικούς υπολογιστικούς ελέγχους, βλ. [50]).*
7. *$\ell = 47, 49, 51, 53$ και 55 (αυτοί βρέθηκαν και ταξινομήθηκαν με μερικούς υπολογιστικούς ελέγχους, βλ. [50]).*
8. *$\ell = 143$ (και επίσης πιστοποιήθηκαν τα αποτελέσματα για $\ell = 3$, 5, 7, 11, 13, 15, 17, 19, 23, 25, 31, 35, 37, 41, 43, 53, 59, 61, 63 βλ. [60]).*

§7.2 Μέθοδοι Κρυπτανάλυσης για Κρυπτογραφήματα Hadamard

Οι κύριες κρυπτογραφικές επιθέσεις μπορούν να ταξινομηθούν στις ακόλουθες τρεις κατηγορίες:

- επιθέσεις εξαντλητικών υπολογισμών (brute force attacks).
- επιθέσεις αρχικού κειμένου (plaintext attacks).
- επιθέσεις κρυπτογραφημένου κειμένου (ciphertext attacks).

Σε αυτήν την ενότητα, δείχνουμε ότι η ασφάλεια των Hadamard Ciphers και των υποκατηγοριών τους, Hadamard Core Ciphers και Hadamard Cores Ciphers, δεν παραβιάζεται από επιθέσεις εξαντλητικών

υπολογισμών και επιθέσεις κρυπτογραφημένου κειμένου, ενώ θεωρώντας κάποιους περιορισμούς στα κρυπτογραφήματα Hadamard αυτά είναι ασφαλή ενάντια σε επιθέσεις γνωστού μηνύματος (known-plaintext attacks), επιθέσεις επιλεγμένου μηνύματος (chosen-plaintext attacks) και επιθέσεις επιλεγμένου κρυπτογραφημένου κειμένου (chosen-ciphertext attacks).

§7.2.1 Κρυπτανάλυση Επιθέσεων Εξαντλητικών Υπολογισμών για Κρυπτογραφήματα Hadamard

Ορισμός 30 *Μια επίθεση εξαντλητικού υπολογισμού είναι μια μέθοδος παραβίασης της ασφάλειας ενός κρυπτοσυστήματος δοκιμάζοντας ένα μεγάλο αριθμό συνδυασμών των κλειδιών. Για τα περισσότερα κρυπτογραφήματα, μια τέτοια επίθεση τυπικά σημαίνει έναν εξαντλητικό υπολογισμό όλου του χώρου κλειδιών, δηλαδή ο έλεγχος όλων των δυνατών κλειδιών έτσι ώστε να ανακτηθεί το αρχικό μήνυμα το οποίο χρησιμοποιήθηκε για να παραχθεί ένα συγκεκριμένο κρυπτογραφημένο κείμενο.*

Ένας τρόπος για τον επιτιθέμενο να σπάσει κάποιον από τους Hadamard Ciphers με μια επίθεση εξαντλητικού υπολογισμού είναι να παράγει όλους τους δυνατούς πίνακες με στοιχεία ± 1, δηλαδή 2^{n^2} πίνακες, καθώς οι πίνακες Hadamard τάξεως n αναπαριστώνται με n^2 bits. Όμως λόγω της κυκλικής δομής των πινάκων υπάρχει μια πιο αποδοτική μέθοδος επίθεσης αυτού του τύπου που θα αναπτύξουμε στη συνέχεια αυτής της ενότητας.

Κρυπτανάλυση Επιθέσεων Εξαντλητικών Υπολογισμών για Hadamard Core Ciphers Για να μπορέσει ο επιτιθέμενος να σπάσει κάποιον από τους Hadamard Core Ciphers με μια επίθεση εξαντλητικού υπολογισμού, θα πρέπει να εξάγει το κλειδί κρυπτογράφησης $k = A_c$ που είναι το δυαδικό διάνυσμα $A_c = [a_1, a_2, \ldots, a_p]$ μήκους p δοκιμάζοντας ένα μεγάλο αριθμό συνδυασμών των κλειδιών.

Στην περίπτωσή μας, ο επιτιθέμενος θα πρέπει να προσομοιώσει έναν εξαντλητικό υπολογισμό όλου του χώρου κλειδιών. Υποθέτοντας ότι, ο επιτιθέμενος έχει γνώση του μηχανισμού κρυπτογράφησης των

Hadamard Core Ciphers θα πρέπει να ψάξει p δυαδικές μεταβλητές. Καθώς το κλειδί κρυπτογράφησης αποτελείται από δυαδικές μεταβλητές με απλή απαρίθμηση το μέγεθος του χώρου κλειδιών, $\mathsf{K}(\mathcal{H}_p)$, είναι $|\ \mathsf{K}(\mathcal{H}_p)\ | = 2^p$, συνεπώς n τάξη μεγέθος του $\mathcal{O}(2^n)$ μεταβάλλεται εκθετικά καθώς το $n = p + 1$ αυξάνει. Επιπλέον, n πιθανότητα μια λύση που παράγεται από έναν εξαντλητικό υπολογισμό του χώρου κλειδιών να είναι ένα κλειδί κρυπτογράφησης δίνεται από το συνολικό αριθμό πινάκων Hadamard με έναν κυκλικό πυρήνα που υπάρχει για κάποια τάξη δια το μέγεθος του χώρου κλειδιών σε αυτή την τάξη.

Για παράδειγμα, αν θεωρήσουμε Hadamard Core Ciphers που κάνουν χρήση πινάκων Hadamard τάξεως $24 = 23 + 1$, τότε ο χώρος κλειδιών αποτελείται από 23 δυαδικές μεταβλητές ενώ ο συνολικός αριθμών πινάκων Hadamard αυτού του τύπου που υπάρχουν σε αυτή την τάξη είναι 46. Συνεπώς, έχουμε 46 πιθανά κλειδιά κρυπτογράφησης. Όπως μπορούμε να δούμε από τον ακόλουθο πίνακα, n πιθανότητα να σπάσει αυτό το κρυπτογράφημα μέσω μιας επίθεσης εξαντλητικού υπολογισμού είναι πολύ μικρή, $\mathsf{P} = \frac{46}{2^{23}} \approx 0.00002$. Αξίζει να αναφερθεί ότι χρησιμοποιώντας ένα κλειδί μεγέθους μόνον 23 bits, παρέχεται σχεδόν πλήρης ασφάλεια ενάντια σε επιθέσεις εξαντλητικών υπολογισμών για τους Hadamard Core Ciphers.

Συνοψίζουμε στον ακόλουθο πίνακα τους διαθέσιμους πίνακες Hadamard με έναν κυκλικό πυρήνα, που συμβολίζουμε με $|\ \mathsf{V}(\mathcal{H}_p)\ |$, για τάξεις $n = p + 1$ όπου $p = 3, 7, 11, 15, 19, 23$ χρησιμοποιώντας τα αποτελέσματα που δόθηκαν στην [135], τη πληθικότητα του χώρου κλειδιών $|\ \mathsf{K}(\mathcal{H}_p)\ |$, και την πιθανότητα P_{BA} να σπάσει το κρυπτογράφημα μέσω μιας επίθεσης εξαντλητικού υπολογισμού για κάθε τάξη.

p	Τάξη	$\lvert\ \mathsf{V}(\mathcal{H}_p)\ \rvert$	$\lvert\ \mathsf{K}(\mathcal{H}_p)\ \rvert = 2^p$	$\mathsf{P}_{\mathsf{BA}} = \frac{\lvert\mathsf{V}(\mathcal{H}_p)\rvert}{\lvert\mathsf{K}(\mathcal{H}_p)\rvert}$
3	4	3	2^3	$\mathsf{P} = \frac{3}{2^3} \approx 0.375$
7	8	14	2^7	$\mathsf{P} = \frac{14}{2^7} \approx 0.1$
11	12	22	2^{11}	$\mathsf{P} = \frac{22}{2^{11}} \approx 0.01$
15	16	30	2^{15}	$\mathsf{P} = \frac{30}{2^{15}} \approx 0.0009$
19	20	38	2^{19}	$\mathsf{P} = \frac{38}{2^{19}} \approx 0.00007$
23	24	46	2^{23}	$\mathsf{P} = \frac{46}{2^{23}} \approx 0.00002$

Πίνακας 7.1: Πιθανότητα παραβίασης της ασφάλειας των Hadamard Core Ciphers μέσω επιθέσεων εξαντλητικών υπολογισμών

Από τον προηγούμενο πίνακα, μπορούμε να δούμε ότι η ακολουθία των πιθανοτήτων P_{BA} μειώνεται συνεχώς. Με βάση αυτά τα υπολογιστικά αποτελέσματα, εξάγουμε την ακόλουθη παρατήρηση, όταν η τάξη n είναι αρκετά μεγάλη.

Παρατήρηση 22 *Η ασφάλεια των* Hadamard Core Ciphers *δεν παραβιάζεται από επιθέσεις εξαντλητικών υπολογισμών, όταν η τάξη* n *(των πινάκων Hadamard με έναν κυκλικό πυρήνα) είναι αρκετά μεγάλη.*

Το σύγχρονο υπολογιστικό υλικό κρυπτανάλυσης έχει τη δυνατότητα να εκτελεί έναν εξαντλητικό υπολογισμό για 2^{128} κλειδιά, [203]. Αυτή η παρατήρηση μας δίνει μια εκτίμηση της ασφάλειας που χρειάζεται ενάντια σε επιθέσεις εξαντλητικών υπολογισμών. Προφανώς, η χρήση ενός πίνακα Hadamard τάξης $n > 128$, που μπορεί εύκολα να κατασκευαστεί από το Θεώρημα 33 για μεγάλες τάξεις, ως πίνακα κρυπτογράφησης δικαιολογεί τον προηγούμενο μας ισχυρισμό (βλ. Παρατήρηση 22).

Κρυπτανάλυση Επιθέσεων Εξαντλητικών Υπολογισμών για Hadamard Cores Ciphers Για να μπορέσει ο επιτιθέμενος να σπάσει κάποιον από τους Hadamard Cores Ciphers με μια επίθεση εξαντλητικού υπολογισμού, θα πρέπει να εξάγει το κλειδί κρυπτογράφησης $k = A_c \oplus B_c$ που είναι η παράθεση των δυαδικών διανυσμάτων $A_c = [a_1, a_2, \ldots, a_\ell]$ και $B_c = [b_1, b_2, \ldots, b_\ell]$ συνολικού μήκους 2ℓ, δοκιμάζοντας ένα μεγάλο αριθμό συνδυασμών των κλειδιών.

Στην περίπτωση μας, ο επιτιθέμενος θα πρέπει να προσομοιώσει έναν εξαντλητικό υπολογισμό όλου του χώρου κλειδιών. Υποθέτοντας ότι, ο επιτιθέμενος έχει γνώση του μηχανισμού κρυπτογράφησης των Hadamard Cores Ciphers θα πρέπει να ψάξει 2ℓ δυαδικές μεταβλητές. Καθώς το κλειδί κρυπτογράφησης αποτελείται από δυαδικές μεταβλητές με απλή απαρίθμηση το μέγεθος του χώρου κλειδιών, $K(\mathcal{H}_\ell)$, είναι $| K(\mathcal{H}_\ell) | = 2^{2\ell}$, συνεπώς η τάξη μεγέθος του $\mathcal{O}(2^n)$ μεταβάλλεται εκθετικά καθώς το $n = 2\ell + 2$ αυξάνει. Επιπλέον, η πιθανότητα μια λύση που παράγεται από έναν εξαντλητικό υπολογισμό του χώρου κλειδιών να είναι ένα κλειδί κρυπτογράφησης δίνεται από το συνολικό αριθμό πινάκων Hadamard με δυο κυκλικούς πυρήνες που υπάρχει για κάποια τάξη δια το μέγεθος του χώρου κλειδιών σε αυτή την τάξη.

Για παράδειγμα, αν θεωρήσουμε Hadamard Cores Ciphers που κάνουν χρήση πινάκων Hadamard τάξεως $28 = 2 \cdot 13 + 2$, τότε ο χώρος κλειδιών αποτελείται από 26 δυαδικές μεταβλητές ενώ ο συνολικός αριθμών πινάκων Hadamard αυτού του τύπου που υπάρχουν σε αυτή

την τάξη είναι $7,098$. Συνεπώς, έχουμε $7,098$ πιθανά κλειδιά κρυπτογράφησης. Όπως μπορούμε να δούμε από τον ακόλουθο πίνακα, n πιθανότητα να σπάσει αυτό το κρυπτογράφημα μέσω μιας επίθεσης εξαντλητικού υπολογισμού είναι πολύ μικρή, $\mathrm{P} = \frac{42 \times 13^2}{2^{26}} \approx 0.0001$. Αξίζει να αναφερθεί ότι χρησιμοποιώντας ένα κλειδί μεγέθους μόνον 26 bits, παρέχεται σχεδόν πλήρης ασφάλεια εναντία σε επιθέσεις εξαντλητικών υπολογισμών για τους Hadamard Cores Ciphers.

Συνοψίζουμε στον ακόλουθο πίνακα τους διαθέσιμους πίνακες Hadamard με δύο κυκλικούς πυρήνες, που συμβολίζουμε με $\mid \mathrm{V}(\mathcal{H}_\ell) \mid$, για τάξεις $\mathrm{n} = 2\ell + 2$ όπου $\ell = 3, \ldots, 25$ χρησιμοποιώντας τα αποτελέσματα που δόθηκαν στις [50, 136], τη πληθικότητα του χώρου κλειδιών $\mid \mathrm{K}(\mathcal{H}_\ell) \mid$, και την πιθανότητα P_{BA} να σπάσει το κρυπτογράφημα μέσω μιας επίθεσης εξαντλητικού υπολογισμού για κάθε τάξη.

ℓ	Τάξη	$\mid \mathrm{V}(\mathcal{H}_\ell) \mid$	$\mid \mathrm{K}(\mathcal{H}_\ell) \mid = 2^{2\ell}$	$\mathrm{P}_{\mathrm{BA}} = \frac{\lvert \mathrm{V}(\mathcal{H}_\ell) \rvert}{\lvert \mathrm{K}(\mathcal{H}_\ell) \rvert}$
3	8	$9 = 1 \times 3^2$	2^6	$\mathrm{P} = \frac{1 \times 3^2}{2^6} \approx 14 \cdot 10^{-2}$
5	12	$50 = 2 \times 5^2$	2^{10}	$\mathrm{P} = \frac{2 \times 5^2}{2^{10}} \approx 4 \cdot 10^{-2}$
7	16	$196 = 4 \times 7^2$	2^{14}	$\mathrm{P} = \frac{4 \times 7^2}{2^{14}} \approx 10 \cdot 10^{-3}$
9	20	$972 = 12 \times 9^2$	2^{18}	$\mathrm{P} = \frac{12 \times 9^2}{2^{18}} \approx 4 \cdot 10^{-3}$
11	24	$2,904 = 24 \times 11^2$	2^{22}	$\mathrm{P} = \frac{24 \times 11^2}{2^{22}} \approx 7 \cdot 10^{-4}$
13	28	$7,098 = 42 \times 13^2$	2^{26}	$\mathrm{P} = \frac{42 \times 13^2}{2^{26}} \approx 10 \cdot 10^{-5}$
15	32	$38,700 = 172 \times 15^2$	2^{30}	$\mathrm{P} = \frac{172 \times 15^2}{2^{30}} \approx 3 \cdot 10^{-5}$
17	36	$93,058 = 322 \times 17^2$	2^{34}	$\mathrm{P} = \frac{322 \times 17^2}{2^{34}} \approx 5 \cdot 10^{-6}$
19	40	$161,728 = 448 \times 19^2$	2^{38}	$\mathrm{P} = \frac{488 \times 19^2}{2^{38}} \approx 5 \cdot 10^{-7}$
21	44	$433,944 = 984 \times 21^2$	2^{42}	$\mathrm{P} = \frac{984 \times 21^2}{2^{42}} \approx 10 \cdot 10^{-8}$
23	48	$1,235,744 = 2336 \times 23^2$	2^{46}	$\mathrm{P} = \frac{2336 \times 23^2}{2^{46}} \approx 2 \cdot 10^{-8}$
25	52	$2,075,000 = 3320 \times 25^2$	2^{50}	$\mathrm{P} = \frac{3320 \times 25^2}{2^{50}} \approx 2 \cdot 10^{-9}$

Πίνακας 7.2: Πιθανότητα παραβίασης της ασφάλειας των Hadamard Cores Ciphers μέσω επιθέσεων εξαντλητικών υπολογισμών

Από τον προηγούμενο πίνακα, μπορούμε να δούμε ότι n ακολουθία πιθανοτήτων P_{BA} μειώνεται συνεχώς (και χρησιμοποιώντας την [136, Ιδιότητα 1.]) είναι άνω φραγμένη από το 1. Επιπρόσθετα, δεχόμενοι το αληθές της [136, Εικασίας 1.], τότε για κάθε περιττό $\ell = 3, \ldots$ υπάρχει

ένας πίνακας Hadamard τάξης $2\ell+2$ με δύο κυκλικούς πυρήνες, και ότι η ακολουθία των πληθικοτήτων $|\,V(\mathcal{H}_\ell)\,|$ θα συνεχίσει να αυξάνει μπορούμε να συμπεράνουμε ότι το όριο της ακολουθίας των πιθανοτήτων $\lim_{\ell\to\infty} P_{BA} = \lim_{\ell\to\infty} \frac{|\,V(\mathcal{H}_\ell)\,|}{|\,K(\mathcal{H}_\ell)\,|}$ θα συγκλίνει στο μηδέν. Ιδιαίτερα, εξάγουμε το ακόλουθο λήμμα.

Λήμμα 19 *Υποθέτουμε ότι ισχύουν οι ακόλουθες συνθηκες,*

(i) Υπάρχει ένας πίνακας Hadamard τάξης $2\ell+2$ με δυο κυκλικούς πυρήνες για κάθε περιττό $\ell = 3,\ldots$

(ii) Η ακολουθία των πληθικοτήτων $|\,V(\mathcal{H}_\ell)\,|$ είναι αύξουσα για κάθε περιττό $\ell = 3,\ldots$

Τότε, η ασφάλεια των Hadamard Cores Ciphers *δεν παραβιάζεται από επιθέσεις εξαντλητικών υπολογισμών.*

Απόδειξη. Καθώς, $\lim_{\ell\to\infty} P_{BA} = \lim_{\ell\to\infty} \frac{|\,V(\mathcal{H}_\ell)\,|}{|\,K(\mathcal{H}_\ell)\,|} \to 0$ όπως το $n = 2\ell+2$ αυξάνει, είναι υπολογιστικά ανέφικτο μια επίθεση εξαντλητικού υπολογισμού να εξάγει το κλειδί κρυπτογράφησης. □

§7.2.2 Κρυπτανάλυση Επιθέσεων Αρχικού Κειμένου για Κρυπτογραφήματα Hadamard

Σε αυτήν την ενότητα, παρουσιάζεται μια μελέτη κρυπτανάλυσης επιθέσεων αρχικού κειμένου για Κρυπτογραφήματα Hadamard. Συγκεκριμένα, αναλύονται μέθοδοι κρυπτανάλυσης επιθέσεων γνωστού και επιλεγμένου μηνύματος.

