ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Τομέας Μαθηματικών

ΠΟΛΛΑΠΛΗ ΠΡΟΣΠΕΛΑΣΗ ΜΕ ΔΙΑΙΡΕΣΗ ΚΩΔΙΚΑ ΚΑΙ ΟΠΤΙΚΟΙ ΟΡΘΟΓΩΝΙΟΙ ΚΩΔΙΚΕΣ

Διπλωματική Εργασία

Δημητροπούλου Μαρία

Επιβλέπων Καθηγητής

Χρήστος Κουκουβίνος (Καθηγητής Ε.Μ.Π)

ΠΟΛΛΑΠΛΗ ΠΡΟΣΠΕΛΑΣΗ ΜΕ ΔΙΑΙΡΕΣΗ ΚΩΔΙΚΑ ΚΑΙ ΟΠΤΙΚΟΙ ΟΡΘΟΓΩΝΙΟΙ ΚΩΔΙΚΕΣ

Διπλωματική Εργασία

Δημητροπούλου Μαρία

Αθήνα 2011

Τριμελής Εξεταστική Επιτροπή

Χρήστος Κουκουβίνος

Καθηγητής Ε.Μ.Π. (Επιβλέπων Καθηγητής)

_____

Αλέξανδρος Παπαϊωάννου

Αν. Καθηγητής Ε.Μ.Π.

_____

Πέτρος Στεφανέας

Λέκτορας Ε.Μ.Π.

_____

Στους γονείς μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής μου κ. Χ. Κουκουβίνο, γιατί μου έδωσε τη δυνατότητα να ασχοληθώ με τα OCDMA συστήματα και τους οπτικούς ορθογώνιους κώδικες. Έχοντας ως βασικό υπόβαθρο, κάποια συγγράμματα του καθηγητή μου, Χ. Κουκουβίνου, κατάφερα να ολοκληρώσω την εργασία αυτή. Θα ήθελα επίσης να ευχαριστήσω τον υποψήφιο διδάκτορα Δ. Σίμο για τη συνεχή καθοδήγηση και ενθάρρυνση.

Δημητροπούλου Μαρία

2011

Εισαγωγή

Στην εργασία αυτή θα αναδιπλωθούν τα οπτικά συστήματα πολλαπλής προσπέλασης με διαίρεση κώδικα και οι κατασκευές των οπτικών ορθογώνιων κωδίκων.

Η εργασία χωρίζεται σε δύο μέρη.

Το πρώτο μέρος πραγματεύεται με την οπτική πολλαπλή προσπέλαση με διαίρεση κώδικα (OCDMA), τα τεχνικά χαρακτηριστικά και τις ταξινομήσεις των συστημάτων. Επιπλέον, αναφέρονται τα συστήματα και τα δίκτυα που αντικατοπτρίζουν επαρκώς τα τρέχοντα παγκόσμια αποτελέσματα από έρευνες για OCDMA θεωρίας και πειραμάτων.

Το δεύτερο μέρος χωρίζεται σε τέσσερα κεφάλαια.

Στο πρώτο κεφάλαιο παρατίθενται βασικές έννοιες, στις οποίες βασίζεται όλη η εργασία.

Στο δεύτερο κεφάλαιο θα παρουσιαστούν όρια πληθικότητας, διάφορες κατασκευές (όπως συνδυαστικές, προβολικής γεωμετρίας, αλγεβρικές και αναδρομικές) και θα αναφερθούν παραδείγματα για σταθερού βάρους συμμετρικούς OOCs.

Στο τρίτο κεφάλαιο θα παρουσιαστούν όρια πληθικότητας, διάφορες κατασκευές και θα αναφερθούν κατασκευασμένα παραδείγματα για σταθερού βάρους ασύμμετρους OOCs.

Στο τέταρτο κεφάλαιο μελετώνται ξεχωριστά OOCs μεταβλητού βάρους. Συγκεκριμένα, οι OOCs με βάρος τέσσερα και οι OOCs με βάρος πέντε.

Περιεχόμενα

Βιβλιογραφία υπάρχει στο τέλος της κάθε θεματικής ενότητας.

1ο Μέρος : Πολλαπλή Προσπέλαση με Διαίρεση Κώδικα

Επικοινωνία - Δίκτυα

Η ανάγκη για επικοινωνία ξεκίνησε με την ένταξη των ανθρώπων σε κοινωνίες. Οι άνθρωποι ήθελαν να επικοινωνούν μεταξύ τους και να ενημερώνονται για γεγονότα και καταστάσεις που διαδραματίζονταν ακόμα και σε μεγάλες αποστάσεις. Η πρόσβαση στην γνώση και την πληροφορία είναι πλέον δικαίωμα όλων και επιτυγχάνεται ευκολότερα μέσω των δικτύων. Η αλματώδης πρόοδος που σημειώνεται στον τομέα της τεχνολογίας, και η διαρκής αναζήτηση του ανθρώπου για ποιότητα στην επικοινωνία οδηγούν στη συνεχή εξέλιξη των τηλεπικοινωνιακών συστημάτων.

Από αρχαιοτάτων χρόνων, οι άνθρωποι κάποιες φορές επιδίωκαν μετάδοση πληροφοριών χρησιμοποιώντας κώδικες επικοινωνίας.

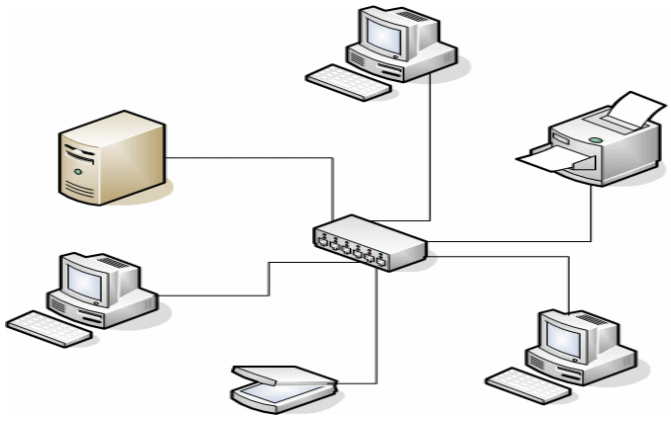
Ο Αισχύλος στο έργο του «Αγαμέμνων» περιγράφει πως η είδηση της πτώσης της Τροίας, μεταδόθηκε στις Μυκήνες, χρησιμοποιώντας το σύστημα φρυκτωριών (σύστημα επικοινωνίας). Οι ιθαγενείς της Αφρικανικής ζούγκλας επικοινωνούσαν με ήχους τυμπάνων και οι ινδιάνοι της Αμερικής επικοινωνούσαν με σήματα καπνού. Στον 20ο αιώνα οι άνθρωποι έχουν εξασφαλίσει την απομακρυσμένη επικοινωνία και τη μετάδοση της πληροφορίας μέσω του τηλεφωνικού δικτύου, του ταχυδρομικού δικτύου, των τηλεοπτικών και ραδιοφωνικών δικτύων, καθώς και μέσω δικτύων των ηλεκτρονικών υπολογιστών.

Δίκτυο Υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων, το οποίο συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές και περιφερειακές συσκευές. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες.

Σκοπός των Δικτύων

Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε υλικό (hardware), όπως υπολογιστές, εκτυπωτές, plotters, σκληροί δίσκοι είτε λογισμικό (software), όπως δεδομένα, προγράμματα εφαρμογών, υπηρεσίες.