Κρυπτανάλυση Επιθέσεων Γνωστού Μηνύματος για Κρυπτογραφήματα Hadamard

Ορισμός 31 *Μια επίθεση γνωστού μηνύματος είναι εκείνη κατά την οποία ο επιτιθέμενος έχει ποσότητα του αρχικού μηνύματος και του αντίστοιχου κρυπτογραφημένου κειμένου.*

Υποθέτουμε ότι ένας $n \times n$ πίνακας A χρησιμοποιείται για την κρυπτογράφηση, όπως περιγράφηκε προηγουμένως. Για να μπορέσουμε να ανακτήσουμε τον πίνακα A χωρίς να έχουμε γνώση του ιδιωτικού κλειδιού, θα χρειαστούμε n $\overline{m}^i$, όπου με $\overline{m}^i = (m_1^i,\ m_2^i,\ \ldots,\ m_n^i)$, $i = 1,\ \ldots,\ n$ θα συμβολίζουμε το διάνυσμα που αποτελείται από n χαρακτήρες και το μήνυμα έχει μετατραπεί στις αριθμητικές του τιμές, και επίσης θα χρειαστούμε n $\overline{c}^i$, όπου $\overline{c}^i = (c_1^i,\ c_2^i,\ \ldots,\ c_n^i)$ είναι n κρυπτογράφηση των $\overline{m}^i$. Για να βρούμε την i στήλη του πίνακα A, $A(i) = (a_{1,i},\ a_{2,i},\ \ldots,\ a_{n,i})$, θα πρέπει να λύσουμε τα ακόλουθα n-γραμμικά συστήματα, για $i = 1,\ \ldots,\ n$:

$$\begin{aligned} m_1^1 a_{1,i} + m_2^1 a_{2,i} + \cdots + m_n^1 a_{n,i} &= c_i^1 \\ m_1^2 a_{1,i} + m_2^2 a_{2,i} + \cdots + m_n^2 a_{n,i} &= c_i^2 \\ \vdots &\quad \vdots \\ m_1^n a_{1,i} + m_2^n a_{2,i} + \cdots + m_n^n a_{n,i} &= c_i^n \end{aligned}$$

ή ισοδύναμα συμβολίζουμε το προηγούμενο σύστημα ως

$$MA(i) = C(i)\ ,$$

όπου $C(i) = (c_i^1,\ c_i^2,\ \ldots,\ c_i^n)$.

Πρόταση 20 *Η ασφάλεια των* Hadamard Ciphers*, και των υποκατηγοριών τους* Hadamard Core Ciphers *και* Hadamard Cores Ciphers*, δεν παραβιάζεται από επιθέσεις γνωστού μηνύματος, υπό την προϋπόθεση ότι ο επιτιθέμενος έχει γνώση λιγότερων από n μηνυμάτων μήκους n του αρχικού κειμένου και του αντίστοιχου κρυπτογραφημένου κειμένου.*

Απόδειξη. Με τη μέθοδο που περιγράφηκε προηγουμένως, ο επιτιθέμενος μπορεί να βρει τον πίνακα κρυπτογράφησης A, αν ο πίνακας M είναι μη-ιδιάζων (αντιστρέψιμος). □

Κρυπτανάλυση Επιθέσεων Επιλεγμένου Μηνύματος για Κρυπτογραφήματα Hadamard

Ορισμός 32 *Μια επίθεση επιλεγμένου μηνύματος είναι εκείνη κατά την οποία ο επιτιθέμενος επιλέγει το αρχικό μήνυμα και στη συνέχεια του δίνεται το αντίστοιχο κρυπτογραφημένο κείμενο.*

Σε αυτόν τον τύπο της επίθεσης το επιπλέον πλεονέκτημα που έχει ο επιτιθέμενος είναι η γνώση του μηχανισμού κρυπτογράφησης. Όμως στην περίπτωση μας, αυτή η επιπλέον γνώση δεν αποκαλύπτει κάποια περαίτερω πληροφορία σε σχέση με μια επίθεση γνωστού μηνύματος, καθώς ο επιτιθέμενος για να σπάσει το κρυπτογράφημα πάλι έχει να λύσει n γραμμικά συστήματα,

$$MA(i) = C(i)$$

για $i = 1, \ldots, n$ όπως περιγράφεται στην Ενότητα 7.2.2.

Παρατήρηση 23 *Ο επιτιθέμενος θα πρέπει να λάβει υπόψιν ότι ο πίνακας* M *του επιλεγμένου μηνύματος πρέπει να είναι μη-ιδιάζων. Αυτή η παρατήρηση, περιορίζει την επιλογή των διαθέσιμων αρχικών κειμένων για τον επιτιθέμενο καθώς* $\overline{m}^i \neq \lambda \overline{m}^j$*, δηλαδή τα διανύσματα* $\overline{m}^i$ *πρέπει να είναι γραμμικά ανεξάρτητα.*

Πρόταση 21 *Η ασφάλεια των* Hadamard Ciphers*, και των υποκατηγοριών τους* Hadamard Core Ciphers *και* Hadamard Cores Ciphers*, δεν παραβιάζεται από επιθέσεις επιλεγμένου μηνύματος, καθώς αυτά τα κρυπτογραφήματα είναι ασφαλή ενάντια σε επιθέσεις γνωστού μηνύματος.*

§7.2.3 Κρυπτανάλυση Επιθέσεων Κρυπτογραφημένου Κειμένου για Κρυπτογραφήματα Hadamard

Σε αυτήν την ενότητα, παρουσιάζεται μια μελέτη κρυπτανάλυσης επιθέσεων κρυπτογραφημένου κειμένου για Κρυπτογραφήματα Hadamard. Συγκεκριμένα, αναλύονται μέθοδοι κρυπτανάλυσης της ανάλυσης συχνότητας (frequency analysis) των χαρακτήρων του κρυπτογραφημένου κειμένου καθώς και επιλεγμένου κρυπτογραφημένου κειμένου.

Κρυπτανάλυση της Ανάλυσης Συχνότητας για Κρυπτογραφήματα Hadamard

Ορισμός 33 *Η ανάλυση συχνότητας είναι μια επίθεση που αναφέρεται μόνον στο κρυπτογραφημένο κείμενο (ciphertext-only attack) και κατα την οποία ο επιτιθέμενος προσπαθεί να εξάγει το κλειδί αποκρυπτογράφησης ή το αρχικό μήνυμα με απλή παρατήρηση του κρυπτογραφημένου κειμένου. Οποιοδήποτε κρυπτογράφημα είναι ευάλωτο σε αυτό το τύπο επίθεσης θεωρείται εντελώς ανασφαλές.*

Δύο χαρακτήρες του αρχικού μηνύματος, m αντιστοιχούν σε διαφορετικές τιμές του κρυπτογραφημένου κειμένου, $\bar{c}$. Αναλύωντας το σενάριο χείριστης περιπτώσεως για αυτό τον τύπο επίθεσης, υποθέτουμε ότι όλοι οι χαρακτήρες του αρχικού μηνύματος είναι ίδιοι. Τότε στο αντίστοιχο κρυπτογραφημένο κείμενο όλες οι αριθμητικές τους τιμές θα είναι όλες διαφορετικές μεταξύ τους (λόγω της υφής του αλγορίθμου κρυπτογράφησης). Επομένως ο επιτιθέμενος δεν μπορεί να εξάγει οποιαδήποτε επιπλέον πληροφορία σχετική με το κλειδί κρυπτογράφησης ή το αρχικό μήνημα, καθώς οποιαδήποτε τιμή του κρυπτογραφημένου κειμένου είναι συνάρτηση n τιμών του αρχικού μηνύματος και μιας στήλης του πίνακα κρυπτογράφησης A. Συνεπώς, δύο ή περισσότερες ίδιες τιμές του κρυπτογραφημένου κειμένου δεν αναπαριστούν τον ίδιο χαρακτήρα στο αρχικό μήνυμα. Σημειώνουμε ότι, καθώς το n αυξάνει είναι περισσότερο δύσκολο για τον επιτιθέμενο να εξάγει το κλειδί κρυπτογράφησης ή το κρυπτογραφημένο κείμενο με απλή παρατήρηση.

Πρόταση 22 *Η ασφάλεια των* Hadamard Ciphers*, και των υποκατηγοριών τους* Hadamard Core Ciphers *και* Hadamard Cores Ciphers*, δεν παραβιάζεται από επιθέσεις που βασίζονται στην ανάλυση συχνότητας του κρυπτογραφημένου κειμένου.*

Κρυπτανάλυση Επιθέσεων Επιλεγμένου Κρυπτογραφημένου Κειμένου για Κρυπτογραφήματα Hadamard

Ορισμός 34 *Μια επίθεση επιλεγμένου κρυπτογραφημένου κειμένου είναι εκείνη κατά την οποία ο επιτιθέμενος επιλέγει το κρυπτογραφημένο κείμενο και στη συνέχεια του δίνεται το αντίστοιχο αρχικό μήνυμα. Ένας τρόπος να εκτελεστεί αυτή η επίθεση είναι ο επιτιθέμενος να έχει πρόσβαση στο εξοπλισμό που χρησιμοποιήθηκε για την αποκρυπτογράφηση (αλλά όχι και στο κλειδί αποκρυπτογράφησης). Ο στόχος της επίθεσης αυτής είναι ο επιτιθέμενος, χωρίς να έχει πρόσβαση σε τέτοιον εξοπλισμό, να εξάγει το αρχικό μήνυμα από (διαφορετικό) κρυπτογραφημένο κείμενο.*

Παρόμοια, και σε αυτόν τον τύπο επίθεσης το επιπλέον πλεονέκτημα του επιτιθέμενου να έχει γνώση του μηχανισμού αποκρυπτογράφησης, δεν του παρέχει επιπλέον πληροφόρηση σε σχέση με μια επίθεση γνωστού μηνύματος καθώς πάλι για να σπάσει το κρυπτογράφημα θα πρέπει να λύσει n γραμμικά συστήματα,

$$MA(i) = C(i)$$

για $i = 1, \ldots, n$ όπως περιγράφεται στην Ενότητα 7.2.2.

Πρόταση 23 *Η ασφάλεια των* Hadamard Ciphers*, και των υποκατηγοριών τους* Hadamard Core Ciphers *και* Hadamard Cores Ciphers*, δεν παραβιάζεται από επιθέσεις επιλεγμένου κρυπτογραφημένου κειμένου, καθώς αυτά τα κρυπτογραφήματα είναι ασφαλή ενάντια σε επιθέσεις γνωστού μηνύματος.*

§7.3 Κρυπτογραφική Σύνθεση Κρυπτογραφημάτων Hadamard

Σε αυτήν την ενότητα, εφαρμόζουμε τη μέθοδο κρυπτογραφικής σύνθεσης (product cryptosystems) για κρυπτογραφήματα Hadamard, που έχει ως κύριο χαρακτηριστικό της το γινόμενο Kronecker ορθογώνιων πινάκων. Αυτή η τεχνική κρυπτογραφικής σύνθεσης είναι αρκετά διαδεδομένη για κρυπτογραφικούς αλγορίθμους δέσμης στη σημερινή εποχή της σύγχρονης κρυπτογραφίας. Ενδεικτικά, αναφέρουμε ότι τα ευρέως γνωστά κρυπτογραφήματα Des, Aes, 3Des ανήκουν σε αυτήν την κατηγορία, [203].

Ενδιαφερομάστε ειδικότερα για το γινόμενο Kronecker πινάκων Hadamard (βλ. και όγδοο κεφάλαιο). Από το Θεώρημα 35, αν H_1 και H_2 είναι πίνακες Hadamard τάξεως m και n αντίστοιχα, τότε το αντίστοιχο γινόμενο Kronecker $H_1 \otimes H_2$ είναι ένας πίνακας Hadamard τάξεως mn.

Παρατήρηση 24 *Μπορούμε να επαναλάβουμε την προηγούμενη κατασκευή χρησιμοποιώντας* p *πίνακες Hadamard* $H_1, H_2, \ldots, H_p$ *τάξεων* $n_1, n_2, \ldots, n_p$*. Τότε το γινόμενο Kronecker των* $\bigotimes_{i=1}^{p} H_i := H_1 \otimes H_2 \otimes \ldots \otimes H_p$ *είναι ένας πίνακας Hadamard τάξης* $\prod_{i=1}^{p} n_i$.

Ο στόχος μας είναι η βελτίωση των κενών ασφαλείας των κρυπτογραφημάτων που παρουσιάστηκαν στις προηγούμενες ενότητες έτσι ωστε να είναι εντελώς ασφαλή ενάντια σε επιθέσεις γνωστού μηνύματος, επιθέσεις επιλεγμένου μηνύματος και επιλεγμένου κρυπτογραφημένου κειμένου (κάνοντας χρήση του γινομένου Kronecker). Παρουσιάζουμε την μέθοδο κρυπτογραφικής σύνθεσης για τους Hadamard Core Ciphers και Hadamard Cores Ciphers, που έχει ως αποτέλεσμα κρυπτογραφήματα που θα καλούμε Kronecker Hadamard Core Ciphers και Kronecker Hadamard Cores Ciphers, αντίστοιχα.

Παράδειγμα 31 (Kronecker Hadamard Core Ciphers) Έστω H_i, για $i = 1, \ldots, k$ να είναι πίνακες Hadamard με έναν κυκλικό πυρήνα τάξεων $n_i = p_i + 1$, για $i = 1, \ldots, k$ αντίστοιχα. Συσχετίζοντας αυτούς τους πίνακες με τα αντίστοιχα κλειδιά κρυπτογράφησης $A_{c_i} = [a_{1_i}, a_{2_i}, \ldots, a_{p_i}]$ για $i = 1, \ldots, k$ όπου το κάθε ιδιωτικό κλειδί A_{c_i} αποτελείται από p_i bits, σχηματίζουμε μια k-οικογένεια κρυπτογραφικών σχημάτων. Αν θεωρήσουμε το γινόμενο Kronecker $\bigotimes_{i=1}^{k} H_i$ αυτών των πινάκων, ο παραγόμενος πίνακας είναι ένας πίνακας τάξης $\prod_{i=1}^{k} n_i$. Καθώς ο παραλήπτης μπορεί να κατασκευάσει τον κάθε πίνακα Hadamard H_i από τα αντίστοιχα ιδιωτικά κλειδιά A_{c_i}, ο πίνακας που παράγεται από το γινόμενο Kronecker μπορεί να χρησιμοποιηθεί ως πίνακας κρυπτογράφησης όπου το ιδιωτικό του κλειδί $\bigoplus_{i=1}^{k} A_{c_i}$ είναι η παράθεση των ιδιωτικών κλειδιών A_{c_i}, και αποτελείται από $\sum_{i=1}^{k} p_i$ bits. Ας συμβολίσουμε με n τη μεγαλύτερη τάξη των πινάκων Hadamard που χρησιμοποιήσαμε, δηλαδή $n = \max_i\{n_i\}$. Με όρους υπολογιστικής πολυπλοκότητας, καθώς $\prod_{i=1}^{k} n_i \leq \prod_{i=1}^{k} n = n^k$, n τάξη μεγέθους του πίνακα κρυπτογράφησης, $\mathcal{O}(n^k)$ αυξάνει εκθετικά. Όμως, το μέγεθος του ιδιωτικού κλειδιού αυξάνει γραμμικά καθώς $\sum_{i=1}^{k} p_i = \sum_{i=1}^{k} (n_i - 1) = \sum_{i=1}^{k} (n_i) - k \leq \sum_{i=1}^{k} (n) - k = kn - k = k(n-1)$, συνεπώς n τάξη μεγέθους του είναι $\mathcal{O}(n)$.

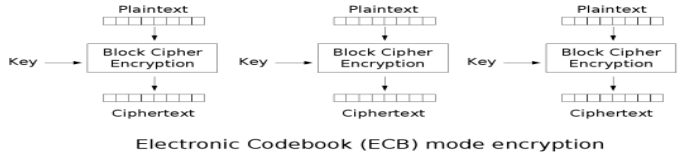
Παράδειγμα 32 (Kronecker Hadamard Cores Ciphers) Έστω H_i, για $i = 1, \ldots, k$ να είναι πίνακες Hadamard με δύο κυκλικούς πυρήνες τάξεων $n_i = 2\ell_i + 2$, για $i = 1, \ldots, k$ αντίστοιχα. Συσχετίζοντας αυτούς τους πίνακες με τα αντίστοιχα κλειδιά κρυπτογράφησης $A_{c_i} \oplus B_{c_i} = [a_{1_i}, a_{2_i}, \ldots, a_{\ell_i}] \oplus [b_{1_i}, b_{2_i}, \ldots, b_{\ell_i}] = [a_{1_i}, a_{2_i}, \ldots, a_{\ell_i}, b_{1_i}, b_{2_i}, \ldots, b_{\ell_i}]$ για $i = 1, \ldots, k$ όπου το κάθε ιδιωτικό κλειδί $A_{c_i} \oplus B_{\ell_i}$ αποτελείται από $2\ell_i$ bits, σχηματίζουμε μια k-οικογένεια κρυπτογραφικών σχημάτων. Αν θεωρήσουμε το γινόμενο Kronecker $\bigotimes_{i=1}^{k} H_i$ αυτών των πινάκων, ο παραγόμενος πίνακας είναι ένας πίνακας τάξης $\prod_{i=1}^{k} n_i$. Καθώς ο παραλήπτης μπορεί να κατασκευάσει τον κάθε πίνακα Hadamard H_i από τα αντίστοιχα ιδιωτικά κλειδιά $A_{c_i} \oplus B_{c_i}$, ο πίνακας που παράγεται από το γινόμενο Kronecker μπορεί να χρησιμοποιηθεί ως πίνακας κρυπτογράφησης όπου το ιδιωτικό του κλειδί $\bigoplus_{i=1}^{k}(A_{c_i} \oplus B_{c_i})$ είναι η παράθεση των ιδιωτικών κλειδιών $A_{c_i} \oplus B_{c_i}$, και αποτελείται από $\sum_{i=1}^{k} 2\ell_i = 2k \sum_{i=1}^{k} \ell_i$ bits. Ας συμβολίσουμε με n τη μεγαλύτερη τάξη των πινάκων Hadamard που χρησιμοποιήσαμε, δηλαδή $n = \max_i\{n_i\}$. Με όρους υπολογιστικής πολυπλοκότητας, καθώς $\prod_{i=1}^{k} n_i \leq \prod_{i=1}^{k} n = n^k$, n τάξη μεγέθους του πίνακα κρυπτογράφησης, $\mathcal{O}(n^k)$ αυξάνει εκθετικά. Όμως, το μέγεθος του ιδιωτικού κλειδιού αυξάνει γραμμικά καθώς $\sum_{i=1}^{k} 2\ell_i = \sum_{i=1}^{k}(n_i - 2) = \sum_{i=1}^{k}(n_i) - 2k \leq \sum_{i=1}^{k}(n) - 2k = nk - 2k = k(n-2)$, συνεπώς n τάξη μεγέθους του είναι $\mathcal{O}(n)$.

Σε κάθε περίπτωση, με τη μέθοδο της κρυπτογραφικής σύνθεσης επιτυγχάνουμε μια "έκρηξη" στο μέγεθος του πίνακα κρυπτογράφησης ενώ ταυτόχρονα διατηρούμε το μέγεθος του κλειδιού σε λογικά μήκη. Ένας από τους στόχους μας ήταν να κάνουμε μια γραμμική κρυπτανάλυση (linear cryptanalysis) των σχημάτων, υπολογιστικά ανέφικτη. Αυτή πραγματοποιείται με τη επίλυση ενός γραμμικού συστήματος, συνεπώς γίνεται χρήση της απαλοιφής Gauss, έτσι ώστε ο επιτιθέμενος να πραγματοποιήσει επιτυχημένες επιθέσεις γνωστού μηνύματος, επιλεγμένου μηνύματος και επιλεγμένου κρυπτογραφημένου κειμένου, όπως είδαμε από την κρυπτανάλυση που παρουσιάστηκε στην Ενότητα 7.2.2.

Πρόταση 24 *Η ασφάλεια των* Kronecker Hadamard Core Ciphers *και* Kronecker Hadamard Cores Ciphers, *δεν παραβιάζεται από επιθέσεις γνωστού μηνύματος, επιθέσεις επιλεγμένου μηνύματος και επιλεγμένου κρυπτογραφημένου κειμένου, καθώς μια γραμμική κρυπτάναλυση αυτών των κρυπτογραφημάτων είναι υπολογιστικά ανέφικτη.*

§7.3.1 Η ECB Μέθοδος Κρυπτογράφησης

Πλεόν μπορούμε να περιγράψουμε ένα κενό ασφαλείας στο σχεδιασμό των απλών Hadamard Ciphers που σε ορισμένες περιπτώσεις μπορεί να εξαλειφθεί κάνοντας χρήση της προηγούμενης μεθόδου κρυπτογραφικής σύνθεσης. Όπως έχουμε ήδη αναφέρει, στις περιπτώσεις που το αρχικό μήνυμα έχει περισσότερους από n χαρακτήρες, επαναλαμβάνουμε τη μέθοδο κρυπτογράφησης. Αυτή η μέθοδος κρυπτογράφησης είναι επίσης γνωστή ως *electronic codebook mode*, ή απλούστερα ECB στη βιβλιογραφία ([49, 178, 184, 221]). Ένα μειονέκτημα αυτής της μεθόδου είναι ότι αν δύο τμήματα του αρχικού μηνύματος είναι ίδια, τότε και τα αντίστοιχα τμήματα του κρυπτογραφημένου μηνύματος θα είναι ταυτόσημα, και αυτό θα είναι ορατό στον επιτιθέμενο.
Η κρυπτογραφική σύνθεση των κρυπτογραφημάτων Hadamard μπορεί να ελαχιστοποιήσι το πόσο πληροφορίας που μπορεί να ανακτήσει ο επιτιθέμενος όταν χρησιμοποιούμε την ECB μέθοδο κρυπτογράφησης περιορίζοντας τις διαθέσιμες επιλογές για πίνακες Hadamard A_i, $i = 1, \ldots, k$ να είναι $A_f \neq A_g$ για $i \leq f, g \leq k$ με $f \neq g$. Γενικότερα, αν επιλέξουμε A_i πίνακες κρυπτογράφησης τάξεων n_i όπου $\sum_{i=1}^{k} n_i = n$, και n είναι το μέγεθος του αρχικού μηνύματος, αυτό το κενό ασφαλείας εξαλείφεται τελείως καθώς κατά τη διαδικασία κρυπτογράφησης δεν προκύπτουν επαναλαμβανόμενα τμήματα.



Σχήμα 7.1: Η ECB μέθοδος κρυπτογράφησης

§7.4 Συμμετρικά Κρυπτοσυστήματα από Σχηματισμούς Plotkin

Σε αυτήν την ενότητα, προτείνουμε κρυπτοσυστήματα ιδιωτικού κλειδιού τα οποία προέρχονται από σχηματισμούς Plotkin (Plotkin arrays).

§7.4.1 Προδιαγραφές

Είχαμε ως κίνητρο να χρησιμοποιήσουμε τους σχηματισμούς Plotkin ως ενδιάμεσο στάδιο κατασκευής δυαδικών σχηματισμών για τον σχεδιασμό των κρυπτογραφικών σχημάτων αυτής της ενότητας, καθώς αυτοί είναι μέρος της ευρύτερης κλάσης των συνδυαστικών σχεδιασμών και η μαθηματική τους δομή επιτρέπει την υλοποίηση αποδοτικών κρυπτογραφικών αλγορίθμων.

Το προτεινόμενο κρυπτογράφημα έχει ομοιότητες με το κρυπτογράφημα του Hill, δηλαδή την χρησιμοποίηση του πίνακα πρόσπτωσης για κρυπτογράφηση και αποκρυπτογράφηση, και το One Time Pad. Για περαιτέρω λεπτομέρειες σχετικά με τη μέθοδο κρυπτογράφησης του Hill και το One Time Pad, βλ. [219] και [184]. Μια εκτενής αναφορά σε επιθέσεις που αναφέρονται σε κρυπτοσυστήματα, και περιγραφή των πιο σημαντικών κρυπτογραφικών πρωτοκόλλων μπορεί να βρεθεί στις [49] και [18], αντίστοιχα. Οι προδιαγραφές, με βάση τις οποίες σχεδιάσαμε τα κρυπτογραφικά σχήματα από σχηματισμούς Plotkin επεκτείνουν εκείνες των κρυπτογραφημάτων Hadamard, καθώς μια από αυτές είναι να προσεγγίσουμε το One Time Pad. Ιδιαίτερα, οι προδιαγραφές των κρυπτογραφημάτων Plotkin είναι οι ακόλουθες.

Ερευνητικό Πρόβλημα 9 *Ο σχεδιασμός κρυπτοσυστημάτων ιδιωτικού κλειδιού από συνδυαστικές δομές όπου,*

1. *Η διαδικασία κρυπτογράφησης διέπεται από τυχαιότητα*
2. *Το συμμετρικό κλειδί (κρυπτογράφησης και αποκρυπτογράφησης) μοιράζεται μόνον μια φορά*
3. *Το μέγεθος του κλειδιού είναι σχετικά μικρό*
4. *Οι αντίστοιχοι κρυπτογραφικοί αλγόριθοι είναι υπολογιστικά γρήγοροι*
5. *Δεν παραβιάζεται η ασφάλεια των κρυπτοσυστημάτων από επιθέσεις εξαντλητικών υπολογισμών*

Η υλοποίηση των κρυπτογραφικών σχημάτων αυτής της ενότητας κάνει χρήση των πρώτων τεσσάρων προδιαγραφών. Σκοπός αυτής της ενότητας είναι να δείξουμε ότι η ασφάλεια των κρυπτογραφημάτων Plotkin δεν παραβιάζεται από επιθέσεις εξαντλητικών υπολογισμών. Επιπλέον, τα κρυπτογραφήματα Plotkin μπορούν να θεωρηθούν και ως η γενίκευση εκείνων που παρουσιάστηκαν στην [106, 150].

§7.4.2 Κρυπτογραφικά Σχήματα από Σχηματισμούς Plotkin

Ενδιαφερόμαστε για την κατασκευή κρυπτογραφικών σχημάτων χρησιμοποιώντας ορθογώνιους πίνακες. Αυτή η διαδικασία επιτυγχάνεται χρησιμοποιώντας ορθογώνιους σχεδιασμούς, εν προκειμένω μιας κλάσης αυτών, που μας επιτρέπουν να παράγουμε μεγάλους ορθογώνιους πίνακες.

Το κρυπτογράφημα μπορεί να περιγραφεί από την ακόλουθη διαδικασία: Θεωρούμε ένα δίαυλο επικοινωνίας, με δύο κανάλια εξόδου, ένα το οποίο θα μεταφέρει το μήνυμα και το άλλο το οποίο θα μεταφέρει θόρυβο. Το μήνυμα, μαζί με το θόρυβο θα μεταδοθεί μέσω αυτού του καναλιού. Ο παραλήπτης τότε φιλτράρει το θόρυβο και αυτό που απομένει είναι το αρχικό μήνυμα.
Σημειώνουμε ότι, μια επίθεση σε ένα κρυπτοσύστημα θεωρείται επιτυχημένη αν παραβιάζει κάποια από τις προδιαγράφες σχεδίασης του.

Παρατήρηση 25 *Εφόσον συμπεριλάβαμε στις προδιαγραφές του κρυπτογραφικού σχήματος, το κρυπτογράφημα να είναι ασφαλές ενάντια σε επιθέσεις εξαντλητικών υπολογισμών, ένας ορισμός παραβίασης της ασφάλειας του κρυπτοσυστήματος είναι είτε να βρεθεί μια μέθοδος πιο αποδοτική από την επίθεση εξαντλητικού υπολογισμού, είτε αυτός ο τύπος επίθεσης να μπορεί να αναπαραγάγει το αρχικό κείμενο που χρησιμοποιήθηκε για την παραγωγή ενός κρυπτογραφημένου κειμένου σε λογικό υπολογιστικό χρόνο.*

Υπενθυμίζουμε τον ορισμό ενός ορθογωνίου σχεδιασμού.

Ορισμός 35 *Ένας ορθογώνιος σχεδιασμός τάξης* n *και τύπου* $(s_1, s_2, \ldots, s_k)$ *στις μεταθετικές μεταβλητές* $x_1, x_2, \ldots, x_k$ *που συμβολίζεται με* $\mathrm{OD}(n; s_1, s_2, \ldots, s_k)$*, είναι ένας τετραγωνικός πίνακας τάξης* n *με στοιχεία από το σύνολο* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ *που ικανοποιεί τη σχέση*

$$DD^T = \sum_{i=1}^{k} (s_i x_i^2) I_n,$$

όπου I_n *είναι ο ταυτοτικός πίνακας τάξης* n*.*

Οι ορθογώνιοι σχεδιασμοί έχουν χρησιμοποιηθεί εκτεταμένα στη Συνδυαστική, τη Στατιστική, τη Θεωριά κωδίκων και σε διάφορες άλλες περιοχές. Περαιτέρω λεπτομέρειες για ορθογώνιους σχεδιασμούς μπορούν να βρεθούν στις [70, 206, 208]. Ένας ορθογώνιος σχεδιασμός έχει τις ακόλουθες ιδιότητες:

1. Σε κάθε γραμμή του σχεδιασμού υπάρχουν s_1 στοιχεία $\pm x_1$, s_2 στοιχεία $\pm x_2$, ..., s_k στοιχεία $\pm x_k$, και αντίστοιχα το ίδιο ισχύει για τις στήλες.

2. Οι γραμμές και οι στήλες του σχεδιασμού είναι αμοιβαία ορθογώνιες.

Η επιλογή των ορθογώνιων σχεδιασμών για την κατασκευή ορθογώνιων πινάκων και μετέπειτα κρυπτογραφικών σχημάτων μας επιτρέπει να επιλέξουμε από μια μεγάλη ποικιλία κλάσεων ορθογώνιων σχεδιασμών με διαφορετική δομή. Ο Plotkin στην [196] έδειξε ότι, αν υπάρχει ένας πίνακας Hadamard τάξης $2t$, τότε υπάρχει ένας $\mathrm{OD}(8t; t, t, t, t, t, t, t, t)$. Αποτελεί ανοιχτό πρόβλημα στη Θεωρία σχεδιασμών, η ύπαρξη $\mathrm{OD}(8n; n, n, n, n, n, n, n, n)$ για κάθε περιττό n. Αυτοί οι ορθογώνιοι σχεδιασμοί, καλούνται σχηματισμοί Plotkin.

Κρυπτογραφικά Σχήματα Plotkin Ξεκινάμε την κατασκευή των κρυπτογραφικών σχημάτων βασιζόμενοι στους σχηματισμούς Plotkin, που θα καλούμε PLOTKIN CIPHERS. Δίνουμε ως παράδειγμα την κατασκευή του σχηματισμού Plotkin τάξης 8 και τύπου $(1,1,1,1,1,1,1,1)$. Ο αντίστοιχος ορθογώνιος σχεδιασμός δίνεται παρακάτω:

$$\mathrm{OD}(8;1,1,1,1,1,1,1,1) = \begin{pmatrix} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{pmatrix}, \tag{7.1}$$

Εάν συμβολίσουμε τον προηγούμενο πίνακα P, έχουμε οτι $PP^T = fI_8$ όπου $f = A^2 + B^2 + \ldots + H^2$. Οι σχηματισμοί Plotkin επιτρέπουν την εύκολη κατασκευή των πινάκων που χρειαζόμαστε στην κατασκευή των κρυπτογραφικών σχημάτων. Για την διαδικασία κρυπτογράφησης έχουμε μόνο να υπολογίσουμε τον πίνακα P. Η διαδικασία κρυπτογράφησης έχει ως είσοδο ένα μήνυμα m αυθαίρετου μήκους, το οποίο m χωρίζουμε σε τμήματα $m_1, \ldots, m_q$ μήκους 4 (παραθέτοντας στο τελευταιό τμήμα μηδενικά εάν είναι απαραίτητο). Στη συνέχεια, επιλέγονται τυχαία διανύσματα $g_1, \ldots, g_q$ μήκους 4. Για την κατασκευή των διανυσμάτων θορύβου $g_1, \ldots, g_q$ χρησιμοποιούνται ψευδοτυχαίες γεννήτριες (pseudorandom generators) [174]. Τελικά, ο πίνακας P εφαρμόζεται διαδοχικά στα $m_i \oplus g_i$. Τότε, το κρυπτογραφημένο κείμενο είναι $c = P(m_1 \oplus g_1) \oplus \ldots \oplus P(m_q \oplus g_q)$.
Το μήνυμα αποκρυπτογραφείται αν χωρίσουμε το c σε τμήματα $c_1, \ldots, c_q$ μήκους 8, υπολογίζοντας το $fP^T c_i$ για $i = 1, \ldots, q$ ανακατασκευάζοντας έτσι το μήνυμα χρησιμοποιώντας τις τέσσερις πρώτες εισόδους αυτών των τμημάτων.

Παρατήρηση 26 *Το ιδιωτικό κλειδί για τον παραλήπτη είναι οι επιλεγμένες είσοδοι του P, συνεπώς σε αυτή την περίπτωση είναι οι είσοδοι $A, B, \ldots, H$ του πίνακα P.*

Αφού οι σχηματισμοί Plotkin που χρησιμοποιήσαμε μέχρι τώρα είναι σχετικά μικροί, θα συνεχίσουμε τροποποιώντας κατάλληλα την διαδικασία κρυπτογράφησης χρησιμοποιώντας τους σχηματισμούς Plotkin

τάξεων 16 και 24. Σημειώνουμε οτι η χρήση σχηματισμών Plotkin διαφόρων τάξεων δεν έχει ως αποτέλεσμα την αύξηση του χώρου κλειδιών, καθώς ο αριθμός των μεταβλητών που εμφανίζονται σε αυτούς τους σχεδιασμούς παραμένει ο ίδιος. Πειραματικά αποτελέσματα των παραπάνω υπολογισμών θα δοθούν στην επόμενη ενότητα. Οι προηγούμενοι σχηματισμοί μπορούν να βρεθουν στην [70].

Κρυπτογραφική Σύνθεση Κρυπτογραφημάτων Plotkin Αν και οι σχηματισμοί Plotkin υπάρχουν και για μεγαλύτερες τάξεις, θα κάνουμε χρήση της μεθόδου της κρυπτογραφικής σύνθεσης μέσω του γινομένου Kronecker για σχηματισμούς Plotkin, έτσι ώστε να προσθέσουμε επιπλέον επίπεδα ασφαλείας κατά τη διαδικασία κρυπτογράφησης. Αυτού του είδους τα κρυπτογραφήματα, θα καλούνται Kronecker Plotkin Ciphers.

Για τη διαδικασία κρυπτογράφησης επιλέγουμε p σχηματισμούς Plotkin $P_1, P_2, \ldots, P_p$. Κάθε σχηματισμός μπορεί να έχει διαφορετικό μέγεθος, έστω $e_i \times e_i$ για $1 \leq i \leq p$ όπου το e_i μπορεί να είναι $8, 16$ ή 24. Έπειτα, κατασκευάζουμε τον πίνακα M τάξης $e_1 e_2 \ldots e_p$ από το γινόμενο Kronecker αυτών των p πινάκων:

$$M = \bigotimes P_i := P_1 \otimes P_2 \otimes \ldots \otimes P_p.$$

Το κρυπτογραφημένο κείμενο τότε είναι το $c = M(m \oplus g)$. Με αυτή την κατασκευή εξαλείφουμε κάθε πιθανή αραιή δομή των μηδενικών στον πίνακα κρυπτογράφησης M. Σημειώνουμε οτι το κλειδί σε αυτή την περίπτωση είναι οι είσοδοι των πρώτων γραμμών των P_1 εώς P_p, συνεπώς είναι μια λίστα αριθμών μεγέθους $e_1 + e_2 + \ldots + e_p$ και έτσι είναι σχετικά μικρή. Ο συμβολισμός $m \oplus g$ σημαίνει ότι στο m παραθέτουμε το g.

Η ECB Μέθοδος Κρυπτογράφησης Πλεόν μπορούμε να περιγράψουμε ένα κενό ασφαλείας στο σχεδιασμό των απλών Plotkin Ciphers που σε ορισμένες περιπτώσεις μπορεί να εξαλειφθεί κάνοντας χρήση της προηγούμενης μεθόδου κρυπτογραφικής σύνθεσης. Όπως έχουμε ήδη αναφέρει, στις περιπτώσεις που το αρχικό μήνυμα m έχει περισσότερους από n χαρακτήρες, επαναλαμβάνουμε τη μέθοδο κρυπτογράφησης. Αυτή η μέθοδος κρυπτογράφησης, όπως ήδη αναφέραμε σε προηγούμενη ενότητα, είναι γνωστή ως *electronic codebook mode*, ή απλούστερα ECB στη βιβλιογραφία ([49, 178, 184, 221]) και ένα μειονέκτημα αυτής είναι ότι αν δύο τμήματα του αρχικού μηνύματος είναι ίδια,

τότε και τα αντίστοιχα τμήματα του κρυπτογραφημένου μηνύματος θα είναι ταυτόσημα, και αυτό θα είναι ορατό στον επιτιθέμενο.
Η κρυπτογραφική σύνθεση των κρυπτογραφημάτων Plotkin μπορεί να ελαχιστοποιήσι το πόσο πληροφορίας που μπορεί να ανακτήσει ο επιτιθέμενος όταν χρησιμοποιούμε την ECB μέθοδο κρυπτογράφησης περιορίζοντας τις διαθέσιμες επιλογές για σχηματισμούς Plotkin P_i, $i = 1, \ldots, p$ να είναι $P_f \neq P_g$ για $i \leq f, g \leq p$ με $f \neq g$. Γενικότερα, αν επιλέξουμε P_i πίνακες κρυπτογράφησης τάξεων n_i όπου $\sum_{i=1}^{k} n_i = n$, και n είναι το μέγεθος του αρχικού μηνύματος, αυτό το κενό ασφαλείας εξαλείφεται τελείως καθώς κατά τη διαδικασία κρυπτογράφησης δεν προκύπτουν επαναλαμβανόμενα τμήματα.

§7.4.3 Υλοποίηση Κρυπτογραφικών Αλγορίθμων

Σε αυτήν την ενότητα, δίνουμε μια σύντομη παρουσίαση των αλγορίθμων που χρησιμοποιήσαμε για την κρυπτογράφηση, αποκρυπτογράφηση και ανάλυση των αποτελέσματων σε μορφή ψευδοκώδικα. Ο αλγόριθμος που αναπτύξαμε για την διαδικασία κρυπτογράφησης υλοποιείται στην EncoderFunction. Η HackerFunction είναι μια προσομοίωση επιθέσης εξαντλητικού υπολογισμού για τους Plotkin Ciphers και Kronecker Plotkin Ciphers. Για να εφαρμόσουμε ανάλυση συχνότητας στο κρυπτογραφημένο κείμενο υλοποιήσαμε την AnalyzerFunction. Η υλοποίηση των προηγούμενων αλγορίθμων πραγματοποιήθηκε στην γλώσσα προγραμματισμού C. Ορισμένες προγραμματιστικές τεχνικές που αφορούν κρυπτογραφικούς αλγορίθμους μπορούν να βρεθούν στην [203].

Algorithm 22 AnalyzerScheme Function

function AnalyzerScheme(Receives the output from the HackerFunction and calculates the frequency of occurence of every ASCII symbol)

Step. 1 For each line of text, count number of appearances of each ASCII value.

Step. 2 Output information to text file.

end function

Algorithm 23 EncoderScheme Function

function EncoderScheme(Encodes a sample plaintext)

Step 1. Compute the encryption matrix M

Step 1a. Convert the corresponding characters of the plaintext to ASCII values.

Step 1b. Input the possible range of entries for the matrices P_i.

Step 1c. Choose the corresponding Plotkin arrays that will form the matrices P_i.

Step 1d. Compute the tensor product $M := P_1 \otimes P_2 \otimes \ldots \otimes P_p$.

Step 2. Encode the input message

Step 2a. Compute $m \oplus g$ by converting the message to ASCII values and filling the noise vector g with random numbers.

Step 2b. Compute $M(m \oplus g)$

end function

Algorithm 24 HACKERSCHEME FUNCTION

function HACKERSCHEME(Simulation of a brute force attack method to a ciphertext)

Step 1. Input min, max and range of key guesses.

Step 2. Input ciphertext.

Step 3. Exhaustive key search with respect to Step 1.

For all possible values of the variables of the orthogonal designs chosen for encryption perform the following steps.

Step 3a. Generate the matrices using as entries the possible values from previous step.

Step 3b. Compute the tensor product of the matrices created in previous step.

Step 3c. Calculate possible text messages.