Σύνδεση υπολογιστών και περιφερειακών συσκευών

Μετάδοση Πληροφορίας Δικτύων

Κάθε πληροφορία μεταδίδεται ως ψηφιακό σήμα μέσα από ένα σύνδεσμο, που ονομάζεται κανάλι. Ψηφιακό σήμα (digital signal) καλείται το σήμα που λαμβάνει διακριτές τιμές. Πολλές φορές για ευκολία γίνεται αναφορά στα bits πληροφορίας και όχι στο σήμα που μεταδίδεται. Εκτός από το ψηφιακό σήμα, υπάρχει και το αναλογικό σήμα (analog signal), το οποίο έχει συνεχές πεδίο τιμών. Η μετάδοση του αναλογικού σήματος μέσα σ' ένα σύνδεσμο είναι εφικτή, αλλά δεν είναι αποδοτική. Το αναλογικό σήμα αλλοιώνεται εύκολα από το θόρυβο που υπάρχει στο κανάλι. Θόρυβος, καλείται οποιοδήποτε σήμα το οποίο παρεισφύει στο κανάλι και αλλοιώνει το σήμα πληροφορίας. Το ψηφιακό σήμα είναι ανθεκτικό στο θόρυβο επειδή λαμβάνει διακριτές τιμές, και γίνεται με ασφάλεια η μετάδοση της πληροφορίας μέσω κρυπτογράφησης. Συνεπώς, όλα τα δίκτυα υπολογιστών είναι ψηφιακά.

Η μετάδοση της πληροφορίας σ' ένα κανάλι γίνεται εφόσον κωδικοποιηθεί. Η κωδικοποίηση (encoding) είναι η διαδικασία μετατροπής της πληροφορίας σε ψηφιακό σήμα για να μεταδοθεί σ' ένα κανάλι. Ένας κώδικας πρέπει να:

- επιτρέπει το συγχρονισμό του αποστολέα και του παραλήπτη,
- επιτρέπει τον εντοπισμό και τη διόρθωση σφαλμάτων (error detection and error correction) που παρουσιάζονται κατά τη μετάδοση της πληροφορίας
- εξοικονομεί ενέργεια και
- χαρακτηρίζεται από ανθεκτικότητα στο θόρυβο.

Κάθε φυσικό κανάλι χαρακτηρίζεται από μία συνάρτηση μεταφοράς, η οποία εξαρτάται από το είδος και το μήκος του. Πολλές φορές, το εύρος ζώνης συχνοτήτων του καναλιού εντοπίζεται σε υψηλές συχνότητες ενώ, το φάσμα ενός σήματος πληροφορίας σε χαμηλές. Στόχος, είναι λοιπόν, η δημιουργία ενός σήματος πληροφορίας σε υψηλότερες συχνότητες ώστε να είναι δυνατή η μετάδοση μέσα στο κανάλι. Αυτό επιτυγχάνεται με τη χρησιμοποίηση ενός περιοδικού σήματος υψηλής συχνότητας που ονομάζεται φέρον σήμα (carrier wave). Η παραγωγή ενός σήματος πληροφορίας που προκύπτει από τη μεταβολή μιας ή και περισσότερων παραμέτρων ενός φέροντος σήματος (όπως πλάτος, συχνότητα, φάση) που είναι κατάλληλο για μετάδοση, λέγεται διαμόρφωση (modulation). Η αντίστροφη διαδικασία ονομάζεται αποδιαμόρφωση (demodulation). Η μονάδα διαμόρφωσης και αποδιαμόρφωσης ενός σήματος ονομάζεται modem (Modulator – DEModulator).

Το εύρος ζώνης και η καθυστέρηση είναι οι βασικές παράμετροι αξιολόγησης ενός συνδέσμου και γενικότερα ενός δικτύου. Η σημασία της κάθε παραμέτρου εξαρτάται από τον όγκο των δεδομένων που μεταδίδει μια εφαρμογή και από το μήκος της επικοινωνίας.

Για κάθε κανάλι υπάρχει ένα όριο στο ρυθμό με τον οποίο μπορεί να μεταδοθούν τα δεδομένα. Το όριο αυτό ονομάζεται μέγιστη ταχύτητα μετάδοσης (transmission speed) ή εύρος ζώνης (bandwidth) του καναλιού. Υπάρχει πολλές φορές σύγχυση στη χρήση των όρων «εύρος ζώνης» και «εύρος ζώνης συχνοτήτων».

Η μετάδοση της πληροφορίας σε ένα κανάλι χαρακτηρίζεται από καθυστέρηση (delay). Αυτή διαφοροποιείται στην καθυστέρηση διάδοσης (propagation delay) και την καθυστέρηση μετάδοσης (transmission delay).

Αρχιτεκτονική των Δικτύων

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι υπόλοιπες συσκευές συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες να μοιράζονται πληροφορίες.

Τα δίκτυα μπορούν να χωριστούν σε κατηγορίες, με βάση:

1. Τη γεωγραφική τους κάλυψη

    A. Δίκτυα ευρείας περιοχής ($Wide\ Area\ Networks, WAN$), που καλύπτουν αποστάσεις μερικών χιλιομέτρων (συνήθως άνω των 5 km) στην ίδια πόλη, μέχρι χιλιάδων χιλιομέτρων σε διαφορετικές πόλεις - κράτη - ηπείρους. Αποτελούνται από υπολογιστές, τηλεπικοινωνιακές συσκευές και γραμμές. Παραδείγματα τέτοιων δικτύων είναι τα δίκτυα των αεροπορικών εταιρειών, τα τραπεζικά δίκτυα, τα δημόσια δίκτυα δεδομένων.
    B. Δίκτυα μικρών αποστάσεων ή τοπικά δίκτυα ($Local\ Area\ Networks$, LAN) που καλύπτουν μικρές αποστάσεις (μερικών εκατοντάδων μέτρων ή λίγων χιλιομέτρων). Χρησιμοποιούνται από επιχείρησεις. Ο διαχωρισμός τους από τα δίκτυα ευρείας περιοχής οφείλεται στο ότι χρησιμοποιούν διαφορετικές τεχνικές λειτουργίας.
    C. Αστικά ή Μητροπολιτικά δίκτυα ($Metropolitan\ Area\ Networks, MAN$), που καλύπουν δίκτυα που δεν ξεπερνούν τα σύνορα μιας πόλης. Είναι ταχύτερα από τα τοπικά δίκτυα και μπορούν να μεταδίδουν αποδοτικότερα εικόνα, φωνή και δεδομένα.
    D. Δίκτυα προσωπικής κάλυψης ($Personal\ Area\ Networks, PAN$). Ένα τέτοιο δίκτυο χρησιμοποιείται κυρίως μεταξύ ενός προσωπικού υπολογιστή και όλων των τοπικών περιφερειακών συσκευών, όπως εκτυπωτές και scanners.

    Όλα τα δίκτυα μπορεί να είναι και ασύρματα - wireless (W).