Step 3d. Output text to file for later examination.

end function

§7.5 Πειραματικά Αποτελέσματα και Μέθοδοι Κρυπτανάλυσης για Κρυπτογραφήματα Plotkin

Εκτελέσαμε ορισμένα αριθμητικά πειράματα για τα δυο κρυπτογραφικά σχήματα που παρουσιάστηκαν στην προηγούμενη ενότητα, τους PLOTKIN CIPHERS και KRONECKER PLOTKIN CIPHERS. Τα πειραματικά αποτελέσματα που θα παρουσιαστούν σε αυτή την ενότητα αφορούν προσομοιώσεις επιθέσεων εξαντλητικών υπολογισμών. Επίσης, δίνεται και μια μέθοδος κρυπτανάλυσης επιθέσεων γνωστού μηνύματος για αυτά τα κρυπτογραφήματα στο τέλος της ενότητας.

§7.5.1 Προσομοίωση Επιθέσεων Εξαντλητικών Υπολογισμών για Plotkin Ciphers

Για να εκτελέσουμε μια επίθεση εξαντλητικού υπολογισμού στους Plotkin Ciphers, ακολουθήσαμε τα παρακάτω βήματα σε κάθε προσομοίωση.

1. Χρησιμοποιήσαμε ένα αρχικό κειμένο 384 χαρακτήρων και ένα τυχαίο διάνυσμα θορύβου ίδιου μήκους.
2. Θεωρήσαμε τα στοιχεία των $A, B, \ldots, H$ ως δυαδικές μεταβλητές.
3. Αποκωδικοποιήσαμε το κρυπτογραφημένο κείμενο χρησιμοποιώντας κάθε δυνατό συνδυασμό κλειδιού, όπου τα στοιχεία του κλειδιού είχαν τιμές ίσες με ± 1.

Από τα πειραματικά αποτελέσματα που λάβαμε από τις προσομοιώσεις, πήραμε τις ακόλουθες πληροφορίες:

1. Για τους σχηματισμούς Plotkin $\mathrm{OD}(8t; t, t, t, t, t, t, t, t)$ για $t = 1, 2, 3$ μια επίθεση εξαντλητικού υπολογισμού είχε ως αποτέλεσμα την πλήρη παραβίαση της ασφάλειας του κρυπτογραφήματος. Αναφέρουμε όμως, ότι ο υπολογιστικός χρόνος αυξάνεται με μη-γραμμικό τρόπο.
2. Αφού αυτό το κρυπτογραφικό σχήμα δεν είναι ασφαλές ενάντια σε επιθέσεις εξαντλητικού υπολογισμού, έχουμε μια πλήρης παραβίαση των προδιαγραφών που θέσαμε για αυτό το κρυπτογράφημα.

Ο ακόλουθος πίνακας παρουσιάζει τα υπολογιστικά αποτελέσματα για τις προσομοιώσεις που εκτελέσαμε. Για κάθε ορθογώνιο σχεδιασμό δίνουμε το μέγεθος του χώρου κλειδιών και τον υπολογιστικό χρόνο που χρειάστηκε μια επίθεση εξαντλητικού υπολογισμού να σπάσει το κρυπτογράφημα.

§7.5.2 Προσομοίωση Επιθέσεων Εξαντλητικών Υπολογισμών για Kronecker Plotkin Ciphers

Για να εκτελέσουμε μια επίθεση εξαντλητικού υπολογισμού στους Kronecker Plotkin Ciphers, ακολουθήσαμε τα παρακάτω βήματα σε κάθε προσομοίωση.

Σχεδιασμός	Χώρος Κλειδιών	Υπολογιστικός Χρόνος
$\mathrm{OD}(8;1,1,1,1,1,1,1,1)$	2^8	4 ώρες
$\mathrm{OD}(16;2,2,2,2,2,2,2,2)$	2^8	12 ώρες
$\mathrm{OD}(24;3,3,3,3,3,3,3,3)$	2^8	34 ώρες

Πίνακας 7.3: Πειραματικά αποτελέσματα επιθέσεων εξαντλητικών υπολογισμών γις Plotkin Ciphers

1. Χρησιμοποιήσαμε ένα αρχικό κειμένο 23 χαρακτήρων.
2. Κρυπτογραφήσαμε το αρχικό κείμενο χρησιμοποιώντας το κρυπτογραφικό σχήμα Plotkin που έχει παραχθεί με τη μέθοδο της κρυπτογραφικής σύνθεσης, προσεγγίζοντας το μέγεθος των εισόδων για τους σχηματισμούς Plotkin και προσεγγίζοντας το μέγεθος του διανύσματος θορύβου g.
3. Χρησιμοποιήσαμε τους σχηματισμούς Plotkin τάξης 8 για να υπολογίσουμε τον πίνακα κρυπτογράφησης M.
4. Αποκρυπτογραφήσαμε το κρυπτογραφημένο κείμενο χρησιμοποιώντας κάθε δυνατό συνδυασμό κλειδιού, όπου τα στοιχεία του κλειδιού είχαν τιμές ίσες με ± 1.
5. Μετατρέψαμε το αποκρυπτογραφημένο κείμενο που βρήκαμε στο προηγούμενο βήμα σε τιμές ASCII.
6. Μετρήσαμε την συχνότητα της κάθε τιμής που εμφανίστηκε στους δυνατούς συνδυασμούς.

Από τα πειραματικά αποτελέσματα που λάβαμε από τις προσομοιώσεις, πήραμε τις ακόλουθες πληροφορίες:

1. Μια επίθεση εξαντλητικού υπολογισμού δεν είναι ένας εφικτός τρόπος παραβίασης της ασφάλειας του κρυπτογραφήματος.
2. Ένα πλεονέκτημα του One Time Pad είναι οτι μια επίθεση εξαντλητικού υπολογισμού καταλήγει στην αποκρυπτογράφηση όλων των αρχικών μηνυμάτων, αναγκάζοντας έτσι τον κρυπταναλυτή να διαλέξει πιο απο αυτά ήταν το αρχικό μήνυμα. Σκοπός μας ήταν να καθορίσουμε αν αυτη η περίπτωση ήταν αληθής και για το δικό μας κρυπτογράφημα. Τα υπολογιστικά αποτελέσματα υποδεικνύουν ότι η απάντηση είναι αρνητική.

3. Τέλος θέλαμε να καθορίσουμε αν το μέγεθος των στοιχείων του διανύσματος θορύβου g διαδραμάτισε σημαντικό ρόλο στην διαδικασία αποκρυπτογράφησης. Τα υπολογιστικά αποτελέσματα έδειξαν οτι η απάντηση σε αυτό το ερώτημα ήταν θετική.

4. Και οι πέντε προδιαγραφές που είχαμε θέσει κατά τον σχεδιασμό αυτού του κρυπτογραφήματος, ικανοποιούνται.

Ο ακόλουθος πίνακας παρουσιάζει τα υπολογιστικά αποτελέσματα για τις προσομοιώσεις που εκτελέσαμε. Για κάθε προσομοίωση μια επίθεσης εξαντλητικού υπολογισμού δίνουμε των αριθμό εμφανίσεων των τιμών ASCII στο αντίστοιχο διάστημα τους και τις προσεγγίσεις των μεγεθών του κλειδιού και του διανύσματος θορύβου. Ο πίνακας δείχνει οτι οι περισσότεροι χαρακτήρες που εμφανίζονται στην προσομοίωση της επίθεσης είναι εκείνοι που είχαν κωδικοποιηθεί χρησιμοποιώντας το αρχικό κείμενο.

Μέγεθος Κλειδιού	Μέγεθος Θορύβου	Εμφανίσεις τιμών ASCII $\times 10^5$				
		$0-25$	$26-50$	$51-75$	$76-100$	$101-127$
10-14	128	25	5	5	7	8
10-14	1024	10	12	8	6	14
30-34	128	120	30	40	30	50
30-34	1024	65	90	45	50	40
50-54	128	310	50	70	30	40
50-54	1024	110	100	90	80	120

Πίνακας 7.4: Πειραματικά αποτελέσματα επιθέσεων εξαντλητικών υπολογισμών για Kronecker Plotkin Ciphers

§7.5.3 Κρυπτανάλυση Επιθέσεων Γνωστού Μηνύματος για Κρυπτογραφήματα Plotkin

Η μέθοδος κρυπτανάλυσης επιθέσεων γνωστού μηνύματος για κρυπτογραφήματα Plotkin, είναι παρόμοια με εκείνη που δόθηκε για τα κρυπτογραφήματα Hadamard.

Υποθέτουμε ότι ένας $n \times n$ πίνακας P έχει χρησιμοποιηθεί για την κρυπτογράφηση, όπως αυτός περιγράφεται στο σχεδισμό των PLOTKIN CIPHERS. Για να μπορέσουμε να ανακτήσουμε τον πίνακα P χωρίς να έχουμε γνώση του ιδιωτικού κλειδιού, θα χρειαστούμε n $\overline{m}^i$, όπου με $\overline{m}^i = (m_1^i,\ m_2^i,\ \ldots,\ m_n^i),\ \ i = 1,\ \ldots,\ n$ θα συμβολίζουμε το διάνυσμα που αποτελείται από n χαρακτήρες του αρχικού κειμένου και έχει μετατραπεί στις αντίστοιχες αριθμητικές του τιμές, και n $\overline{c}^i$, όπου κάθε $\overline{c}^i = (c_1^i,\ c_2^i,\ \ldots,\ c_n^i)$ είναι n κρυπτογράφηση των $\overline{m}^i$. Για να ανακτήσουμε την i στήλη του P, $P(i) = (p_{1,i},\ p_{2,i},\ \ldots,\ p_{n,i})$, θα πρέπει να λύσουμε τα ακόλουθα n-γραμμικά συστήματα, για $i = 1, \ldots, n$:

$$\begin{aligned} m_1^1 p_{1,i} + m_2^1 p_{2,i} + \cdots + m_n^1 p_{n,i} &= c_i^1 \\ m_1^2 p_{1,i} + m_2^2 p_{2,i} + \cdots + m_n^2 p_{n,i} &= c_i^2 \\ \vdots \qquad\qquad &\quad \vdots \\ m_1^n p_{1,i} + m_2^n p_{2,i} + \cdots + m_n^n p_{n,i} &= c_i^n \end{aligned}$$

ή ισοδύναμα συμβολίζουμε το προηγούμενο σύστημα με

$$MP(i) = C(i)\ ,$$

όπου $C(i) = (c_i^1,\ c_i^2,\ \ldots,\ c_i^n)$.

Πρόταση 25 *Η ασφάλεια των* PLOTKIN CIPHERS*, δεν παραβιάζεται από επιθέσεις γνωστού μηνύματος, υπό την προϋπόθεση ότι ο επιτιθέμενος έχει γνώση λιγότερων από* n *μηνυμάτων μήκους* n *του αρχικού κειμένου και του αντίστοιχου κρυπτογραφημένου κειμένου.*

Απόδειξη. Με τη μέθοδο που περιγράφηκε προηγουμένως, ο επιτιθέμενος μπορεί να βρει τον πίνακα κρυπτογράφησης P, αν ο πίνακας M είναι μη-ιδιάζων (αντιστρέψιμος). □

Secrets are things
we give to others
to keep for us.

Elbert Hubbard (1856-1915)

8

Κρυπτογραφικά Σχήματα Διαμοιρασμού Μυστικού Μηνύματος

Στο όγδοο αυτό κεφάλαιο, παρουσιάζονται ορισμένες μέθοδοι παραγωγής νέων (κρυπτογραφικών) σχημάτων διαμοιρασμού μυστικού μηνύματος (secret-sharing schemes) από πίνακες Hadamard οι οποίοι προκύπτουν από ορθογώνιους 3-σχεδιασμούς. Επίσης, εδραιώνεται μια αντιστοιχία μεταξύ Hadamard σχεδιασμών και κρυπτογραφικών σχημάτων διαμοιρασμού μυστικού μηνύματος. Στη συνέχεια, περιγράφουμε ορισμένες από τις πιο γνωστά υποσχόμενες μεθόδους κατασκευής πινάκων Hadamard, παρέχοντας με αυτόν τον τρόπο τις απαραίτητες δομές για να περιγράψουμε ένα κρυπτογραφικό σχήμα διαμοιρασμού μυστικού μηνύματος με δυο μέρη το οποίο βασίζεται σε σχεδιασμούς Hadamard. Επιπρόσθετα, επιδεικνύουμε πως ορισμένες αλγεβρικές ιδιότητες της Κρυπτογραφίας σχημάτων διαμοιρασμού μυστικού μηνύματος αντιστοιχούν σε όρους της Συνδυαστικής Θεωρίας Σχεδιασμών, όπως για παράδειγμα η δομή πρόσβασης και η ασφάλεια των κρυπτογραφικών σχημάτων.

Τα ερευνητικά αποτελέσματα αυτού του κεφαλαίου δημοσιεύθηκαν στην επιστημονική εργασία [165].

§8.1 Στοιχεία Θεωρίας Σχεδιασμών και Κρυπτογραφικών Σχημάτων

Σε αυτήν την εισαγωγική ενότητα, θα αναπτύξουμε τα απαραίτητα εργαλεία που χρησιμοποιήσαμε απο το χώρο της Θεωρίας σχεδιασμών για την κατασκευή των κρυπτογραφικών σχημάτων διαμοιρασμού μυστικού μηνύματος. Ιδιαίτερα, θα παρουσιάσουμε τους Hadamard 3-σχεδιασμούς και την εύρεση αυτών μέσω γνωστών μεθόδων κατασκευής πινάκων Hadamard, καθώς και θα αναπτύξουμε το κίνητρο το οποίο είχαμε να ασχοληθούμε με κρυπτογραφικά σχήματα της προηγούμενης μορφής.

Ερευνητικό Πρόβλημα 10 *Η κατασκευή διμερών κρυπτογραφικών σχημάτων διαμοιρασμού από συνδυαστικούς σχεδιασμούς που έχουν καλές ιδιότητες.*

§8.1.1 Hadamard 3-Σχεδιασμοί

Ένας $t-(v,k,\lambda)$ **σχεδιασμός** είναι ένα ζεύγος $(\mathcal{P},\mathcal{B})$ όπου $\mathcal{P}$ είναι ένα σύνολο από v στοιχεία, που καλούνται σημεία, και $\mathcal{B}$ είναι μια συλλογή από διακεκριμένα υποσύνολα του $\mathcal{P}$ μεγέθους k, τα οποία καλούνται blocks, τέτοια ώστε κάθε υποσύνολο των σημείων μεγέθους t να περιέχεται σε λ ακριβώς blocks. Κάθε $t-(v,k,\lambda)$ σχεδιασμός είναι επίσης ένας $s-(v,k,\lambda_s)$ σχεδιασμός για $s \leq t$, όπου $\lambda_s = \frac{(v-s)}{(k-s)}\lambda_{s+1}$ και $\lambda_t = \lambda$. Επιπλέον, αν $(\mathcal{P},\mathcal{B})$ είναι ένας $t-(v,k,\lambda)$ σχεδιασμός τότε $(\mathcal{P}\{x\}, \mathrm{DER}_x(\mathcal{B}))$ είναι ένας $(t-1)-(v-1,k-1,\lambda)$ σχεδιασμός, που καλείται ο παραγόμενος σχεδιασμός για $(\mathcal{P},\mathcal{B})$, όπου $x \in \mathcal{P}$ και $\mathrm{DER}_x(\mathcal{B}) = \{B\{x\} : x \in B \in \mathcal{B}\}$ [5].

Κάθε 3-σχεδιασμός με $v = 4m$, $k = 2m$, και $\lambda = m-1$, καλείται Hadamard 3-σχεδιασμός, λόγω της στενής σχέσης του με τους πίνακες Hadamard, όπως θα εξηγήσουμε παρακάτω. Επιπλέον, αν $\mathcal{D}$ είναι ένας Hadamard 3-σχεδιασμός, τότε κάθενας από τους παραγόμενους σχεδιασμούς, $\mathcal{D}_P$, που προκύπτει παραλείπτοντας ένα σημείο P και όλα τα blocks τα οποία δεν προσπίπτουν στο P, είναι συμμετρικός. Οι $\mathcal{D}_P$ και $\overline{\mathcal{D}}_P$, θα καλούνται Hadamard 2-σχεδιασμοί. Οι παράμετροί τους είναι,

αντίστοιχα, $(4m-1, 2m-1, m-1)$ και $(4m-1, 2m, m)$. Για περισσότερες λεπτομέρειες παραπέμπουμε στις [32] και [5].

Έστω H ένας πίνακας Hadamard τάξεως $4m$ και $r = (r_1, r_2, ..., r_{4m})$ να είναι μια οποιαδήποτε γραμμή του H. Τότε για οποιαδήποτε άλλη γραμμή s του H, το $l_s = \{j | s_j = r_j\}$ είναι ένα $2m$-υποσύνολο του $\mathcal{P} = \{1, 2, ..., 4m\}$, και το ίδιο είναι αληθές για $l_s = \mathcal{P} - l_s = \{j | s_j \neq r_j\}$. Είναι αρκετά γνωστό και στοιχειώδες κάποιος να αποδείξει (βλ. [115]) ότι η συλλογή

$$\mathcal{B}(H(r)) = \{l_s | s \neq r\} \cup \{\bar{l}_s | s \neq r\} \qquad (8.1)$$

σχηματίζει το σύνολο των block ενός Hadamard 3-σχεδιασμού. Για να πάρουμε έναν 2-σχεδιασμό, επιλέγουμε ένα σημείο j, και διατηρούμε το block l_s αν $j \in l_s$, και το $\bar{l}_s$ αν $j \notin l_s$.

§8.1.2 Κρυπτογραφικά Σχήματα Διαμοιρασμού

Τα υπολογιστικά συστήματα απαιτούν εξεζητημένη ασφάλεια, η οποία διασφαλίζεται καλύτερα όταν το κλειδί ή ο κωδικός πρόσβασης μοιράζεται ανάμεσα σε αρκετά άτομα με τέτοιον τρόπο έτσι ώστε να μπορεί να ανακατασκευαστεί από έναν αρκετά μεγάλο αριθμό ομάδων που φτάνει σε συμφωνία. Ασφάλεια τέτοιας μορφής χρησιμοποιείται σε τράπεζες και σε παρόμοιους οικονομικούς οργανισμούς, σε δίκτυα τηλεποικωνίας και σε υπολογιστικά συστήματα πανεπιστημίων, αν και η καλύτερα γνωστή εφαρμογή της είναι σε στρατιωτικές εφαρμογές. Για παράδειγμα, στην ενεργοποίηση πυρηνικών κεφαλών, μια ομάδα από ανώτερους αξιωματικούς πρέπει να έλθει σε συμφωνία πρίν ο απαιτούμενος κωδικός να είναι σε θέση να ανακατασκευαστεί.

Ένα **κρυπτογραφικό σχήμα διαμοιρασμού μυστικού μηνύματος** ή απλούστερα κρυπτογραφικό σχήμα διαμοιρασμού, είναι ένας τρόπος να μοιραστεί ένα μυστικό ανάμεσα σε ένα πεπερασμένο σύνολο από ανθρώπους ή οντότητες τέτοιος ώστε μόνον ορισμένα διακεκριμένα υποσύνολα αυτών να έχουν πρόσβαση στο μυστικό. Η συλλογή Γ όλων των διακεκριμένων υποσυνόλων καλείται η **δομή πρόσβασης** του σχήματος. Ένα τέλειο κρυπτογραφικό σχήμα διαμοιρασμού μυστικού μηνύματος για την συλλογή Γ είναι μια μέθοδος με την οποία τα μερίδια (shares), που αποτελούν το μυστικό, διανέμονται σε ομάδες τέτοιες ώστε:

1. κάθε υποσύνολο της Γ να μπορεί να ανακατασκευάσει το μυστικό από τα αντίστοιχα μερίδια του, και

2. κάθε υποσύνολο που δεν ανήκει στην Γ να μην μπορεί να αποκαλύψει οποιαδήποτε πληροφορία ή μέρος του μυστικού (με την έννοια της Θεωρία πληροφοριών).

Τα κρυπτογραφικά σχήματα διαμοιρασμού εισήχθησαν για πρώτη φορά από τους Blakley [10] και Shamir [213] για την οριακή (threshold) περίπτωση, δηλαδή για την περίπτωση όπου τα υποσύνολα που μπορούν να ανακατασκευάσουν το μυστικό είναι όλα εκείνα τα σύνολα που η πληθικότητα τους φράσσεται από κάποιο όριο. Σε αυτό το κεφάλαιο, θα θεωρήσουμε κάποιες ειδικές ιδιότητες των πινάκων Hadamard που διαδραματίζουν καθοριστικό ρόλο στην μελέτη μας όταν απαριθμούμε τις δομές πρόσβασης των σχημάτων με βάση το μέγεθος τους.

§8.1.3 Κατασκευές Πινάκων Hadamard

Υπάρχει ένας μεγάλος αριθμός κατασκευών για πίνακες Hadamard, ο οποίος μπορεί να ταξινομηθεί σε τρεις κατηγορίες:

- πολλαπλασιαστικά (αναδρομικά) θεωρήματα
- άμεσες κατασκευές
- "plug-in" μεθόδους

Μια καλή επισκόπηση του θέματος παρουσιάζεται στην [208]. Οι κατασκευές που δίνουμε σε αυτήν την ενότητα με κανένα τρόπο δεν εξαντλούν τις ήδη υπάρχουσες, αλλά επαρκούν για την κατασκευή ενός πίνακα Hadamard για κάθε επιτρεπτή τάξη μικρότερη ή ίση του 100.

Πίνακες Hadamard που παράγονται μέσω του Γινομένου Kronecker Τα θεμέλια των περισσότερων πολλαπλασιαστικών μεθόδων είναι το γινόμενο Kronecker δυο πινάκων. Συγκεκριμένα, αν $A = (a_{ij})$ είναι ένας $m \times p$ πίνακας και $B = (b_{ij})$ είναι ένας $n \times q$ πίνακας, τότε το

γινόμενο Kronecker $A \otimes B$ είναι ένας $mn \times pq$ πίνακας

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1p}B \\ a_{21}B & a_{22}B & \dots & a_{2p}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \vdots & a_{mp}B \end{bmatrix}.$$

Ο Jacques Hadamard απέδειξε το ακόλουθο τανυστικό (που επίσης καλείται Kronecker) γινόμενο για τους εν λόγω πίνακες.

Θεώρημα 35 (Hadamard [97]) *Αν* H_1 *και* H_2 *είναι πίνακες Hadamard τάξεως* m *και* n *αντίστοιχα, τότε το αντίστοιχο γινόμενο Kronecker* $H_1 \otimes H_2$ *είναι ένας πίνακας Hadamard τάξεως* mn*.*

Η πρώτη μεγάλη οικογένεια πινάκων Hadamard παρόλα αυτά ανακαλύφθηκε από τον Sylvester στην πρωτοποριακή του εργασία [222] για όλες τις τάξεις 2^k, $k \geq 1$. Εφαρμόζοντας την κατασκευή που βασίζεται στο γινόμενο Kronecker, τα αποτελέσματα του μπορούν να περιγραφούν θέτοντας $S_1 = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$ ως το γίνόμενο Kronecker $S_1 \otimes H(n)$.

Λήμμα 20 (Sylvester [222]) *Οι πίνακες Sylvester Hadamard, είναι οι πίνακες της οικογένειας* $\{S_k = \otimes^k S_1 : k \geq 1\}$*.*

Πίνακες Hadamard Τύπου Paley Ακόμη μια μεγάλη οικογένεια πινάκων Hadamard είναι οι λεγόμενοι *πίνακες Hadamard τύπου Paley*. Αυτές οι οικογένειες των πινάκων Hadamard βρέθηκαν από την άμεση κατασκευή του Paley [191] χρησιμοποιώντας τα τετραγωνικά υπόλοιπα (δηλαδή, τα μη-μηδενικά τέλεια τετράγωνα) σε ένα πεπερασμένο σώμα $GF(q)$ περιττής τάξης. Στο σώμα $GF(q)$, τα μισά μη-μηδενικά στοιχεία είναι τετραγωνικά υπόλοιπα τετραγώνων και τα υπόλοιπα μισά είναι μη-τετραγωνικά υπόλοιπα των μη-τετραγώνων. Ιδιαίτερα, το $+1$ είναι τετράγωνο και το -1 είναι ένα μη-τετράγωνο μόνο αν $q \equiv 3 \pmod 4$.

Ο τετραγωνικός χαρακτήρας του $GF(q)$ είναι η συνάρτηση χ που δίνεται από

$$\chi(x) = \begin{cases} 0 & \text{αν } x = 0, \\ +1 & \text{αν } x \text{ είναι ένα τετραγωνικό υπόλοιπο,} \\ -1 & \text{αν } x \text{ είναι ένα μη-τετραγωνικό υπόλοιπο.} \end{cases}$$

Θεώρημα 36 (Paley [191]) *Για* q *μια περιττή δύναμη πρώτου, και μια διάταξη* $\{g_0 = 0, g_1, \ldots, g_{q-1}\}$ *του* $\mathrm{GF}(q)$*, θέτουμε* $Q = [\chi(g_i - g_j)]_{0 \le i,j < q}$ *και* $S = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{1}^\mathsf{T} & Q \end{bmatrix}$*, όπου με* $\mathbf{1}$ *συμβολίζουμε το διάνυσμα μονάδων μήκους* q*.*

1. *(Πίνακας Hadamard τύπου Paley I) Αν* $q \equiv 3 \pmod 4$ *τότε ο*

$$P_q = \begin{bmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^\mathsf{T} & Q + I_q \end{bmatrix}$$

   είναι ένας πίνακαςHadamard τάξεως $(q+1)$*.*

2. *(Πίνακας Hadamard τύπου Paley II) Αν* $q \equiv 1 \pmod 4$ *τότε ο*

$$P'_q = \begin{bmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{bmatrix}$$

   είναι ένας πίνακας Hadamard τάξεως $2(q+1)$*.*

Παρατήρηση 27 *Οι πίνακες Hadamard τύπου Paley I τάξεως* $q+1$ *είναι στενά συνδεδεμένοι με τους* $2-(q, \frac{q-1}{2}, \frac{q-3}{4})$ *σχεδιασμούς. Για παράδειγμα, αν κανονικοποιήσουμε τον* P_q*, ο παραγόμενος σχεδιασμός μπορεί να περιγραφεί ως ακολούθως: το σύνολο σημείων είναι το* $\mathrm{GF}(q)$*, ένα block είναι το σύνολο* J *των μη-τετραγωνικών υπολοίπων του* $\mathrm{GF}(q)$*, και τα υπόλοιπα είναι τα σύμπλοκα* $J + x = \{j + x : j \in J\}$ *για* $x \in \mathrm{GF}(q)$*. Όπως αναφέραμε νωρίτερα, αυτοί οι σχεδιασμοί καλούνται Hadamard 2-σχεδιασμοί.*

Πίνακες Hadamard παραγόμενοι από Κυκλικούς Υποπίνακες Στη συνέχεια, δίνουμε μια μέθοδο που χρησιμοποιεί "plug-in" πίνακες σε έναν κατάλληλο σχηματισμό, και η οποία δόθηκε πρώτα από τον Yang [236].

Θεώρημα 37 (Yang [236]) *Αν* A *και* B *είναι* $n \times n$ *κυκλικοί πίνακες με στοιχεία* ± 1 *που ικανοποιούν την σχέση:*

$$AA^\mathsf{T} + BB^\mathsf{T} = 2nI_n \tag{8.2}$$

τότε ο πίνακας $H = \begin{bmatrix} A & B \\ -B^\mathsf{T} & A^\mathsf{T} \end{bmatrix}$ *είναι ένας πίνακας Hadamard τάξεως* $2n$*.*

Για να βρούμε κατάλληλους υποπίνακες που ικανοποιούν την προσθετική ιδιότητα της σχέσης (8.2), χρησιμοποιούμε ένα σημαντικό αποτέλεσμα που προέρχεται από τις ακολουθίες με μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης (NPAF), όπως περιγράφεται στην [153] και στο πρώτο μέρος της διατριβής.

Παρατήρηση 28 *Αν υπάρχουν δύο ακολουθίες* A *και* B *μήκους* n *με στοιχεία* $\{\pm 1\}$ *και μηδενική μη-περιοδική συνάρτηση αυτοσυσχέτισης, τότε αυτές οι ακολουθίες μπορούν να χρησιμοποιηθούν ως οι πρώτες γραμμές των κυκλικών πινάκων που κάνει χρήση ο σχηματισμός του Yang για να σχηματίσουν έναν πίνακα Hadamard τάξεως* $2n$.

Οι ακολουθίες Golay ([71, 72]), $GS(n)$ μήκους n, πληρούν τις προϋποθέσεις της Παρατήρησης (28) όπως έχουμε ήδη περιγράψει στο πρώτο μέρος της διατριβής. Υπενθυμίζουμε ότι, οι $GS(n)$ υπάρχουν για $n = 2^a \cdot 10^b \cdot 26^c$ όπου a, b, c είναι μη-αρνητικοί ακέραιοι. Άπειρα μήκη ακολουθιών Golay μπορούν να παραχθούν μέσω μιας αναδρομικής κατασκευής που οφείλεται στον Turyn [229]. Συνεπώς, μια άπειρη οικογένεια πινάκων Hadamard μπορεί να παραχθεί από ακολουθίες Golay (μέσω του Θεωρήματος 37 και της Παρατήρησης 28). Ιδιαίτερα, υπάρχει n ακόλουθη οικογένεια: $\{H(2n)$ είναι ένας πίνακας Hadamard τάξεως $2n : n = 2^a \cdot 10^b \cdot 26^c$, a, b, c μη-μηδενικοί ακέραιοι τέτοιοι ώστε οι $GS(n)$ να υπάρχουν$\}$.

Πίνακες Hadamard παραγόμενοι από άλλες Πολλαπλασιαστικές Μεθόδους Όπως ήδη είδαμε στο δεύτερο κεφάλαιο αυτής της διατριβής, μια αρκετά παραγωγική μέθοδος κατασκευής πινάκων Hadamard χρησιμοποιεί T-πίνακες ή T-ακολουθίες. Αυτή η μέθοδος έχει ως κύρια χαρακτηριστικά της, τις βασικές ακολουθιές και τους αριθμούς Yang. Για περισσότερες πληροφορίες πάνω σε αυτές τις πολλαπλασιαστικές μεθόδους για T-ακολουθίες παραπέμπουμε στις [122, 143].

Σε αυτήν την ενότητα, παραθέτουμε για λόγους πληρότητας μόνον το θεώρημα κατασκευής πινάκων Hadamard τάξεως $4t$ από T-ακολουθίες μήκους t, στη μορφή που το χρησιμοποιήσαμε σαν ενδιάμεσο στάδιο στην παραγωγή των κρυπτογραφικών σχημάτων διαμοιρασμού.

Θεώρημα 38 (Cooper και Wallis [29]) *Υποθέτουμε ότι υπάρχουν κυκλικοί* T*-πίνακες (ή ισοδύναμα* T*-ακολουθίες)* T_i, $i = 1, \ldots, 4$ *τάξεως* n. *Τότε οι πίνακες,*

$$\begin{aligned} A &= T_1 + T_2 + T_3 + T_4 \\ B &= -T_1 + T_2 + T_3 - T_4 \\ C &= -T_1 - T_2 + T_3 + T_4 \\ D &= -T_1 + T_2 - T_3 + T_4 \end{aligned}$$

μπορούν να χρησιμοποιηθούν στο σχηματισμό Goethals-Seidel (βλ. [70, σελ. 107]), για να παράγουν έναν πίνακα Hadamard τάξεως $4n$.

Λίστα Πινάκων Hadamard τάξεων μέχρι 100 Στον ακόλουθο πίνακα δίνουμε μια λίστα από πίνακες Hadamard τάξεων μέχρι το 100, χρησιμοποιώντας μόνο τις μεθόδους κατασκευής που δώσαμε προηγουμένως. Συνεπώς, αυτοί οι πίνακες Hadamard κατασκευάζονται με σχετική ευκολία και κατα συνέπεια μπορούν να παρέσχουν άμεσα τα κρυπτογραφικά σχήματα που παρουσιάζουμε σε αυτό το κεφάλαιο. Για μεγαλύτερες τάξεις παραπέμπουμε στους αντίστοιχους πίνακες των [140] και [142]. Σημειώνουμε ότι, για κάθε επιτρεπτή τάξη ενός πίνακα Hadamard, $H(n)$, μπορεί να υπάρχουν διαθέσιμες περισσότερες από μια κατασκευές. Αναφέρουμε μόνο μια από αυτές για κάθε περίπτωση.

Τάξη	Οικογένεια	Κατασκευή	Τάξη	Οικογένεια	Κατασκευή
4	Sylvester	Λήμμα 20	8	Υπάρχουν GS(4)	Θεώρημα 37
12	Paley τύπου I	Θεώρημα 36	16	Υπάρχουν GS(8)	Θεώρημα 37
20	Υπάρχουν GS(10)	Θεώρημα 37	24	Paley τύπου I	Θεώρημα 36
28	Paley τύπου II	Θεώρημα 36	32	Sylvester	Λήμμα 20
36	Paley τύπου II	Θεώρημα 36	40	Υπάρχουν GS(20)	Θεώρημα 37
44	Υπάρχουν TS(11)	Θεώρημα 38	48	Paley τύπου I	Θεώρημα 36
52	Υπάρχουν GS(26)	Θεώρημα 37	56	$H(2) \otimes H(28)$	Θεώρημα 35
60	Paley τύπου II	Θεώρημα 36	64	Sylvester	Λήμμα 20
68	Paley τύπου I	Θεώρημα 36	72	Paley τύπου I	Θεώρημα 36
76	Paley τύπου II	Θεώρημα 36	80	$H(4) \otimes H(20)$	Θεώρημα 35
84	Paley τύπου II	Θεώρημα 36	88	$H(2) \otimes H(44)$	Θεώρημα 35
92	Υπάρχουν TS(23)	Θεώρημα 38	96	$H(2) \otimes H(48)$	Θεώρημα 35
100	Υπάρχουν TS(25)	Θεώρημα 38			

Πίνακας 8.1: Μέθοδοι Κατασκευής για $H(n)$, $4 \leq n \leq 100$

§8.2 Hadamard 3-Σχεδιασμοί και Κρυπτογραφικά Σχήματα Διαμοιρασμού

Σε αυτό το κεφάλαιο, όπως ήδη είδαμε, μελετούμε τους πίνακες Hadamard τάξεως $n = 4m$ και τους αντίστοιχους 3-σχεδιασμούς τους. Στη συνέχεια τους χρησιμοποιούμε για να περιγράψουμε ένα κρυπτογραφικό σχήμα διαμοιρασμού με δυο μέρη, το οποίο βασίζεται σε Hadamard 3-σχεδιασμούς.

§8.2.1 Κρυπτογραφικά Σχήματα από Γραμμικούς Κώδικες

Οι Dougherty, Mesnager και Solé πρότειναν το ακόλουθο κρυπτογραφικό σχήμα διαμοιρασμού μυστικού μηνύματος [45]. Το μυστικό αποτελείται από στοιχεία του F_q και μοιράζεται σε μερίδια. Έστω $s \in F_q$ το μυστικό το οποίο επιθυμούμε να μοιράσουμε, και έστω G ο γεννήτορας πίνακας ενός κώδικα C μήκους n με στήλες $G_0, G_1, \ldots, G_{n-1}$. Έστω z ένα διάνυσμα πληροφορίας τέτοιο ώστε $zG_0 = s$, και $u = zG$. Η αντίστοιχη συντεταγμένη u_i, $i = 1, 2, \ldots, n-1$, ανατίθεται σε κάθε ομάδα. Υποθέτουμε ότι, G_0 είναι ο γραμμικός συνδυασμός των $n-1$ στηλών $G_1, \ldots, G_{n-1}$. Το μυστικό s τότε καθορίζεται από το σύνολο των μεριδίων $\{u_{i_1}, u_{i_2}, \ldots, u_{i_m}\}$, αν και μόνον αν ο G_0 είναι γραμμικός συνδυασμός των $G_0 = \sum_{j=1}^{m} x_j G_{i_j}$, όπου $1 \leq i_1 < \cdots < i_m \leq n-1$ και $m \leq n-1$.
Συνεπώς, επιλύοντας αυτή τη γραμμική εξίσωση βρίσκουμε τα x_j και στη συνέχεια το μυστικό από την σχέση, $s = zG_0 = \sum_{j=1}^{m} x_j zG_{i_j} = \sum_{j=1}^{m} x_j u_{i_j}$. Το σύνολο των m μεριδίων $\{u_{i_1}, u_{i_2}, \ldots, u_{i_m}\}$ καθορίζει το μυστικό αν και μόνον αν υπάρχει μια κωδικολέξη $(1, 0, ..., 0, c_{i_1}, 0, ..., 0, c_{i_m}, 0.., 0) \in C^{\perp}$, όπου $c_{i_j} \neq 0$ για τουλάχιστον ένα j [45] (βλ. επίσης [182] για την περιγραφή αυτής της τεχνικής). Έστω $\mathcal{P}$ το σύνολο των ομάδων που συμμετέχουν στο διαμοιρασμό του μυστικού. Σε αυτή την περίπτωση $\mathcal{P}$ είναι το σύνολο των συντεταγμένων εκτός της πρώτης. Το σύνολο Γ, καλείται όπως είπαμε στην αρχή του κεφαλαίου η **δομή πρόσβασης** του κρυπτογραφικού σχήματος διαμοιρασμού, και αποτελείται από υποσύνολα του $\mathcal{P}$ τέτοια ώστε κάθε στοιχείο του Γ να μπορεί να

αποκαλύψει το μυστικό.

Στην [16] παρουσιάστηκε το ακόλουθο κρυπτογραφικό σχήμα διαμοιρασμού: Έστω ότι οι κωδικολέξεις βάρους i δοσμένου δυαδικού αυτοδϋικού $[n, n/2]$ κώδικα C σχηματίζουν ένα $3-(\nu, k, \lambda)$ σχεδιασμό D_i, όπου $\nu = n$ και $k = i$ (οι κωδικολέξεις βάρους i είναι τα blocks του D_i). Για το πρώτο μέρος του μυστικού n κατανομή των μεριδίων είναι n ίδια όπως με το προηγούμενο κρυπτογραφικό σχήμα. Για το δεύτερο μέρος του μυστικού θα πρέπει να αφαιρέσουμε τους δυο πρώτους συμμετέχοντες, έτσι ώστε να παραμείνουν μονο $n-3$ συμμετέχοντες σε αυτό το μέρος. Το δεύτερο μέρος του μυστικού είναι $s' = s + zG_1 + zG_2 = z(G_0 + G_1 + G_2)$. Τότε το s' μπορεί να καθοριστεί από το σύνολο των μεριδίων $\{u_{i_3}, u_{i_4}, \ldots, u_{i_m}\}$, αν και μόνον αν $G_2 = G_0 + G_1 + \sum_{j=3}^{m} x_j G_{i_j}$ όπου $3 \leq i_3 < \cdots < i_m \leq n-1$ και $m \leq n-1$. Συνεπώς το s' μπορεί να καθοριστεί από το σύνολο των μεριδίων $\{u_{i_3}, u_{i_4}, \ldots, u_{i_m}\}$, αν και μόνον αν υπάρχει μια κωδικολέξη $x \in C$ με $supp(x) = \{1, 2, 3, i_3, \ldots, i_m\}$.

Εν συντομία, η ιδέα αυτού του διμερούς κρυπτογραφικού σχήματος διαμοιρασμού είναι η ακόλουθη. Υπάρχουν δυο πόρτες (η μια μετά την άλλη) και n χρήστες (κάθε χρήστης έχει ένα μέρος του κλειδιού) και μικρότερες ομάδες χρηστών μπορούν να ξεκλειδώσουν την *εσωτερική* πόρτα συνδυάζοντας τα δικά τους μερίδια του κλειδιού. Ακριβώς μετά από αυτή τη φάση, μεγαλύτερες ομάδες χρηστών μπορούν να συνδυάσουν τα αντίστοιχα μερίδια τους (που είναι και αυτά μέρος του κλειδιού) έτσι ώστε να μπορούν να ξεκλειδώσουν την *εξωτερική* πόρτα.