2. Τον τηλεπικοινωνιακό φορέα εξυπηρέτησης

    A. Ιδιωτικά δίκτυα (Private Networks)
    B. Δημόσια δίκτυα (Public Networks)

3. Την τεχνική προώθησης της πληροφορίας

    A. Δίκτυα μεταγωγής (Switched)
    B. Δίκτυα ακρόασης (Broadcast)
    C. Δικτύωση (Networked)

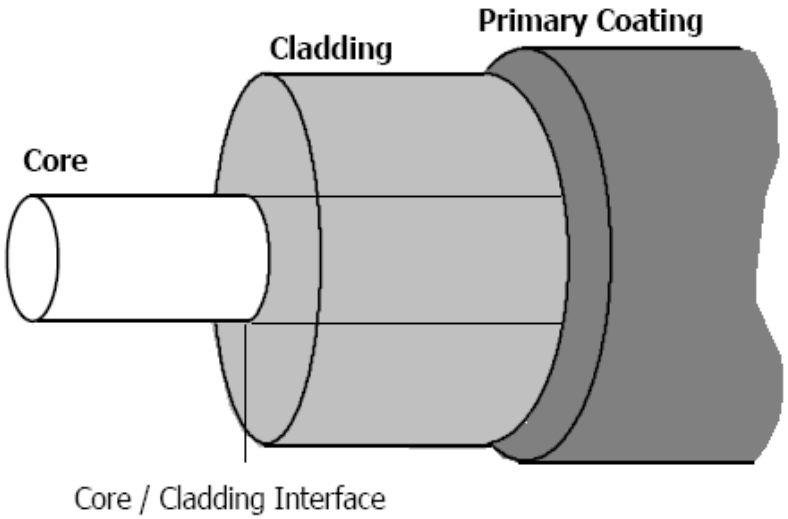
4. Το μέσο ή τον φορέα διασύνδεσής τους

    A. Ενσύρματα
    Τα πιο συνηθισμένα φυσικά μέσα είναι το ομοαξονικό καλώδιο (coaxial cable), το ζεύγος συνεστραμμένων καλωδίων (twisted pair) και οι οπτικές ίνες (optical fiber). Κάθε μέσο έχει τα δικά του φυσικά χαρακτηριστικά, εύρος ζώνης και ανοχή στον θόρυβο, επηρεάζοντας έτσι, άμεσα τον τρόπο και την ταχύτητα μετάδοσης.
    B. Ασύρματα
    Επικοινωνία μέσω ραδιοκυμάτων, μικροκυμάτων και δορυφορικά.

Το ομοαξονικό καλώδιο αποτελείται από ένα μονωμένο χάλκινο αγωγό και ένα μεταλλικό πλέγμα. Προσφέρει θωράκιση και συνεπώς μεγαλύτερη προστασία από το θόρυβο. Έχει εύρος ζώνης συχνοτήτων μέχρι 100Mbps σε αποστάσεις έως 500m. Το κόστος κατασκευής του είναι χαμηλό, αλλά μεγαλύτερο από του συνεστραμμένου ζεύγους.

Το συνεστραμμένο ζεύγος αποτελείται από ζεύγη χάλκινων αγωγών. Χαρακτηρίζεται από σχετικά μικρό εύρος ζώνης συχνοτήτων (~100Mbps σε αποστάσεις έως 100m), μεγάλη εξασθένιση σήματος και ευαισθησία στην επίδραση του θορύβου. Χρησιμοποιείται κυρίως στο τηλεφωνικό δίκτυο και σε τοπικά δίκτυα υπολογιστών (Ethernet, Token Ring).

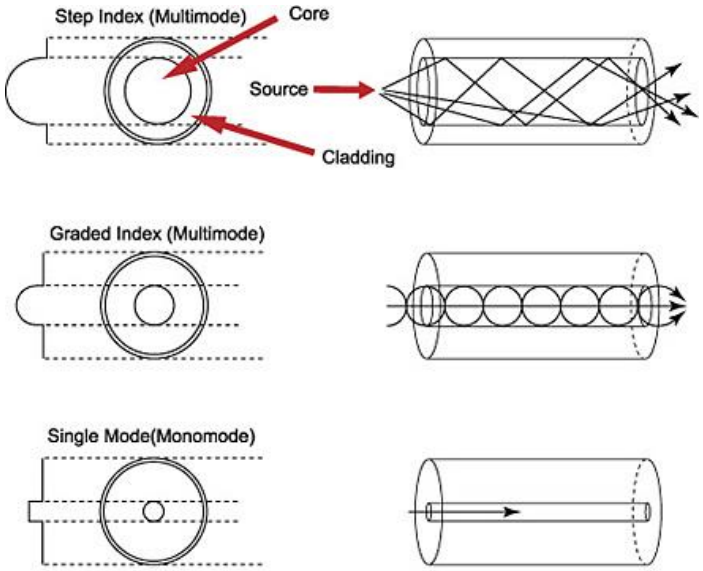
Η οπτική ίνα είναι ένας γυάλινος κυματοδηγός κυλινδρικής διατομής. Η βασική της δομή περιλαμβάνει μια κεντρική κυλινδρική ράβδο που ονομάζεται πυρήνας (core) και έναν σωλήνα, που περιβάλλει τον πυρήνα και ονομάζεται μανδύας (cladding) . Για λόγους προστασίας από εξωτερικούς παράγοντες, ο μανδύας καλύπτεται από πρωτογενή επικάλυψη πλαστικού γνωστή ως πρωτεύουσα επικάλυψη ή εξωτερικό περίβλημα (coating).



Οι οπτικές ίνες:

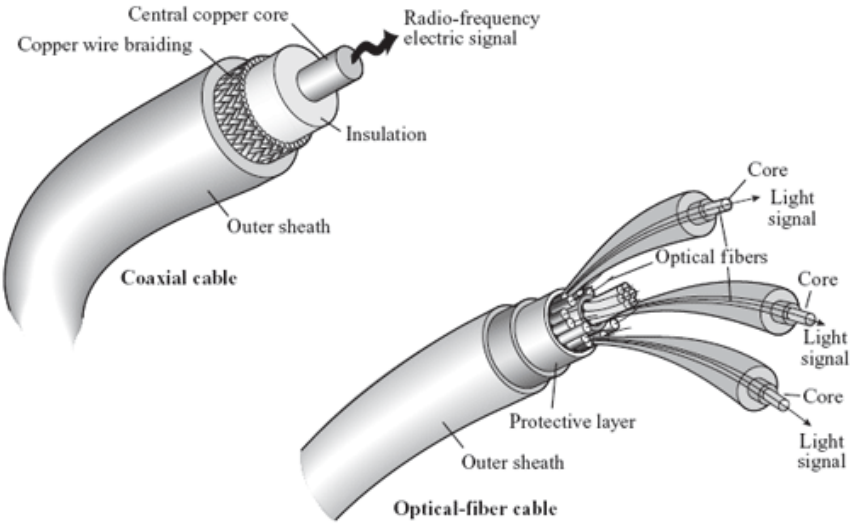
- Είναι ανεπηρέαστες από ηλεκτρομαγνητικές παρεμβολές
- Υποστηρίζουν πολύ μεγάλα BW
- Παρέχουν μεγάλη αξιοπιστία
- Έχουν πολύ υψηλό βαθμό ασφάλειας
- Καλύπτουν πολύ μεγάλες αποστάσεις

Υπάρχουν τρία είδη οπτικών ινών:



A Graphic Representation of How Light Rays Travel in Three Fiber Types

step index multi-mode fiber : πολύτροπη ίνα βηματικού δείκτη, graded index multi-mode fiber : πολύτροπη ίνα βαθμιαίου δείκτη,
single-mode fiber: μονότροπη ίνα (βηματικού δείκτη)



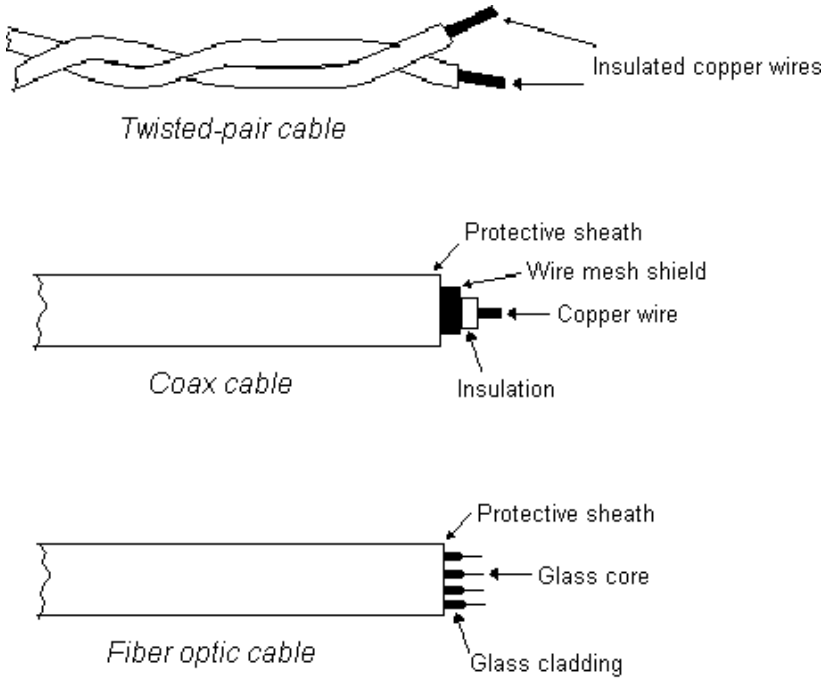
Ομοαξονικό Καλώδιο

outer sheath: πλαστικό περίβλημα, copper wire braiding: χάλκινο συρμάτινο πλέγμα
insulation: μονωτικό υλικό, central copper core: κεντρικός πυρήνας χαλκού
radio-frequency electric signal: ηλεκτρικό σήμα ραδιοσυχνοτήτων

Καλώδιο Οπτικής Ίνας

protective layer: προστατευτικό στρώμα
light signal: οπτικό σήμα

Τύποι καλωδίων



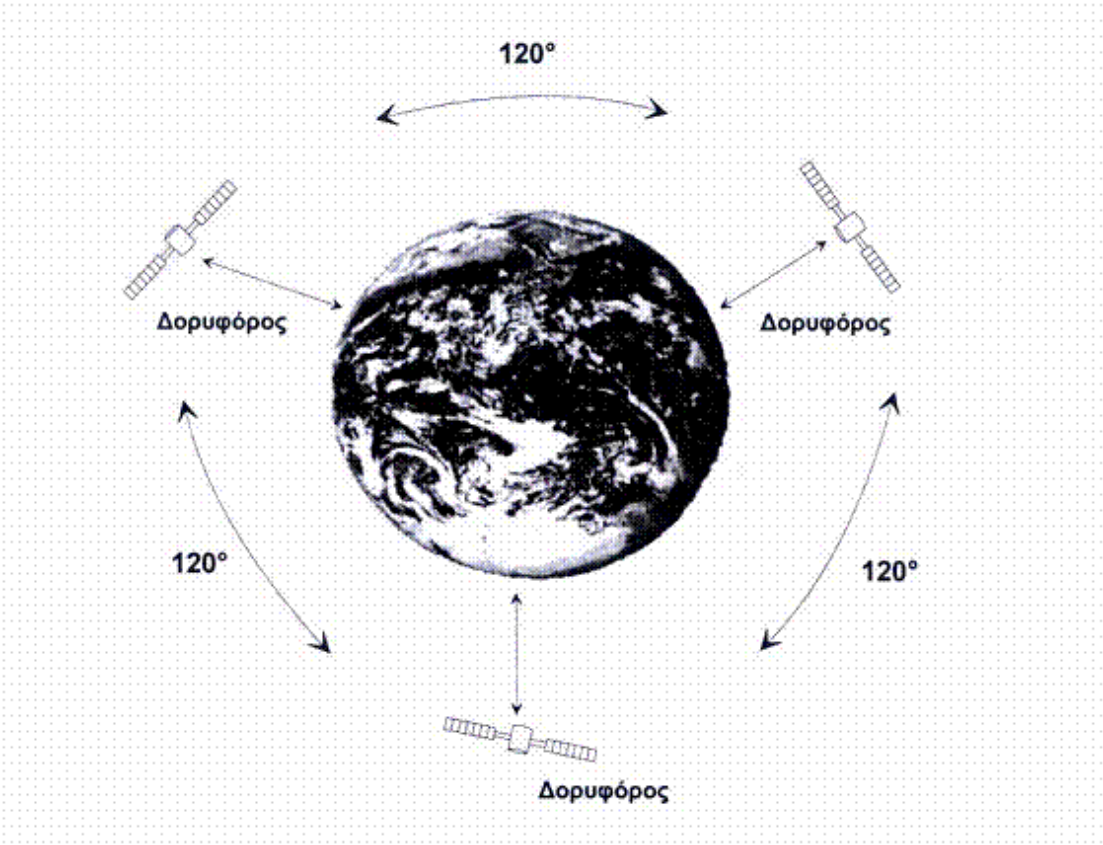
Cable types

Twisted pair cable: ζεύγος συνεστραμμένων καλωδίων
insulated copper wires: μονωτικά σύρματα χαλκού

Coax cable: κανάλι ομοαξονικού καλωδίου
protective sheath: προστατευτικό περίβλημα, wire mesh shield: περίβλημα συρμάτινου πλέγματος, copper wire: καλώδιο πυρήνα, insulation: μονωτικό υλικό

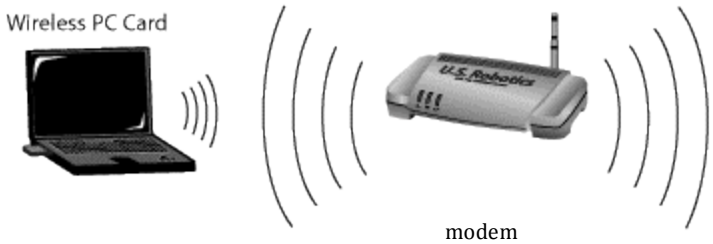
Fiber optic cable: καλώδιο οπτικής ίνας
protective sheath: προστατευτικό περίβλημα, glass cladding: γυάλινο περίβλημα, glass core: γυάλινος πυρήνας

Η μετάδοση της πληροφορίας μπορεί να γίνει και με τη χρήση των ηλεκτρομαγνητικών κυμάτων. Για τη μετάδοση χρησιμοποιείται μια περιοχή συχνοτήτων (ασύρματο κανάλι). Μπορούν να χρησιμοποιηθούν διαφορετικές περιοχές συχνοτήτων με διαφορετικά χαρακτηριστικά, όπως μεγαλύτερη εξασθένιση σε μεγαλύτερες συχνότητες και διαφορετικές αποστάσεις διάδοσης. Η ασύρματη μετάδοση έχει πολλές εφαρμογές λόγω της ευελιξίας της και χρησιμοποιείται κυρίως στα ασύρματα τοπικά δίκτυα, στα δίκτυα κινητής τηλεφωνίας και στα δορυφορικά δίκτυα.