§8.2.2 Νέα Κρυπτογραφικά Σχήματα Διαμοιρασμού

Σε αυτήν την ενότητα προτείνουμε το ακόλουθο νέο κρυπτογραφικό σχήμα διαμοιρασμού: Έστω $H(4m)$ ένας πίνακας Hadamard τάξεως $4m$ με όλα τα στοιχεία της πρώτης γραμμής να είναι ίσα με 1. Με βάση αυτόν τον πίνακα, κατασκευάζουμε έναν Hadamard $3-(4m, 2m, m-1)$ σχεδιασμό $\mathcal{D}$, ο οποίος διέπεται από μια ιδιότητα ορθογωνιότητας. Το κρυπτογραφικό σχήμα βασίζεται στη δομή του σχεδιασμού και την ορθογωνιότητα δυο οποιονδήποτε γραμμών.

Για το πρώτο μέρος του μυστικού s, η δομή πρόσβασης του κρυπτογραφικού σχήματος διαμοιρασμού δίνεται από την

$$\Gamma = \{A \mid A \text{ είναι το στήριγμα ενός block του } B \in \mathcal{B} \text{ with } B_0 = 1\}. \quad (8.3)$$

Θεωρούμε τα block που έχουν 1 στην πρώτη θέση. Είναι εύκολο να υπολογίσουμε ότι υπάρχουν $\frac{(v-1)(v-2)}{(k-1)(k-2)}\lambda$ τέτοια block όπου $v = 4m, k = 2m$, και $\lambda = m-1$ (τότε $\frac{(v-1)(v-2)}{(k-1)(k-2)}\lambda = 4m-1$). Αυτά τα block χωρίς το πρώτο σημείο σχηματίζουν έναν $2-(v-1, k-1, \lambda)$ σχεδιασμό $\mathcal{D}'$.

Για το δεύτερο μέρος, θεωρούμε $\frac{v-2}{k-2}\lambda$ $(= 2m-1)$ block του $\mathcal{D}'$ που έχουν 1 στην πρώτη θέση. Αυτά τα block χωρίς το πρώτο σημείο σχηματίζουν έναν $1-(v-2, k-2, \lambda)$ σχεδιασμό $\mathcal{D}''$. Συνεπώς, για το δεύτερο μέρος του μυστικού, η δομή πρόσβασης αποτελείται από λ ομάδες μεγέθους $k-3$.

Για να αποκαλυφθεί το διμερές μυστικό θα πρέπει αρχικά να χρησιμοποιήσουμε τις ομάδες που έχουν μέγεθος $k-3$. Αυτές μπορούν να αποκαλύψουν το δεύτερο μέρος του μυστικού. Στη συνέχεια, για να αποκαλυφθεί και το πρώτο μέρος του μυστικού χρησιμοποιούμε αυτές τις ομάδες (οι οποίες είναι ήδη μεγέθους $k-2$) και τις υπόλοιπες $\frac{v-2}{k-2}\lambda - \lambda = \frac{v-k}{k-2}\lambda$ ομάδες μεγέθους $k-2$. Προσθέτουμε ένα νέο συμμετέχοντα του οποίου η αντίστοιχη δομή πρόσβασης έχει μονάδες σε αυτές τις ομάδες μεγέθους $k-2$ (οι υπόλοιπες τιμές είναι 0). Στη τελευταία φάση, χρησιμοποιούμε τις παραγόμενες $\frac{v-2}{k-2}\lambda$ ομάδες μεγέθους $k-1$, και τις υπόλοιπες $\frac{(v-1)(v-2)}{(k-1)(k-2)}\lambda - \frac{v-2}{k-2}\lambda = \frac{(v-k)(v-2)}{(k-1)(k-2)}\lambda$ ομάδες ίδιου μεγέθους για να αποκαλύψουμε τελικά το πρώτο μέρος του μυστικού. Συνοπτικά, έχουμε την ακόλουθη νέα κατασκευή κρυπτογραφικού σχήματος διαμοιρασμού:

Θεώρημα 39 *Έστω* $H(4m)$ *ένας πίνακας Hadamard τάξεως* $4m$ *σε κανονική μορφή (όλα τα στοιχεία της πρώτης του γραμμής είναι μονάδες). Τότε υπάρχει ένα κρυπτογραφικό σχήμα διαμοιρασμού μυστικού μηνύματος με δύο μέρη, το οποίο παράγεται από έναν Hadamard* $3-(4m, 2m, m-1)$ *σχεδιασμό με την ακόλουθη δομή πρόσβασης:*

(i) $4m-1$ *ομάδες μεγέθους* $2m-1$ *μπορούν να αποκαλύψουν το πρώτο μέρος του μυστικού*

(ii) $m-1$ *ομάδες μεγέθους* $2m-3$ *μπορούν να αποκαλύψουν το δεύτερο μέρος του μυστικού*

Θυμίζουμε ότι, από την ενότητα 8.1.3, υπάρχουν άπειρες οικογένειες πινάκων Hadamard οι οποίες παράγονται από ακολουθίες Golay (σε δυνάμεις του $2, 10$ και του 26), και τύπου Sylvester (σε δυνάμεις του 2)

ή Paley (για πρώτους αριθμούς). Χρησιμοποιώντας αυτή τη παρατήρηση με το προηγούμενο θεώρημα, το ακόλουθο πόρισμα είναι άμεσο.

Πόρισμα 26 *Έστω* $H(4m)$ *ένας πίνακας Hadamard σε ημικανονική μορφή όπως προηγουμένως, ο οποίος κατασκευάζεται από ακολουθίες Golay ή είναι τύπου Paley ή τύπου Sylvester. Τότε υπάρχει μια άπειρη οικογένεια διμερών κρυπτογραφικών σχημάτων διαμοιρασμού με δομή πρόσβασης όπως στο Θεώρημα 39.*

Σημειώνουμε ότι η δομή πρόσβασης για το δεύτερο μέρος του κρυπτογραφικού σχήματος δεν είναι οριακή (όπως στο επόμενο παράδειγμα). Αυτή η περίπτωση είναι χρήσιμη, όταν ορισμένοι χρήστες (ή ορισμένες ομάδες χρηστών) έχουν περισσότερα προνόμια από τους άλλους χρήστες. Για παράδειγμα, ο system administrator ενός τοπικού δικτύου σε σύστημα Unix είναι μια τέτοια περίπτωση.

Παράδειγμα 33 Έστω $H(16)$ ένας πίνακας Hadamard τάξης 16 (τύπου Sylvester ή κατασκευασμένος από τις $GS(8)$). Ο αντίστοιχος Hadamard σχεδιασμός είναι ο $3-(16,8,3)$ σχεδιασμός $\mathcal{D}$. Για το πρώτο μέρος του μυστικού s, η δομή πρόσβασης αυτού του κρυπτογραφικού σχήματος διαμοιρασμού περιέχει 15 block του $\mathcal{D}$ που έχουν 1 στην πρώτη θέση. Τότε, υπάρχουν 15 ομάδες μεγέθους 7. Αυτά τα block χωρίς το πρώτο σημείο σχηματίζουν ένα $2-(15,7,3)$ σχεδιασμό $\mathcal{D}'$. Για το δεύτερο μέρος (του μυστικού), επιλέγουμε εκείνα τα 7 block του $\mathcal{D}'$ που έχουν επίσης 1 στην πρώτη θέση. Αυτά τα block χωρίς το πρώτο σημείο σχηματίζουν ένα $1-(14,6,3)$ σχεδιασμό $\mathcal{D}''$. Τότε, για το δεύτερο μέρος του μυστικού, η δομή πρόσβασης αποτελείται από 3 ομάδες μεγέθους 5. Για να αποκαλύψουμε το διμερές μυστικό θα πρέπει αρχικά να χρησιμοποιήσουμε τις ομάδες μεγέθους 5. Στη συνέχεια, για να αποκαλύψουμε το υπόλοιπο μέρος του μυστικού χρησιμοποιούμε αυτές τις ομάδες (που είναι πλέον μεγέθους 6) και τις υπόλοιπες 4 ομάδες μεγέθους 6. Μετέπειτα, προσθέτουμε ένα νέο συμμετέχοντα του οποίου η δομή πρόσβασης σε αυτές τις ομάδες μεγέθους 6 έχει μονάδες (οι υπόλοιπες τιμές είναι 0). Στη τελευταία φάση, χρησιμοποιούμε τις παραγόμενες 15 ομάδες μεγέθους 7, και τις υπόλοιπες 15 ομάδες ίδιου μεγέθους για να αποκαλύψουμε το πρώτο μέρος του μυστικού.

Παράδειγμα 34 Έστω $H(56)$ ένας πίνακας Hadamard τάξης 56. Ο αντίστοιχος Hadamard σχεδιασμός είναι ένας $3-(56,28,13)$ σχεδιασμός $\mathcal{D}$. Με παρόμοιο τρόπο όπως στο προηγούμενο παράδειγμα, για το πρώτο μέρος του μυστικού s, η δομή πρόσβασης αυτού του κρυπτογραφικού σχήματος διαμοιρασμού περιέχει 55 block του $\mathcal{D}$ τα οποία έχουν 1 στην πρώτη θέση. Τότε, υπάρχουν 55 ομάδες μεγέθους 27. Αυτά τα block χωρίς το πρώτο σημείο σχηματίζουν έναν $2-(55,27,13)$ σχεδιασμό $\mathcal{D}'$. Για το δεύτερο μέρος (του μυστικού), επιλέγουμε εκείνα τα 27 block του $\mathcal{D}'$ τα οποία έχουν 1 στην πρώτη θεση. Αυτά τα block χωρίς την πρώτη θέση σχηματίζουν εναν $1-(54,26,13)$ σχεδιασμό $\mathcal{D}''$. Τότε, για το δεύτερο μέρος του μυστικού, η δομή πρόσβασης αποτελείται από 13 ομάδες μεγέθους 25. Για να αποκαλύψουμε το διμερές μυστικό θα πρέπει αρχικά να χρησιμοποιήσουμε τις ομάδες μεγέθους 25. Στη συνέχεια, για να αποκαλύψουμε το υπόλοιπο μέρος του μυστικού χρησιμοποιούμε αυτές τις ομάδες (που είναι πλέον μεγέθους 26) και τις υπόλοιπες ομάδες μεγέθους επίσης 26. Μετέπειτα, προσθέτουμε ένα νέο συμμετέχοντα του οποίου η δομή πρόσβασης σε αυτές τις ομάδες μεγέθους 26 έχει μονάδες (οι υπόλοιπες τιμές είναι 0). Στη τελευταία φάση, χρησιμοποιούμε τις παραγόμενες 55 ομάδες μεγέθους 27, και τις υπόλοιπες 55 ομάδες ίδιου μεγέθους για να αποκαλύψουμε το πρώτο μέρος του μυστικού.

§8.3 Αλγοριθμική Κατασκευή Κρυπτογραφικών Σχημάτων από Πίνακες Hadamard

Στην τελευταία ενότητα αυτού του κεφαλαίου, παρουσιάζουμε μια αλγοριθμική κατασκευή κρυπτογραφικών σχημάτων διαμοιρασμού από πίνακες Hadamard, βασιζόμενοι στις πολλαπλασιαστικές μεθόδους για βασικές ακολουθίες που παρουσιάστηκαν στο πρώτο μέρος της διατριβής και στην Ενότητα 8.1.3. Σημειώνουμε ότι, οι βασικές ακολουθίες, $BS(n+1,n)$, υπάρχουν για κάθε μήκος $n=1,\ldots,35$. Όλες οι βασικές ακολουθίες $BS(n+1,n)$ για $n=1,\ldots,35$ μπορούν να βρεθούν στην [146].

Algorithm 25 BASESEQS2SECRETSHARINGSCHEME ALGORITHM

function BASESEQS2SECRETSHARINGSCHEME(B1, B2, B3, B4)
Require: $BS(n+1, n)$ exist
$X, Y, Z, W \leftarrow$ BASESEQS2TSEQS(B1, B2, B3, B4) ▷ X, Y, Z, W are $TS(2n+1)$
$H(4(2n+1)) \leftarrow$ TSEQS2HADAMARD(X, Y, Z, W) ▷ Theorem 38 Construction
$H(4m(2n+1)) \leftarrow H(4(2n+1)) \otimes H(m)$ ▷ Theorem 35 Construction
HADAMARD3DESIGN$(4m(2n+1), 2m(2n+1), 2mn+m-1) \leftarrow$
HADAMARD2HADAMARDDESIGN$(H(4m(2n+1)))$
return (SecretSharingScheme)
end function

Επεξηγούμε την εκτέλεση του Αλγορίθμου 25 για $n = 1$, οπτικοποιώντας με αυτό τον τρόπο την προτεινόμενη μέθοδο μας για κρυπτογραφικά σχήματα διαμοιρασμού στο ακόλουθο παράδειγμα.

Είσοδος. $BS(2,1)$: $B_1 = [1,1]$, $B_2 = [1,-1]$, $B_3 = [1]$, $B_4 = [1]$

Βήμα 1. $TS(3)$: $X = [1,0,0]$, $Y = [0,1,0]$, $Z = [0,0,1]$, $W = [0,0,0]$

Βήμα 2. $H(24)$: θεωρούμε το γινόμενο Kronecker του παραγόμενου $H(12)$ από τις $TS(3)$ με τον $H(2)$, δηλαδή $H(24) = H(12) \otimes H(2)$

Βήμα 3. Κανονικοποιούμε τον παραγόμενο πίνακα Hadamard τάξης 24, $H(24)$:

$$H(24) = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\
1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\
1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\
1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - \\
1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & 1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - \\
1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\
1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\
1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\
1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - \\
1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 \\
1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & - & - & - & - \\
1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 \\
1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - \\
1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & - & - & - & 1 & 1 & - & 1 & - & - & - & 1 & 1 \\
1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 & 1 \\
1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 \\
1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 & - & - & - & - \\
1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - & - \\
1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - \\
1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - \\
1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - \\
1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & - & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 1
\end{pmatrix}$$

Βήμα 4. Ο πίνακας πρόσπτωσης (incidence matrix) του αντίστοιχου

Hadamard 3-σχεδιασμού είναι:

$$
\mathrm{D} = \begin{pmatrix}
10101110001010101011100010\\
01010001110101010100011101\\
10010111000110010111000 01\\
01101000111001101000 1110\\
11001011100011001011 1000\\
00110100011100110100 0111\\
10100101110010100101 1100\\
01011010001101011010 0011\\
10010010111010010010 1110\\
01101101000101101101 0001\\
10001001011110001001 0111\\
01110110100001110110 1000\\
11000100101111000100 1011\\
00111011010000111011 0100\\
11100010010111100010 0101\\
00011101101000011101 1010\\
11110001001011110001 0010\\
00001110110100001110 1101\\
10111000100110111000 1001\\
01000111011001000111 0110\\
11011100010011011100 0100\\
00100011101100100011 1011\\
11111111111100000000 0000\\
00000000000011111111 1111\\
10101110001001010001 1101\\
01010001110110101110 0010\\
10010111000101101000 1110\\
01101000111010010111 0001\\
11001011100000110100 0111\\
00110100011111001011 1000\\
10100101110001011010 0011\\
01011010001110100101 1100\\
10010010111001101101 0001\\
01101101000110010010 1110\\
10001001011101110110 1000\\
01110110100010001001 0111\\
11000100101100111011 0100\\
00111011010011000100 1011\\
11100010010100011101 1010\\
00011101101011100010 0101\\
11110001001000001110 1101\\
00001110110111110001 0010\\
10111000100101000111 0110\\
01000111011010111000 1001\\
11011100010000100011 1011\\
00100011101111011100 0100
\end{pmatrix}
$$

Βήμα 4. Ο πίνακας D_1 αναπαριστά το κλειδί (η πρώτη συντεταγμένη αυτού του πίνακα) για το πρώτο μέρος του μυστικού. Τα block του D_1 χωρίς αυτήν την συντεταγμένη σχηματίζουν τις ομάδες μεγέθους 11, και τον $2-(23,11,5)$ σχεδιασμό D'. Ο πίνακας D_2 περιέχει τα block του D' που έχουν 1 στην πρώτη συντεταγμένη. Χωρίς αυτή τη συντεταγμένη, αυτά τα block του D' σχηματίζουν έναν $1-(22,10,5)$ σχεδιασμό. Ο πίνακας D_3 αναπαριστά το κλειδί (η τρίτη συντεταγμένη αυτού του πίνακα) για το δεύτερο μέρος του μυστικού. Αυτές οι δύο γραμμές (χωρίς τις συντεταγμένες τους

που απεικονίζουμε με έντονη γραμματοσειρά) σχηματίζουν ομάδες μεγέθους 9.

$$\mathrm{D}_1 = \begin{pmatrix}
\mathbf{1}01011100010101011100010\\
\mathbf{1}00101110001100101110001\\
\mathbf{1}10010111000110010111000\\
\mathbf{1}01001011100101001011100\\
\mathbf{1}00100101110100100101110\\
\mathbf{1}00010010111100010010111\\
\mathbf{1}10001001011110001001011\\
\mathbf{1}11000100101111000100101\\
\mathbf{1}11100010010111100010010\\
\mathbf{1}01110001001101110001001\\
\mathbf{1}10111000100110111000100\\
\mathbf{1}11111111111000000000000\\
\mathbf{1}01011100010010100011101\\
\mathbf{1}00101110001011010001110\\
\mathbf{1}10010111000001101000111\\
\mathbf{1}01001011100010110100011\\
\mathbf{1}00100101110011011010001\\
\mathbf{1}00010010111011101101000\\
\mathbf{1}10001001011001110110100\\
\mathbf{1}11000100101000111011010\\
\mathbf{1}11100010010000011101101\\
\mathbf{1}01110001001010001110110\\
\mathbf{1}10111000100001000111011
\end{pmatrix},$$

$$\mathrm{D}_2 = \begin{pmatrix}
\mathbf{1}10010111000110010111000\\
\mathbf{1}10001001011110001001011\\
\mathbf{1}11000100101111000100101\\
\mathbf{1}11100010010111100010010\\
\mathbf{1}10111000100110111000100\\
\mathbf{1}11111111111000000000000\\
\mathbf{1}10010111000001101000111\\
\mathbf{1}10001001011001110110100\\
\mathbf{1}11000100101000111011010\\
\mathbf{1}11100010010000011101101\\
\mathbf{1}10111000100001000111011
\end{pmatrix}, \quad \mathrm{D}_3 = \begin{pmatrix}
\mathbf{1}11000100101111000100101\\
\mathbf{1}11100010010111100010010\\
\mathbf{1}11111111111000000000000\\
\mathbf{1}11000100101000111011010\\
\mathbf{1}11100010010000011101101
\end{pmatrix}$$

Σε αυτό το παράδειγμα το δεύτερο μέρος του κρυπτογραφικού σχήματος δεν είναι οριακό (threshold). Συγκεκριμένα, το σύνολο των χρηστών $\{3, 4, 5, 6, 7, 8, 9, 10, 11\}$ μπορούν να αποκαλύψουν το μυστικό, αλλά αυτό επίσης μπορεί να αποκαλυφθεί από υποσύνολα των χρηστών $\{3, 4, 6\}$, $\{5, 7, 9\}$, ή $\{8, 10, 11\}$. Αυτή η περίπτωση, είναι ιδιαίτερα χρήσιμη όταν ειδικές ομάδες χρηστών έχουν περισσότερα προνόμια από τους άλλους. Για παράδειγμα, αν οι χρήστες ήταν ο πρόεδρος, ο αντιπρόεδρος και ο σύμβουλος ασφαλείας μιας τράπεζας, ο συνδυασμός μιας τραπεζικής θυρίδας που φυλάσσεται σε αυτή την τράπεζα μπορεί να βρεθεί είτε από τους ιδιοκτήτες της, είτε από την ειδική ομάδα χρηστών: πρέδρος-αντιπρόεδρος-σύμβουλος ασφαλείας.

Βιβλιογραφία

[1] T. L. Alderson. Extending MDS codes. *Annals of Combinatorics* **9** (2005), 125–135.

[2] T. L. Alderson, A. A. Bruen and R. Silverman. Maximum distance separable codes and arcs in projective spaces. *Journal of Combinatorial Theory - Series A* **114** (2007), 1101–1117.

[3] K. T. Arasu and T. A. Gulliver. Self-dual codes over $\mathbb{F}_p$ and weighing matrices. *IEEE Transactions on Information Theory* **47** (2001), 2051–2055.

[4] E. F. Assmus Jr. and H. F. Mattson Jr. New 5-designs. *Journal of Combinatorial Theory - Series A* **6** (1969), 122–151.

[5] E. F. Assmus Jr. and J. D. Key. *Designs and their codes*. Cambridge University Press, Great Britain, 1992.

[6] J. C. Bean. Genetic algorithms and random keys for sequencing and optimization. *ORSA Journal on Computing* **6** (1994), 154–160.

[7] E. R. Berlekamp. Distribution of cyclic matrices in a finite field. *Duke Mathematical Journal* **33** (1966), 45–48.

[8] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos. On self-dual codes over some prime fields. *Discrete Mathematics* **262** (2003), 37–58.

[9] V. K. Bhargava, G. E. Sguin, and J. M. Stein. Some (mk, k) cyclic codes in quasi-cyclic form. *IEEE Transactions on Information Theory* **24** (1978), 630–632.

[10] G. R. Blakley. Safeguarding cryptographic keys. *Proceeding of the AFIPS National Computer Conference*, 1979, pp. 313–317.

[11] C. Blum and A. Roli. Metaheuristics in combinatorial optimization: Overview and conceptual comparison. *ACM Computing Surveys* **35** (2003), 268–308.

[12] I. E. Bocharova, R. Johannesson, B. D. Kudryashov and P. Stahl. Tailbiting codes: bounds and search results. *IEEE Transactions on Information Theory* **48** (2002), 137–148.

[13] M.A. de Boer. Almost MDS codes. *Designs, Codes and Cryptography* **9** (1996), 143–155.

[14] K. H. V. Booth and C. R. Cox. Some systematic supersaturated designs. *Technometrics* **4** (1962), 489–495.

[15] W. Bosma and J. Cannon. *Handbook of Magma Functions*, Version 2.9. University of Sydney, 2002.

[16] S. Bouyuklieva and Z. Varbanov. Some connections between self-dual codes, combinatorial designs and secret-sharing schemes. *Advances in Mathematics of Communications* **5** (2011), 191–198.

[17] S. Boyd. Multitone signals with low crest factor. *IEEE Transactions on Circuits and Systems* **33** (1986), 1018–1022.

[18] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment*. In Information Security and Cryptography Series. Springer-Verlag, Heidelberg, 2003.

[19] A. E. Brouwer. Bounds on linear codes. In *Handbook of Coding Theory*, V. Pless and W. C. Huffman (Eds.), pp. 295–461. Elsevier, Amsterdam, 1998.

[20] A. A. Bruen, J. A. Thas and A. Blokhuis. On M.D.S. codes, arcs in $\mathrm{PG}(n, q)$ with q even, and a solution of three fundamental problems of B. Segre. *Inventiones mathematicae* **3** (1988), 441–459.

[21] J. M. Chao and H. Kaneta. Rational arcs in $\mathrm{PG}(r, q)$ for $11 \leq q \leq 19$. *Discrete Mathematics* **174** (1997), 87–94.

[22] J. M. Chao and H. Kaneta. Rational arcs in $\mathrm{PG}(r, q)$ for $23 \leq q \leq 29$. *Discrete Mathematics* **226** (2001), 377–385.

[23] C. L. Chen, W. W. Peterson and E. J. Weldon, Jr.. Some results on quasi-cyclic codes. *Information and Control* **15** (1969), 407–423.

[24] Z. Chen. Six new binary quasi cyclic codes. *IEEE Transactions on Information Theory* **40** (1994), 1666–1667.

[25] E. Z. Chen. *Web database of binary QC codes*, [Online]. Available: `http://www.tec.hkr.se/ chen/research/codes/searchqc2.htm`.

[26] Y.-P. Chen, T.-L. Yu, K .Sastry and D. E. Goldberg. A survey of linkage learning techniques in genetic and evolutionary algorithms. University of Illinois at Urbana-Champaign, Urbana IL., IlliGAL Report No. **2007014** (2007).

[27] F. Chung, A. J. Salehi ans V. Wei. Optical orthogonal codes: Design, analysis and applications. *IEEE Transactions on Information Theory* **35** (1989), 595–604.

[28] C. J. Colbourn, J. H. Dinitz and D.R. Stinson. Applications of combinatorial designs to communications, cryptography, and networking. In *Surveys in Combinatorics*, J. D. Lamb and D. A. Preece (Eds.), pp. 37–100. Cambridge University Press, Cambridge, 1999.

[29] J. Cooper and J. S. Wallis. A construction for Hadamard arrays. *Bulletin of the Australian Mathematical Society* **7** (1972), 269–278.

[30] T. H. Cormen, C. H. Leiserson, R. L. Rivest and C. Stein. *Introduction to Algorithms*. MIT Press, 2003.

[31] T. J. Cox, J. A. Angus and P. D'Antonio. Ternary and quadriphase sequence diffusers. *Journal of the Acoustical Society of America* **119** (2006), 310–319.

[32] R. Craigen. Hadamard matrices and designs. In *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), pp. 370–377. CRC Press, Boca Raton, Fla., 1996.

[33] R. Craigen. Weighing matrices and conference matrices. In *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), pp. 496–504. CRC Press, Boca Raton, Fla., 1996.

[34] R. Craigen. Products and factorizations of ternary complementary pairs. *The Australasian Journal of Combinatorics* **34** (2006), 269–280.

[35] R. Craigen and H. Kharaghani. Orthogonal designs. In *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), Second Edition. pp. 280–295. Chapman and Hall/CRC Press, Boca Raton, Fla., 2006.

[36] R. Craigen and C. Koukouvinos. A theory of ternary complementary pairs. *Journal of Combinatorial Theory - Series A* **96** (2001), 358–375.

[37] R. Craigen, S. Georgiou, W. Gibson and C. Koukouvinos. Further explorations into ternary complementary pairs. *Journal of Combinatorial Theory - Series A* **113** (2006), 952–965.

[38] R. Craigen, W. Gibson and C. Koukouvinos. An update on primitive ternary complementary pairs. *Journal of Combinatorial Theory - Series A* **114** (2007), 957–963.

[39] W. van Dam. Quantum algorithms for weighing matrices and quadratic residues, *Algorithmica* **34** (2002), 413–428.

[40] L. Davis, (Eds.) *Handbook of Genetic Algorithms*. Van Nostrand, Reinhold, 1991.

[41] J. Day and B. Peterson. Growth in gaussian elimination. *The American Mathematical Monthly* **95** (1988), 489–513.

[42] S. Dodunekov and I. N. Landjev. On near-MDS codes. *Journal of Geometry* **54** (1995), 30–43.

[43] R. Dodunekova, S. M. Dodunekov, T. Kløve. Almost-MDS and near-MDS codes for error detection. *IEEE Transactions on Information Theory* **43** (1997), 285–290.

[44] S. T. Dougherty, T. A. Gulliver and M. Harada. Optimal formally self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$. *Applicable Algebra in Engineering, Communication and Computing* **10** (2000), 227–236.

[45] S. T. Dougherty, S. Mesnager and P. Solé. Secret-sharing schemes based on self-dual codes. *Information Theory Workshop*, ITW, 2008, pp. 338–342.

[46] M. Esmaeili and S. Yari. On complementary-dual quasi-cyclic codes. *Finite Fields and their Applications* **15** (2009), 375–386.

[47] M. Esmaeili, T. A. Gulliver, N. P. Secord and S. A. Mahmoud. A link between quasi-cyclic codes and convolutional codes. *IEEE Transactions on Information Theory* **44** (1998), 431–435.

[48] E. E. Fenimore and T. M. Cannon. Coded aperture imaging with uniformly redundant arrays. *Applied Optics* **17** (1978), 337–347.

[49] N. Ferguson and B. Schneier. *Practical Cryptography*. Wiley Publishing, Inc., 2003.

[50] R. J. Fletcher, M. Gysin and J. Seberry. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. *The Australasian Journal of Combinatorics* **23** (2001), 75–86.

[51] S. Forrest. Genetic algorithms: Principles of natural selection applied to computation. *Science* **261** (1993), 872–878.

[52] P. Gaborit. Quadratic double circulant codes over fields. *Journal of Combinatorial Theory - Series A* **97** (2002), 85–107.

[53] P. Gaborit. Tables of self-dual codes, [Online]. Available: `http://www.unilim.fr/pages_perso/philippe.gaborit/SD`.

[54] P. Gaborit and A. Otmani. Experimental constructions of self-dual codes. *Finite Fields and their Applications* **9** (2003), 372–394.

[55] A. Gavish and A. Lempel. On ternary complementary sequences. *IEEE Transactions on Information Theory* **40** (1994), 522–526.

[56] S. D. Georgiou. Signed differences for weighing designs. *Sankhyā* **72-B** (2010), 107–121.

[57] S. Georgiou, I. S. Kotsireas and C. Koukouvinos. Inequivalent Hadamard matrices of order $2n$ constructed from Hadamard matrices of order n. *Journal of Combinatorial Mathematics and Combinatorial Computing* **63** (2007), 65–79.

[58] S. Georgiou and C. Koukouvinos. On sequences with zero autocorrelation and orthogonal designs. *Journal of Combinatorial Theory - Series A* **94** (2001), 15–33.

[59] S. Georgiou and C. Koukouvinos. Self-dual codes over GF(7) and orthogonal designs. *Utilitas Mathematica* **60** (2001), 79–89.

[60] S. Georgiou and C. Koukouvinos. On generalized Legendre pairs and multipliers of the corresponding supplementary difference sets. *Utilitas Mathematica* **61** (2002), 47–63.

[61] S. Georgiou and C. Koukouvinos. New infinite classes of weighing matrices. *Sankhyā* **64-B** (2002), 26–36.

[62] S. Georgiou and C. Koukouvinos. MDS self-dual codes over large prime fields. *Finite Fields and their Applications* **8** (2002), 455–470.

[63] S. Georgiou and C. Koukouvinos. New infinite classes of orthogonal designs. *Linear and Multilinear Algebra* **50** (2002), 293–300.

[64] S. Georgiou and C. Koukouvinos. Self-orthogonal and self-dual codes constructed via combinatorial designs and diophantine equations. *Designs, Codes and Cryptography* **32** (2004), 193–206.

[65] S. Georgiou and C. Koukouvinos. Self-dual codes over F_p and orthogonal designs. *Journal of Combinatorial Mathematics and Combinatorial Computing* **50** (2004), 159–177.

[66] S. Georgiou and C. Koukouvinos. Combinatorial designs and codes over some prime fields. *Journal of Statistical Planning and Inference* **135** (2005), 93–106.

[67] S. Georgiou, M. Harada and C. Koukouvinos. Orthogonal designs and Type II codes over $\mathbb{Z}_{2k}$. *Designs, Codes and Cryptography* **25** (2002), 163–174.

[68] S. Georgiou, C. Koukouvinos and E. Lappas. Self-dual codes over some prime fields constructed from skew-Hadamard matrices. *Journal of Discrete Mathematical Sciences & Cryptography* **10** (2007), 255–266.

[69] S. Georgiou, C. Koukouvinos and J. Seberry. Hadamard matrices, orthogonal designs and construction algorithms. In *Designs 2002: Further Computational and Constructive Design Theory*, W. D. Wallis (Eds.), pp. 133–205. Kluwer Academic Publishers, Norwell, Massachusetts, 2003.

[70] A. V. Geramita and J. Seberry. *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*. In Series: Lecture Notes in Pure and Applied Mathematics **45**. Marcel Dekker, Inc., New York, 1979.

[71] M. J. E. Golay. Complementary sequences. *IRE Transactions on Information Theory* **7** (1961), 82–87.

[72] M. J. E. Golay. Note on "Complementary series". *Proceedings of the IRE* **50** (1962), 84.

[73] D.E. Goldberg. Simple genetic algorithms and the minimal deceptive problem. In *Genetics Algorithms and Simulated Annealing*, L. Davis (Eds.), pp. 74–88. Pitman, London, 1987.

[74] D. E. Goldberg. *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley, Reading, MA, 1989.

[75] D. E. Goldberg, K. Deb and B. Korb. Messy genetic algorithms: Motivation, analysis, and first results. *Complex Systems* **5** (1989), 493–530.

[76] D. E. Goldberg, K. Deb and B. Korb. Messy genetic algorithms revisited: Studies in mixed size and scale. *Complex Systems* 4 (1990), 415–444.

[77] D. E. Goldberg, K. Deb, H. Kargupta, G. Harik. Rapid, accurate optimization of difficult problems using fast messy genetic algorithms. University of Illinois at Urbana-Champaign, Urbana IL., IlliGAL Report No. **93004** (1993).

[78] D. E. Goldberg, K. Deb, H. Kargupta, G. Harik. Rapid, accurate optimization of difficult problems using fast messy genetic algorithms. *Proceedings of the 5th International Conference on Genetic Algorithms*, San Francisco, CA, USA, 1993, pp. 56-64.

[79] D.E. Goldberg, K. Deb and D. Thierens. Towards a better understanding of mixing in genetic algorithms. *Journal of the Society for Instrumentantion and Control Engineers* **32** (1993), 10–16.

[80] S. W. Golomb and G. Gong. *Signal Design for Good Correlation. For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, Cambridge, 2005.

[81] S. Golomb and H. Taylor. Two-dimensional synchronization patterns for minimum ambiguity. *IEEE Transactions on Information Theory* **28** (1982), 600–604.

[82] J. F. Goncalves and M. G. C. Resende. Biased random-key genetic algorithms for combinatorial optimization. To appear in *Journal of Heuristics*.

[83] M. Grassl. Searching for linear codes with large minimum distance. In *Discovering Mathematics with Magma*, W. Bosma and J. Cannon (Eds.), pp. 287–313. Springer, Heidelberg, 2006.

[84] M. Grassl. Computing extensions of linear codes. *Proceedings of the IEEE International Symposium on Information Theory*, ISIT, 2007, pp. 476–480.

[85] M. Grassl. Bounds on the minimum distance of linear codes, [Online]. Available: `http://www.codetables.de`.

[86] M. Grassl and G. White. New codes from chains of quasi-cyclic codes. *Proceedings of the IEEE International Symposium on Information Theory*, ISIT, 2005, pp. 2095–2099.

[87] D. H. Greene and D. E. Knuth. *Mathematics for the Analysis of Algorithms*. Third Edition. Modern Birkhauser Classics, Birkhauser, Boston, 2008.

[88] P. P Greenough and R. Hill. Optimal ternary quasi-cyclic codes. *Designs, Codes and Cryptography* **2** (1992), 81–91.

[89] T. A. Gulliver and V. K. Bhargava. A systematic (16,8) code for correcting double errors and detecting triple-adjacent errors. *IEEE Transactions on Computers* **42** (1993), 109–112.

[90] T. A. Gulliver and V. K. Bhargava. Some best rate 1/p and rate $(p-1)/p$ systematic quasi-cyclic codes. *IEEE Trans. Inform. Theory* **37** (1991), 552–555.

[91] T. A. Gulliver and V. K. Bhargava. An updated table of rate 1/p binary quasi-cyclic code. *Applied Mathematical Letters* **8** (1995), 81–86.

[92] T. A. Gulliver and M. Harada. New optimal self-dual codes over $GF(7)$. *Graphs and Combinatorics* **15** (1999), 175–186.

[93] T. A. Gulliver and M. Harada. Double circulant self-dual codes over $GF(5)$. *Ars Combinatoria* **56** (2000), 3–13.

[94] T. A. Gulliver and M. Harada. On the minimum weight of codes over $\mathbb{F}_5$ constructed from certain conference matrices. *Designs, Codes and Cryptography* **31** (2004), 139–145.

[95] T. A. Gulliver, M. Harada and H. Miyabayashi. Double circulant self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$. *Advances in Mathematics of Communications* **1** (2007), 223–238.

[96] M. Gysin and J. Seberry. An experimental search and new combinatorial designs via a generalization of cyclotomy. *Journal of Combinatorial Mathematics and Combinatorial Computing* **27** (1998), 143–160.

[97] J. Hadamard. Resolution d'une question relative aux determinants. *Bulletin des Sciences Mathématiques* **17** (1893), 240–246.

[98] M. Hall Jr. A survey of difference sets. *Proceedings of the American Mathematical Society* **7** (1956), 975–986.

[99] M. Hall, Jr. *Combinatorial Theory*. Reprint of the 1986 Second Edition, Wiley Classics Library, Wiley, New York, 1998.

[100] S. Han, J.-L. Kim, H. Lee and Y. Lee. Construction of cubic self-dual codes. *Proceedings of the IEEE International Symposium on Information Theory*, ISIT, 2009, pp. 2396–2399.

[101] M. Harada. On the self-dual $\mathbb{F}_5$-codes constructed from Hadamard matrices of order 24. *Journal of Combinatorial Designs* **13** (2005), 152–156.

[102] M. Harada and H. Kharaghani. Orthogonal designs and MDS self-dual codes. *Australasian Journal of Combinatorics* **35** (2006), 57–67.

[103] M. Harada and A. Munemasa. There exists no self-dual [24,12,10] code over $\mathbb{F}_5$. *Designs, Codes and Cryptography* **52** (2009), 125–127.

[104] M. Harada and P. R. J. Östergård. On the classification of self-dual codes over $\mathbb{F}_5$. *Graphs and Combinatorics* **19** (2003), 203–214.

[105] G.R. Harik and D.E. Goldberg. Learning linkage. *Proceedings of the 4th Workshop on Foundations of Genetic Algorithms*, San Diego, CA, USA, 1996, pp. 247–262.

[106] R. Harkins, E. Weber and A. Westmeyer. Encryption schemes using finite frames and Hadamard arrays. *Experimental Mathematics* **14** (2005), 423–433.

[107] P. Heijnen, H. van Tilborg, T. Verhoeff and S. Weijs. Some new binary, quasi-cyclic codes. *IEEE Transactions on Information Theory* **44** (1998), 1994–1998.

[108] J. E. Hershey and R. Yarlagadda. Two-dimensional synchronisation. *Electronics Letters* **19** (1983), 801–803.

[109] J. W. P. Hirshfeld. Complete arcs. *Discrete Mathematics* **174** (1997), 177–184.

[110] J. W. P. Hirschfeld and J. A. Thas. *General Galois Geometries*. Oxford University Press, Oxford, 1991.

[111] J. H. Holland. *Adaptation in Natural and Artificial Systems, an Introductory Analysis with Applications to Biology, Control and Artificial Intelligence*. University of Michigan Press, Ann Arbor, Michigan, 1975.

[112] W. H. Holzmann and H. Kharaghani. On the Plotkin arrays. *The Australasian Journal of Combinatorics* **22** (2000), 287–299.

[113] K. J. Horadam.*Hadamard matrices and their Applications*. Princeton University Press, Princeton, NJ, 2007.

[114] H. Hotelling. Some improvements in weighing and other experimental techniques. *The Annals of Mathematical Statistics* **16** (1944), 294–300.

[115] D. R. Hughes and F. C. Piper. *Design Theory*. Cambridge University Press, Cambridge, 1985.

[116] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Second Edition. In Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[117] D. B. Jaffe. Binary linear codes: new results on nonexistence, [Online]. Available:
http://www.math.unl.edu/~djaffe2/codes/webcodes/codeform.html

[118] K. A. De Jong. An Analysis of the Behavior of a Class of Genetic Adaptive Systems. Doctoral Thesis, CCS Department, University of Michigan, Ann Arbor, MI, 1975.

[119] M. Karlin. Decoding of circulant codes. *IEEE Transactions on Information Theory* **16** (1970), 797–802.

[120] T. Kasami. A Gilbert-Varshamov bound for quasi-cyclic codes of Rate 1/2. *IEEE Transactions on Information Theory* **20** (1974), 679.