Γεωστατικοί δορυφόροι

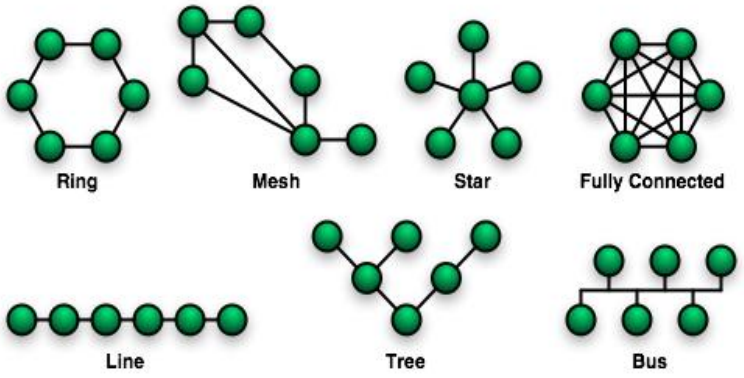
Κάθε γεωστατικός δορυφόρος καλύπτει έναν ορίζοντα 120 μοιρών και γι' αυτό το σύστημα αποτελείται από 3 γεωστατικούς δορυφόρους (και 34 επίγειους σταθμούς).



Ασύρματη σύνδεση Η/Υ και modem

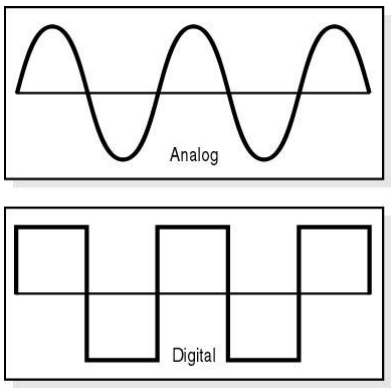
5. Τοπολογία δικτύου
   Καθορίζει τον τρόπο με τον οποίο διασυνδέονται μεταξύ τους οι συσκευές του δικτύου. Η πιο απλή είναι η σύνδεση σημείο με σημείο (γραμμής – line). Οι υπόλοιπες τοπολογίες χαρακτηρίζονται σαν δίκτυα ακρόασης, όπου κάθε κόμβος συνδέεται με όλους τους υπόλοιπους. Τέτοιες τοπολογίες είναι:

   i. αρτηρίας ή διαύλου (bus)
   ii. δακτυλίου (ring)
   iii. αστέρα (star)
   iv. δένδρου (tree)
   v. δικτυωτή (mesh)
   vi. πλήρους σύνδεσης (fully connected)



6. Τεχνική Μετάδοσης και Κωδικοποίησης των Δεδομένων.
   Η πληροφορία, προκειμένου να μεταδοθεί, πρέπει να μετατραπεί στη μορφή που το μέσο μπορεί να μεταδώσει. Οι κυριότερες τεχνικές μετάδοσης είναι:

   - βασικής / ευρείας ζώνης
   - ψηφιακού / αναλογικού σήματος
   - διαμόρφωση / αποδιαμόρφωση
   - σύγχρονη / ασύγχρονη



Αναλογικό και Ψηφιακό Σήμα

7. Ταχύτητα μετάδοσης.
   Μετρείται σε $bits/sec$ και εξαρτάται από το μέσο και την τεχνική μετάδοσης, το εύρος ζώνης και τη μέθοδο πρόσβασης στο μέσο.

8. Πρωτόκολλο επικοινωνίας
   Η λέξη «πρωτόκολλο» αναφέρεται στους κανόνες που ακολουθεί ένα δίκτυο για την αποστολή ή τη λήψη δεδομένων μεταξύ των κόμβων. Τα πιο δημοφιλή πρωτόκολλα επικοινωνιών είναι τα $ARCnet$, $Token\ Ring$, $Ethernet$. Τα πρότυπα των $Token\ Ring$ (802.5) και $Ethernet$ (802.3) είναι αποδεκτά από διεθνείς οργανισμούς τυποποίησης ($IEEE$).

   Κάθε τύπος πρωτοκόλλου έχει πλεονεκτήματα και μειονεκτήματα, ανάλογα με τον τρόπο εγκατάστασης του δικτύου, το πλήθος των δεδομένων που μεταφέρονται και τον αριθμό των σταθμών εργασίας. Τέλος, το πρωτόκολλο που επιλέγεται επηρεάζει και το είδος της καλωδίωσης που μπορεί να χρησιμοποιηθεί.

9. Τρόπος σύνδεσης Η/Υ

   - σύνδεση σημείου προς σημείο - άμεση σύνδεση (point to point)
   - σύνδεση σημείου προς πολλαπλά σημεία (point to multipoint)
   - με πολυπλεξία (multiplexing)

Πολυπλεξία (Multiplexing)

Στις τηλεπικοινωνίες και στα δίκτυα υπολογιστών, πολυπλεξία (multiplexing) λέγεται η μέθοδος, η οποία επιτρέπει σε ψηφιακά δεδομένα ή αναλογικά σήματα από διαφορετικές πηγές, να διέλθουν μέσα από το ίδιο μέσο επικοινωνίας (κανάλι). Το κανάλι μπορεί να είναι ένα καλώδιο στην ενσύρματη επικοινωνία, ή ο χώρος στην ασύρματη επικοινωνία. Με αυτόν τον τρόπο, οι πληροφορίες διαμοιράζονται σε πολλαπλούς χρήστες.

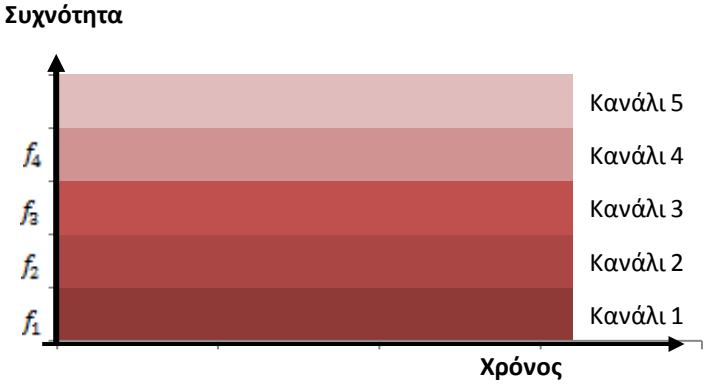
Αναφέρονται τρία είδη πολυπλεξίας:

1. $FDM - Frequency\ Division\ Multiplexing$: πολυπλεξία με διαίρεση συχνότητας. Κάθε σήμα πληροφορίας χρησιμοποιεί διαφορετική ζώνη συχνοτήτων,
2. $TDM - Time\ Division\ Multiplexing$: πολυπλεξία με διαίρεση χρόνου. Κάθε σήμα πληροφορίας καταλαμβάνει διαφορετική χρονοθυρίδα.
3. $CDM - Code\ Division\ Multiplexing$: πολυπλεξία με διαίρεση κώδικα. Κάθε σήμα πληροφορίας διακρίνεται από τα άλλα, με ειδικό κώδικα.