[121] H. Kharaghani. Arrays for orthogonal designs. *Journal of Combinatorial Designs* **8** (2000), 166–173.

[122] H. Kharaghani and C. Koukouvinos. Complementary, base and Turyn sequences. In *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), Second Edition, pp. 317–321. Chapman and Hall/CRC Press, Boca Raton, Fla., 2006.

[123] J.-L. Kim and S. Han. On self-dual codes over $\mathbb{F}_5$. *Designs, Codes and Cryptography* **48** (2008), 43–58.

[124] J.-L. Kim and Y. Lee. Euclidean and Hermitian self-dual MDS codes over large finite fields. *Journal of Combinatorial Theory - Series A* **105** (2004), 79–95.

[125] J.-L. Kim and Y. Lee. Construction of MDS self-dual codes over Galois rings. *Designs, Codes and Cryptography* **45** (2007), 247–258.

[126] J.-L. Kim and P. Sole. Skew Hadamard designs and their codes. *Designs, Codes and Cryptography* **49** (2008), 135–145.

[127] D. Knjazew. OmeGA: A Competent Genetic Algorithm for Solving Permutation and Scheduling Problems. Kluwer, Norwell, 2002.

[128] D. E. Knuth. *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*. Third Edition. In Series: Computer Science and Information Processing, Addison-Wesley Publishing Co., Mass.-London-Don Mills, 1998.

[129] D. E. Knuth. *The Art of Computer Programming, Vol. 3: Sorting and Searching*. Third Edition. In Series: Computer Science and Information Processing, Addison-Wesley Publishing Co., Mass.-London-Don Mills, 1998.

[130] D. E. Knuth. *Selected Papers on Analysis of Algorithms*, Centre for the Study of Language and Information - CSLI Lecture Notes, Vol. **102**. Stanford, California, 2000.

[131] T. Koshy. Polynomial approach to quasi-cyclic codes. *Bulletin of the Calcutta Mathematical Society* **69** (1977), 51–59.

[132] I. S. Kotsireas and C. Koukouvinos. Inequivalent Hadamard matrices with buckets. *Journal of Discrete Mathematical Sciences and Cryptography* **7** (2004), 307–317.

[133] I. S. Kotsireas and C. Koukouvinos. New skew-Hadamard matrices via computational algebra. *Australasian Journal of Combinatorics* **41** (2008), 235–248.

[134] I. S. Kotsireas, C. Koukouvinos, and G. Pinheiro. Metasoftware for Hadamard matrices. *International Journal of Applied Mathematics* **18** (2005), 263–278.

[135] I. S. Kotsireas, C. Koukouvinos and J. Seberry. Hadamard ideals and Hadamard matrices with circulant core. *Journal of Combinatorial Mathematics and Combinatorial Computing* **57** (2006), 47–63.

[136] I. S. Kotsireas, C. Koukouvinos and J. Seberry. Hadamard ideals and Hadamard matrices with two circulant cores. *European Journal of Combinatorics* **27** (2006), 658–668.

[137] I. Kotsireas, C. Koukouvinos, J. Seberry. Weighing matrices and string sorting. *Annals of Combinatorics* **13** (2009), 305•-313.

[138] I. S. Kotsireas, C. Koukouvinos, J. Seberry and D. E. Simos. New classes of orthogonal designs constructed from complementary sequences with given spread. *The Australasian Journal of Combinatorics* **46** (2010), 67–78.

[139] I. S. Kotsireas, C. Koukouvinos and D. E. Simos. Large orthogonal designs via amicable sets of matrices. *International Journal of Applied Mathematics* **12** (2006), 217–232.

[140] I. S. Kotsireas, C. Koukouvinos and D. E. Simos. Inequivalent Hadamard matrices from base sequences. *Utilitas Mathematica* **78** (2009), 3–9.

[141] I. S. Kotsireas, C. Koukouvinos and D. E. Simos. MDS and near-MDS self-dual codes over large prime fields. *Advances in Mathematics of Communications* **3** (2009), 349–361.

[142] I. S. Kotsireas, C. Koukouvinos and D. E. Simos. Inequivalent Hadamard matrices from near normal sequences. *Journal of Combinatorial Mathematics and Combinatorial Computing* **75** (2010), 105–115.

[143] C. Koukouvinos. Sequences with zero autocorrelation. In *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), pp. 452-456. CRC Press, Boca Raton, Fla., 1996.

[144] C. Koukouvinos. Undecided cases for D-optimal designs of order $n \equiv 0 \pmod 4$, [Online]. Available: `http://www.math.ntua.gr/~ckoukouv`.

[145] C. Koukouvinos. Hadamard matrices of order 4t, t odd positive integer, [Online]. Available: `http://www.math.ntua.gr/~ckoukouv`.

[146] C. Koukouvinos. Base sequences $BS(n+1, n)$, [Online]. Available: `http://www.math.ntua.gr/~ckoukouv`.

[147] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang. Multiplication of sequences with zero autocorrelation. *The Australasian Journal of Combinatorics* **10** (1994), 5–15.

[148] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang. On Sequences with zero autocorrelation. *Designs, Codes and Cryptography* **4** (1994), 327–340.

[149] C. Koukouvinos, K. Mylona and D. E. Simos. Exploring k-circulant supersaturated designs via genetic algorithms. *Computational Statistics & Data Analysis* **51** (2007), 2958–2968.

[150] C. Koukouvinos, E. Lappas and D. E. Simos. Encryption schemes using orthogonal arrays. *Journal of Discrete Mathematical Sciences and Cryptography* **12** (2009), 615–628.

[151] C. Koukouvinos, V. Pillwein, D. E. Simos and Z. Zafeirakopoulos. On the average complexity for the verification of compatible sequences. *Information Processing Letters* **111** (2011), 825–830.

[152] C. Koukouvinos and J. Seberry. Weighing matrices and their applications. *Journal of Statistical Planning and Inference* **62** (1997), 91–101.

[153] C. Koukouvinos and J. Seberry. New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function - a review. *Journal of Statistical Planning and Inference* **81** (1999), 153–182.

[154] C. Koukouvinos and D. E. Simos. Construction of new self-dual codes over $GF(5)$ using skew-Hadamard matrices. *Advances in Mathematics of Communications* **3** (2009), 251–263.

[155] C. Koukouvinos and D. E. Simos. Self-dual codes over small prime fields from combinatorial designs. *Lecture Notes in Computer Science* **5725** (2009), S. Bozapalidis and G. Rahonis (Eds.), pp. 278–287. (3rd International Conference on Algebraic Informatics - CAI '09).

[156] C. Koukouvinos and D. E. Simos. Improving the lower bounds on inequivalent Hadamard matrices through orthogonal designs and

meta-programming techniques. *Applied Numerical Mathematics* **60** (2010), 370–377.

[157] C. Koukouvinos and D. E. Simos. New classes of orthogonal designs and weighing matrices derived from near normal sequences. *The Australasian Journal of Combinatorics* **47** (2010), 11–20.

[158] C. Koukouvinos and D. E. Simos. New infinite families of orthogonal designs constructed from complementary sequences. *International Mathematical Forum. Journal for Theory and Applications* **5** (2010), 2655–2665.

[159] C. Koukouvinos and D. E. Simos. Further results on ternary complementary sequences, orthogonal designs and weighing matrices. *The Australasian Journal of Combinatorics* **50** (2011), 97–112.

[160] C. Koukouvinos and D. E. Simos. Encryption schemes using Plotkin arrays. *Applied Mathematics & Information Sciences* **5** (2011), 20–31.

[161] C. Koukouvinos and D. E. Simos. On the computation of the non-periodic autocorrelation function of two ternary sequences and its related complexity analysis. *Journal of Applied Mathematics & Informatics* **29** (2011), 547–562.

[162] C. Koukouvinos and D. E. Simos. Quasi-cyclic codes from cyclic-structured designs with good properties. *Discrete Mathematics, Algorithms and Applications* **3** (2011), 1–21.

[163] C. Koukouvinos and D. E. Simos. Combinatorial optimization for weighing matrices with the ordering messy genetic algorithm. *Lecture Notes in Computer Science* **6630** (2011), P. M. Pardalos and S. Rebennack (Eds.), pp. 148–156. (10th International Symposium on Experimental Algorithms - SEA '11).

[164] C. Koukouvinos and D. E. Simos. Encryption schemes based on Hadamard matrices with circulant cores. (submitted for publication).

[165] C. Koukouvinos, D. E. Simos and Z. Varbanov. Hadamard matrices, designs and their secret-sharing schemes. *Lecture Notes in Computer Science* **6742** (2011), F. Winkler (Eds.), pp. 216–229. (4th International Conference on Algebraic Informatics - CAI '11).

[166] C. Koukouvinos and S. Stylianou. On skew-Hadamard matrices. *Discrete Mathematics* **308** (2008), 2723–2731.

[167] C. W. Krueger. Software reuse. *ACM computing surveys* **24** (1992), 131–183.

[168] C. Lam, S. Lam and V. D. Tonchev. Bounds on the number of affine, symmetric, and Hadamard designs and matrices. *Journal of Combinatorial Theory - Series A* **92** (2000), 186–196.

[169] C. Lam, S. Lam and V. D. Tonchev. Bounds on the number of Hadamard designs of even order. *Journal of Combinatorial Designs* **9** (2001), 363–378.

[170] J. S. Leon, V. Pless and N. J. A. Sloane. Self-dual codes over GF(5). *Journal of Combinatorial Theory - Series A* **32** (1982), 178–194.

[171] S. Ling and P. Solé. On the algebraic structure of quasi-cyclic codes I: finite fields. *IEEE Transactions on Information Theory* **47** (2001), 2751–2760.

[172] J. H. Van Lint. Coding, decoding and combinatorics, In *Applications of Combinatorics*, R. J. Wilson, (Eds.) Shiva, Cheshire, 1982.

[173] Y. Liu and A. Dean. k-circulant supersaturated designs. *Technometrics* **46** (2004), 32–46.

[174] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton Academic Press, Princeton, 1996.

[175] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. *IEEE Transactions on Information Theory* **18** (1972), 794–805.

[176] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. The Netherlands, North-Holland, Amsterdam, 1977.

[177] Y. Magda. Visual C++ Optimization with Assembly Code. A-List, LLC, USA, East Swedesford Rd., 2004.

[178] W. Mao. *Modern Cryptography: Theory and Practice*. Prentice Hall, 2004.

[179] S. Marcugini, A. Milani and F. Pambianco. NMDS codes of maximal length over F_q, $8 \leq q \leq 11$. *IEEE Transactions on Information Theory* **48** (2002), 963–966.

[180] J. L. Massey. Reversible codes. *Information and Control* **7** (1964), 369–380.

[181] J. L. Massey. Linear codes with complementary duals. *Discrete Mathematics* **106/107** (1992), 337–342.

[182] J. L. Massey. Some applications of coding theory in cryptography. In *Codes and Ciphers, Cryptography and Coding IV*, P. G Farrell (Eds.), pp. 33–47. Formara Lt, Esses, England, 1995.

[183] B. D. McKay. Hadamard equivalence via graph isomorphism. *Discrete Mathematics* **27** (1979), 213–214.

[184] A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[185] E. Merchant. Exponentially many Hadamard designs. *Designs, Codes and Cryptography* **38** (2006), 297–308.

[186] O. Moreno, P. V. Kumar, H. F. Lu and R. Omrani. New constructions for optical orthogonal codes, distinct difference sets and synchronous optical orthogonal codes. *Proceedings of the IEEE International Symposium on Information Theory*, ISIT, 2003, pp. 327.

[187] G. Nebe, E. M. Rains and N. J. A. Sloane. *Self-dual Codes and Invariant Theory*. Springer, Heidelberg, 2006.

[188] N. K. Nguyen. An algorithmic approach to constructing supersaturated designs. *Technometrics* **38** (1996), 69–73.

[189] N. K. Nguyen and C. S. Cheng. New $E(s^2)$-optimal supersaturated designs constructed from incomplete block designs. *Technometrics* **50** (2008), 26–31.

[190] W. P. Orrick. Switching operations for Hadamard matrices. *SIAM Journal on Discrete Mathematics* **22** (2008), 31–50.

[191] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics* **12** (1933), 311–320.

[192] R. L. Plackett and J. P. Burman. The design of optimum multifactorial experiments. *Biometrika*, **33** (1946), 305–325.

[193] V. S. Pless, W. C. Huffman and R. A. Brualdi. An introduction to algebraic codes. In *Handbook of Coding Theory*, V. Pless and W.C. Huffman (Eds.), pp. 3–139. Elsevier, Amsterdam, 1998.

[194] V. Pless and J. N. Pierce. Self-dual codes over GF(q) satisfy a modified Varshamov-Gilbert bound. *Information and Control* **23** (1973), 35–40.

[195] V. S. Pless and V. D. Tonchev. Self-dual codes over GF(7). *IEEE Transactions on Information Theory* **33** (1987), 723–727.

[196] M. Plotkin. Decomposition of Hadamard matrices. *Journal of Combinatorial Theory - Series A* **13** (1972), 127–130.

[197] E. C. Posner. Combinatorial structures in planetary reconnaissance. In *Error Correcting Codes*, H. B. Mann (Eds.). Wiley, N.Y., 1968.

[198] E. M. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of Coding Theory*, V. Pless and W. C. Huffman (Eds.), pp. 177–294. Elsevier, Amsterdam, 1998.

[199] D. Raghavarao. *Constructions and Combinatorial Problems in Design of Experiments*. In Wiley Series in Probability and Statistics, John Wiley and Sons, New York-Sydney-London, 1971.

[200] F. Rothlauf. Representations for Genetic and Evolutionary Algorithms. Second Edition. Springer-Physica-Verlag, 2006.

[201] D. G. Sarvate and J. Seberry. Encryption methods based on combinatorial designs. *Ars Combinatoria* **21-A** (1986), 237–246.

[202] G. Sburlati. On the parity of permanents of circulant matrices. *Linear Algebra and its Applications* **428** (2008), 1949–1955.

[203] B. Schneier. *Applied Cryptography*. Second Edition. John Wiley and Sons, New York, 1996.

[204] M. R. Schroeder. *Number Theory in Science and Communication*. Springer-Verlag, New York, 1984.

[205] J. Seberry Wallis. A skew-Hadamard matrix of order 92. *Bulletin of the Australasian Mathematical Society* **5** (1971), 203–204.

[206] J. Seberry and R. Craigen. Orthogonal designs. In *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), pp. 400–406. , CRC Press, Boca Raton, Fla., 1996.

[207] J. R. Seberry, B. J. Wysocki and T. A. Wysocki. On a use of Golay sequences for asynchronous DS CDMA applications. In *Advanced Digital Signal Processing for Communication Systems*, T. A. Wysocki, M. Darnell, and B. Honary (Eds.), pp. 182–196. Kluwer Academic Pulbishers, Boston, Dordrecht, London, 2002.

[208] J. Seberry and M. Yamada. Hadamard matrices, sequences and block designs. In *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson (Eds.), pp. 431–560. J. Wiley and Sons, New York, 1992.

[209] J. Seberry Wallis. On supplementary difference sets. *Aequationes Mathematicae* **8** (1972), 242–257.

[210] J. Seberry Wallis. A note on supplementary difference sets. *Aequationes Mathematicae* **10** (1974), 46–49.

[211] G. E. Séguin and G. Drolet. *The Theory of 1-Generator Quasi-cyclic Codes*, Dept. Elec. Comp. Eng., Royal Military College of Canada, Kingston, ON, Canada, 1990.

[212] N. Sendrier. Linear codes with complementary duals meet the Gilbert-Varshamov bound. *Discrete Mathematics* **285** (2004), 345–347.

[213] A. Shamir. How to share a secret. *Communications of the ACM* **22** (1979), 612–613.

[214] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society* **43** (1938), 377–385.

[215] R. C. Singleton. Maximum distance separable q-nary codes. *IEEE Transactions on Information Theory* **10** (1964), 116–118.

[216] M. Sipser. *Introduction to the Theory of Computation*. Second Edition. Thomson Learning Inc., Boston, Massachusetts, 2006.

[217] N. J. A. Sloane. Self-dual codes and lattices, Relations between combinatorics and other parts of mathematics. American Mathematics Society **34** (1979), pp. 273–308. (Proceedings of Symposium on Pure Mathematics).

[218] E. Spence. Classification of Hadamard matrices of order 24 and 28. *Discrete Mathematics* **140** (1995), 185–243.

[219] W. Stallings. *Cryptography and Network Security: Principles and Practices*. Third Edition. Prentice Hall, 2003.

[220] R. G. Stanton and D. A. Sprott. A family of difference sets. *Canadian Journal of Mathematics* **10** (1958), 73–77.

[221] D. R. Stinson. *Cryptography : Theory and Practice*. Third Edition. In Series: Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Boca Raton, 2006.

[222] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tilework, and the theory of numbers. *Philosophical Magazine* **34** (1867), 461–475.

[223] B. Tang and C. F. J. Wu. A method for constructing supersaturated designs and its $E(s)^2$-optimality. *Canadian Journal of Statistics* **25** (1997), 191–201.

[224] J.A. Thas. Finite geometries, varieties and codes, *Proceedings of the International Congress of Mathematicians*, pp. 397–408. Extra vol. **III**, Berlin, 1998.

[225] H. van Tilborg. On quasi-cyclic codes with rate $1/m$. *IEEE Transactions on Information Theory* **24** (1978), 628–630.

[226] V. D. Tonchev. Codes. In *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, J.H., (Eds.), pp. 517–543. CRC Press, Boca Raton, Fla., 1996.

[227] R. L. Townsend and E. J. Weldon, Jr. Self-orthogonal quasi-cyclic codes. *IEEE Transactions on Information Theory* **13** (1967), 183–195.

[228] M. A. Tsfasman and S. G. Vladut. Algebraic-Geometric Codes, Mathematics and Its Applications. Kluwer Academic Publishers, Dordrecht, 1991.

[229] R. J. Turyn. Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encoding. *Journal of Combinatorial Theory - Series A* **16** (1974), 313–333.

[230] A. Vardy. Algorithmic complexity in coding theory and the minimum distance problem. *Proceedings of the 29th annual ACM symposium on Theory of computing*, ACM, 1997, pp. 92–109.

[231] W. D. Wallis, A. P. Street and J. Seberry, Wallis. *Combinatorics: Room Squares, Sum-Free Sets, Hadamard matrices*. In Series: Lecture Notes in Mathematics **292**, Springer-Verlag, 1972.

[232] G. Weathers and E. M. Holiday. Group-complementary array coding for radar clutter rejection. *IEEE Transactions on Aerospace and Electronic Systems* **19** (1983), 369–379.

[233] E. J. Weldon, Jr. Long quasi-cyclic codes are good. *IEEE Transactions on Information Theory* **13** (1970), 130.

[234] A. L. Whiteman. A family of difference sets. *Illinois Journal of Mathematics* **6** (1962), 107–121.

[235] P. C. Winter, G. I. Hickey and H. L. Fletcher. Instant Notes in Genetics. Third Edition. Springer, New York BIOS Scientific Publishers, Taylor and Francis Ltd., 2006.

[236] C. H. Yang. On hadamard matrices constructible by two circulant submatrices. *Mathematics of Computation* **25** (1971), 181–186.

[237] C. H. Yang. Hadamard matrices and δ-codes of length 3n. *Proceedings of the American Mathematical Society* **85** (1982), 480–482.

[238] C. H. Yang. A composition theorem for δ-codes. *Proceedings of the American Mathematical Society* **89** (1983), 375–378.

[239] C. H. Yang. Lagrange identity for polynomials and δ-codes of lengths 7t and 13t. *Proceedings of the American Mathematical Society* **88** (1983), 746–750.

[240] C. H. Yang. On composition of four-symbol δ-codes and Hadamard matrices. *Proceedings of the American Mathematical Society* **107** (1989), 763–776.

[241] R. K. Yarlagadda and J. E. Hershey. *Hadamard Matrix Analysis and Synthesis: With Applications to Communications and Signal/Image Processing*. Kluwer Acad. Pub., Boston, 1997.

Κατάλογος Αλγορίθμων

Κατάλογος Πινάκων

Κατάλογος Σχημάτων