Frequency Division Multiplexing

Η πολυπλεξία διαίρεσης συχνότητας είναι τεχνολογία για την μετάδοση αναλογικών σημάτων. Το εύρος ζώνης του επικοινωνιακού καναλιού διαιρείται σε ζώνες συχνοτήτων που ονομάζονται κανάλια. Η μετάδοση των σημάτων γίνεται ταυτόχρονα στα κανάλια που έχουν καθοριστεί.

Παράδειγμα πολυπλεξίας διαίρεσης συχνότητας είναι η μετάδοση τηλεοπτικών και ραδιοφωνικών σημάτων. Ο κάθε ραδιοφωνικός ή τηλεοπτικός σταθμός έχει καθορισμένο εύρος ζώνης όπου μπορεί να εκπέμψει, το οποίο αποκαλείται συχνότητα σταθμού. Όλοι οι σταθμοί εκπέμπουν παράλληλα. Περιορίζουν, όμως, τις εκπομπές τους στις ζώνες συχνοτήτων οι οποίες είναι διαφορετικές και έχουν καθοριστεί (συχνότητες σταθμών) από κάθε πολυπλέκτη. Το μέσο μετάδοσης είναι η ατμόσφαιρα, και η εκπομπή γίνεται με ηλεκτρομαγνητικά κύματα.



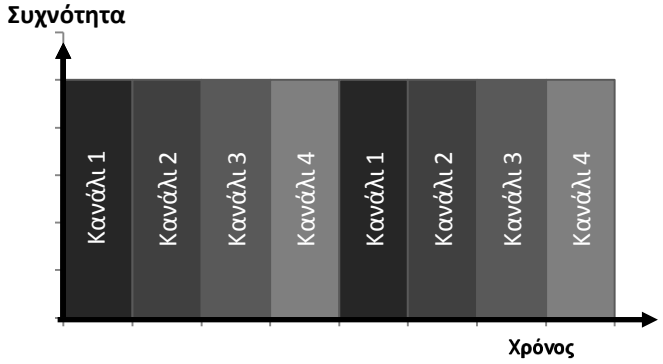
Σε κάθε συχνότητα αντιστοιχεί ένα διαφορετικό κανάλι, μια διαφορετική ζώνη.

Σημείωση

Η πολυπλεξία με διαίρεση μήκους κύματος ($WDM - Wavelength\ Division\ Multiplexing$) είναι ειδική μορφή του FDM με εφαρμογή στις οπτικές ίνες.

Time Division Multiplexing

Η πολυπλεξία διαίρεσης χρόνου είναι τεχνολογία ψηφιακής μετάδοσης σημάτων και χρησιμοποιείται κυρίως στην επικοινωνία υπολογιστών. Ο χρόνος διαιρείται σε χρονοθυρίδες (timeslots) και η μεταφορά των σημάτων γίνεται κυκλικά. Για να σταλούν αναλογικά σήματα, με την πολυπλεξία διαίρεσης χρόνου, γίνεται δειγματοληψία των σημάτων και αποστέλλονται κυκλικά τα δείγματα. Με αυτόν τον τρόπο, δεδομένα διαφορετικών πηγών πολυπλέκονται χρονικά και μεταδίδονται στην ίδια γραμμή (μέσο μετάδοσης). Αυτή η μέθοδος δεν χρησιμοποιείται συχνά.



Σημείωση

Η στατιστική πολυπλεξία (*Statistical Multiplexing*) είναι μια μορφή πολυπλεξίας διαίρεσης χρόνου και χρησιμοποιείται στα δίκτυα υπολογιστών. Σε ένα δίκτυο υπολογιστών όταν χρησιμοποιείται πολυπλεξία διαίρεσης χρόνου με σταθερές χρονοθυρίδες, η επικοινωνία των Η/Υ δεν γίνεται με βέλτιστο τρόπο δηλαδή, δεν εκμεταλλεύονται όλοι οι πόροι (γραμμές) του δικτύου. Αυτό συμβαίνει γιατί, σε ένα δίκτυο οι ηλεκτρονικοί υπολογιστές δεν στέλνουν ή λαμβάνουν δεδομένα ταυτόχρονα και δεν έχουν τις ίδιες ταχύτητες επικοινωνίας κάθε χρονική στιγμή. Στην στατιστική πολυπλεξία ο χρόνος μετάδοσης δεν διαιρείται σε ίσες χρονοθυρίδες, αλλά, μοιράζεται σε χρονοθυρίδες διαφορετικού μεγέθους, ανάλογα με τις τρέχουσες ανάγκες επικοινωνίας των υπολογιστών στο δίκτυο.

Code Division Multiplexing

Μία από τις μεθόδους πολυπλεξίας είναι η πολυπλεξία με διαίρεση κωδίκων. Τα δίκτυα στα οποία επιτρέπεται η προσπέλαση με τη μέθοδο αυτή ονομάζονται δίκτυα πολλαπλής προσπέλασης με διαίρεση κώδικα (*code division multiple access – CDMA*). Η μέθοδος αυτή χρησιμοποιεί τεχνολογία εξάπλωσης φάσματος και συγκεκριμένη κωδικοποίηση. Όταν παράγεται ένα σήμα με συγκεκριμένο εύρος ζώνης συχνοτήτων, τότε αυτό εξαπλώνεται στο χώρο και καταλήγει με μορφή κώδικα σε πολλούς χρήστες που χρησιμοποιούν το ίδιο κανάλι. Σε κάθε σήμα ανατίθεται ένας κώδικας. Οι κώδικες που ανατίθενται σε διαφορετικά σήματα είναι συνήθως ορθογώνιοι ή ψευδοτυχαίοι, ώστε να ελαχιστοποιούνται οι παρεμβολές ανάμεσα σε δύο σήματα. Οι παρεμβολές οφείλονται τόσο σε ασύγχρονες μεταδόσεις όσο και στη διάλειψη πολλαπλών διαδρομών. Η μείωση της ισχύος του σήματος ονομάζεται διάλειψη, και έχει σαν αποτέλεσμα την μη ανάκτηση των δεδομένων από τον δέκτη.

Συμπέρασμα

Στους ηλεκτρονικούς υπολογιστές η μετάδοση δεδομένων γίνεται σποραδικά και άρα η πολυπλεξία διαίρεσης κώδικα είναι πιο κατάλληλη.

OCDMA Τεχνολογία

Το οπτικό δίκτυο μπορεί να εφαρμόσει υπερβολικά υψηλή ταχύτητα μετάδοσης, δρομολόγησης και μεταγωγής δεδομένων σ' ένα οπτικό πεδίο. Μπορεί επίσης να πετύχει τη διαβίβαση διάφορων μορφών δεδομένων με πρωτόκολλα τα οποία αυξάνουν την ευελιξία και τη λειτουργικότητα του δίκτυο.

Η OCDMA τεχνολογία είναι μία από τις πολλά υποσχόμενες τεχνολογίες για την υλοποίηση όλων των οπτικών δικτύων. Έχει τη δυνατότητα να αξιοποιεί το εύρος ζώνης της οπτικής ίνας και επωφελείται από την επικράτηση του ασύρματου CDMA, όπου σ' αυτό γίνεται ευέλικτη και αποτελεσματική η κατανομή των συνδρομητών ανάλογα με τις πηγές φάσματος, χρόνου και χώρου, χωρίς να υπάρχουν παρεμβολές και υποκλοπές.

Η OCDMA είναι μια κατηγορία πολυπλεξίας και δικτυακής τεχνολογίας που κωδικοποιεί και αποκωδικοποιεί σήματα, έτσι ώστε, αυτά να μπορούν εύκολα να πολυπλέκονται, να δρομολογούνται και να μετατρέπονται . Έχει πολλά πλεονεκτήματα, όπως:

- η ασύγχρονη τυχαία πρόσβαση,
- η απλή διαχείριση,
- η ευέλικτη δικτύωση,
- η καλή συμβατότητα με WDM και TDM,
- η καταιγιστική κίνηση (bursty traffic),
- η υποστήριξη πολλαπλών υπηρεσιών,
- η παροχή κάποιας υποτυπώδους εμπιστευτικότητας στη διαβίβαση των δεδομένων

Είναι, συνεπώς, μια πολύ σημαντική τεχνολογία για να εφαρμοστεί σε οπτικά δίκτυα, δίκτυα μητροπολιτικής περιοχής και σε μεταγωγές δικτύων.

Η ιστορία της OCDMA τεχνολογίας είναι σχετικά πρόσφατη και ξεκινά με την πρώτη εισήγηση και την πρώτη πειραματική επίδειξη. Στο παρελθόν, οι απαιτήσεις για τη χωρητικότητα της πληροφορίας ήταν πολύ λιγότερες, και η έκταση της ανάπτυξης των επικοινωνιακών δικτύων ήταν περιορισμένη, γι' αυτό, η σημερινή και αυξημένη λειτουργικότητα των δικτύων δεν ήταν απαραίτητη. Την ίδια στιγμή, η WDM τεχνολογία παρείχε υπόγεια μετάδοση και μεταγωγή του μήκος κύματος δεδομένων, με υπερβολικά υψηλή ταχύτητα. Η OCDMA τεχνολογία παρέμεινε έξω από τις έρευνες οπτικής επικοινωνίας που τότε επικρατούσαν, χρονικό διάστημα, αρκετά μεγάλο. Αργότερα, με τη ραγδαία εξάπλωση της γνώσης και την παγκόσμια εμβέλεια του διαδικτύου, η δυσαρμονία στη μεταφορά δεδομένων και στην πρόσβαση δικτύων γίνεται ένα σοβαρό ζήτημα.

Είναι φανερό πλέον, ότι οι WDM και TDM τεχνολογίες αδυνατούν να λύσουν αυτά τα τρέχοντα ζητήματα και άρα είναι ανεπαρκής. Αντιθέτως, η μεγάλη ευελιξία της δικτύωσης των OCDMA, και οι πολύ καλές συμπληρωματικές ιδιότητες των OCDMA με WDM και TDM αναγνωρίζονται. Ταυτόχρονα, λόγω της ταχείας εξέλιξης της οπτικής τεχνολογίας, όλες οι θεωρίες της OCDMA τεχνολογίας έχουν μετατραπεί σε δυναμικές ζώνες έρευνας, οι οποίες αναμένεται να τονώσουν τη OCDMA ανάπτυξη.

Τα πολλά πλεονεκτήματα της OCDMA τεχνολογίας και οι νέες απαιτήσεις για τη λειτουργικότητα των επερχόμενων οπτικών δικτύων καθιστούν την OCDMA τεχνολογία ελπιδοφόρα, πολλά υποσχόμενη και με προοπτικές εφαρμογής. Τα τελευταία χρόνια η OCDMA έχει καταφέρει να γίνει η δυναμικότερη ζώνη έρευνας στην τεχνολογία της οπτικής επικοινωνίας. Η επέκταση των εφαρμογών της OCDMA τεχνολογίας, θα επιτευχθεί εφόσον γίνουν μεγάλες προσπάθειες από τους ερευνητές.

Τεχνικά Χαρακτηριστικά και Ταξινομήσεις Συστήματος των OCDMA

Η πολλαπλή προσπέλαση με διαίρεση κώδικα (OCDMA) έχει γίνει μια πολλά υποσχόμενη τεχνολογία για να εφαρμοστούν στην πράξη, όλες οι οπτικές επικοινωνίας και δικτύωσης που χρησιμοποιούν άμεσα οπτική επεξεργασία σήματος. Συνδυάζει τα πλεονεκτήματα ηλεκτρικών CDMA με την υπεροχή του εύρους ζώνης των οπτικών ινών και των οπτικών σημάτων των συσκευών επεξεργασίας. Τα παθητικά οπτικά δίκτυά πρόσβασης, LAN και WAN, μπορούν να δημιουργηθούν με τη χρήση OCDMA τεχνολογίας. Ο συνδυασμός OCDMA με WDM ή και με TDM μπορεί να ενισχύσει το σήμα πολυπλεξίας και τη μεταγωγή ετικέτας (πρωτοκόλλου) πέρα από το συνδυασμό OCDMA με WDM ή και με IP (συμβατικό δίκτυο) στο WAN, με το οποίο μπορεί να βελτιωθεί η δυνατότητα μεταφοράς και μετατροπής του δικτύου, μπορεί να ενισχυθεί η ευελιξία του δικτύου και μπορεί να είναι αυξημένη η απόδοση του δίκτυο επικοινωνίας.

Τεχνικά Χαρακτηριστικά OCDMA

1. Στα OCDMA μπορεί να εφαρμοστεί υψηλή ταχύτητα μετάδοσης, μεταφοράς και προσθήκης δεδομένων χρησιμοποιώντας όλα τα οπτικά σήματα επεξεργασίας. Μ' αυτόν τον τρόπο, μπορούν να υλοποιηθούν όλες οι οπτικές επικοινωνίας και όλες οι οπτικές δικτύωσης και να ξεπεραστούν οι συνέπειες της συμφόρησης, η οποία υπάρχει σε κόμβους του παραδοσιακού δικτύου.
2. Οι συνδρομητές μπορούν να έχουν πρόσβαση στο δίκτυο, τυχαία, και το δίκτυο μπορεί να έχει ευνοϊκή χωρητικότητα. Το πρότυπο της δικτύωσης είναι πολύ ευέλικτο.
3. Στα OCDMA δεν χρειάζεται προσωρινή αποθήκευση στην σειρά, επειδή χρησιμοποιείται το πρωτόκολλο tell-to-go.
4. Τα OCDMA δίκτυα μπορούν να εκχωρήσουν δυναμικά το εύρος ζώνης, να εφαρμόσουν την εκχώρηση του εύρους ζώνης με διαφορετική επιδεξιότητα, και να χρησιμοποιήσουν αποτελεσματικά το εύρος ζώνης οπτικών δικτύων .
5. Η κίνηση, το πρωτόκολλο και η τοπολογία του δικτύου είναι ολοφάνερη στο OCDMA δίκτυο. Τα OCDMA μπορούν να υποστηρίξουν μεταβλητή κίνηση του ρυθμού των bit και μπορούν εύκολα να αναβαθμίζονται και να επεκτείνονται.
6. Ένα δίκτυο OCDMA είναι κάπως ασφαλές και αινιγματικό στη διαβίβαση πληροφοριών.
7. Ένα δίκτυο OCDMA έχει απλό εξοπλισμό, και το κόστος εφαρμογής του είναι χαμηλό.
8. Τα OCDMA δίκτυα χρησιμοποιούν κατανεμημένη διαχείριση, η οποία είναι απλή και αυτό είναι βολικό για τον εντοπισμό βλάβης του δικτύου και για την προστασία και την ανάκτηση των δεδομένων.

Λόγω των πλεονεκτημάτων που προαναφέρθηκαν, τα OCDMA δίκτυα μπορούν να υποστηρίξουν πολυμέσα όπως ήχος, εικόνα, δεδομένα.

Ταξινομήσεις Συστημάτων OCDMA

Πολλοί τύποι OCDMA συστημάτων έχουν σχεδιαστεί λόγω της εντατικής έρευνας για OCDMA τα τελευταία 20 χρόνια.

Αν καταταχθούν, λαμβάνοντας υπόψιν τη φύση της επαλληλίας του οπτικού σήματος, τότε μπορούν να χωριστούν σε συνεκτικά OCDMA συστήματα και μη συνεκτικά συστήματα OCDMA. Το συνεκτικό OCDMA σύστημα χρησιμοποιεί τη συνεκτική ιδιότητα του φωτός και υλοποιείται με τη διπολική κωδικοποίηση του οπτικού σήματος, δηλαδή, την κωδικοποίηση της φάσης των οπτικών σημάτων, με την φάση του φωτός που ανιχνεύεται στους τερματικούς σταθμούς. Αυτή η μορφή πρόσθεσης του σήματος, ορίζεται ως η επαλληλία των πλατών του οπτικού σήματος. Αυτό το είδος του συστήματος OCDMA χρειάζεται να χρησιμοποιεί οπτικό παλμό πηγής με βραχύ εύρος ζώνης. Το μη συνεκτικό σύστημα OCDMA χρησιμοποιεί την παρουσία ή την απουσία οπτικού σήματος για να λαμβάνει τιμές "1" και "0" από το δυαδικό σύστημα, που είναι μονοπολικής κωδικοποίησης. Τα οπτικά σήματα ανιχνεύονται από μηχανισμούς στους τερματικούς σταθμούς. Αυτή η μορφή πρόσθεσης του σήματος, ορίζεται ως η επαλληλία της οπτικής ενέργειας. Αυτό το είδος του OCDMA συστήματος μπορεί να χρησιμοποιεί μη συνεκτικές πηγές φωτός, όπως πηγαία εκπομπή ενίσχυσης, δίοδος εκπομπής φωτός.

Εάν κατηγοριοποιηθούν, ανάλογα με τις διαφορετικές προσεγγίσεις κωδικοποίησης για οπτικά σήματα, τότε θα προκύψουν έξι είδη OCDMA συστημάτων:

1. εξάπλωση φασματικής κωδικοποίησης συστημάτων OCDMA
2. φασματικό πλάτος κωδικοποίησης συστημάτων OCDMA
3. φασματική φάση κωδικοποίησης συστημάτων OCDMA
4. φασματικός χρόνος κωδικοποίησης συστημάτων OCDMA
5. δισδιάστατα OCDMA συστήματα κωδικοποίησης χώρου, επίσης γνωστά ως spread-space encoding
6. υβριδικά OCDMA συστήματα κωδικοποίησης, αυτό το είδος χρησιμοποιεί συνδυασμό κωδικοποιήσεων που προαναφέρθηκαν.

Οι επιλογές (1), (2) και (5) αναφέρονται ως μη συνεκτικά συστήματα OCDMA, τα (3) και (4) είναι συνεκτικά συστήματα OCDMA, και η (6) μπορεί να ανήκει και στα δύο είδη.

Αν η ταξινόμηση τους γίνει ανάλογα με το συνολικό χρόνο, το μήκος κύματος και το χώρο που χρησιμοποιείται από τις πηγές, τότε μπορούν να χωριστούν σε μονοδιάστατα συστήματα, δισδιάστατα συστήματα και τρισδιάστατα συστήματα.

Οι προαναφερόμενες κατηγορίες (1), (2), (3) και (4) ανήκουν σε μονοδιάστατα συστήματα κωδικοποίησης, η (5) είναι δισδιάστατο σύστημα κωδικοποίησης, και συστήματα με περισσότερές από δύο διαστάσεις μπορούν να υλοποιηθούν στην (6). Εάν η πόλωση ληφθεί υπόψιν, τα συστήματα κωδικοποίησης τεσσάρων διαστάσεων μπορούν επίσης να επιτευχθούν.

Παρότι υπάρχουν, κωδικοποιήσεις πολλών διαστάσεων, η συγκεκριμένη εργασία θα ασχοληθεί μόνο με μονοδιάστατα συστήματα κωδικοποίησης.

Μονοδιάστατοι OCDMA Κώδικες

Σε ένα οπτικό δίκτυο πολλαπλής προσπέλασης με διαίρεση κώδικα (OCDMA), το μεταφερόμενο σήμα μεταδίδεται μέσω οπτικών ινών καθώς σχηματίζεται συσσώρευση ψευδοτυχαίων OCDMA σημάτων που κωδικοποιούνται από πολλαπλά κανάλια. Το σήμα μεταδίδεται σε κάθε κόμβο του δικτύου και ο δέκτης κάθε κόμβου αποκωδικοποιεί το σήμα. Εάν η έξοδος του αποκωδικοποιητή είναι μια συνάρτηση αυτοσυσχέτισης, τότε ο κόμβος μπορεί να εντοπίσει την πληροφορία που στάλθηκε μέσω των προαναφερθέντων ψευδοτυχαίων σημάτων. Εναλλακτικά, εάν η έξοδος του αποκωδικοποιητή είναι μια συνάρτηση ετεροσυσχέτισης (χωρίς εμφανή μέγιστη τιμή), τότε ο κόμβος δεν μπορεί να λάβει την πληροφορία. Παρόλα αυτά, προκειμένου να εφαρμοστεί η OCDMA επικοινωνία και δικτύωση, απαιτούνται κώδικες διευθύνσεων με επαρκείς επιδόσεις. Εφόσον, επιλεχθεί το σύνολο παραμέτρων ενός κώδικα, τότε ο κώδικας θα μπορεί να κατασκευαστεί κατά τέτοιο τρόπο, ώστε να έχει τόσες κωδικές λέξεις (που αντιστοιχούν στον αριθμό των κόμβων του δικτύου) όσες είναι απαραίτητες, και με αρκετά καλές συναρτήσεις αυτοσυσχέτισης και ετεροσυσχέτισης. Με αυτόν τον τρόπο, μπορεί να επιτευχθεί ακριβής συγχρονισμός και να κατασταλεί αποτελεσματικά η παρεμβολή (ονομάζεται πολλαπλή προσπέλαση παρεμβολής multiple access interference, *MAI*) άλλων κόμβων, καθώς τα σήματα αποκωδικοποιούνται. Αυτό προϋποθέτει ότι, οι κώδικες διεύθυνσης πληρούν δύο προϋποθέσεις:

1. όλες οι κωδικές λέξεις διεύθυνσης μπορούν να προσδιοριστούν εύκολα από μετατοπισμένες μορφές, και
2. όλες οι κωδικές λέξεις διεύθυνσης μπορούν να διακριθούν εύκολα από (πιθανή μετατοπισμένη μορφή) κάθε άλλη κωδική λέξη.

Σύμφωνα με τη θεωρία κωδικοποίησης, οι κωδικές λέξεις διεύθυνσης πρέπει να πληρούν τα εξής:

1. κάθε κωδική λέξη σε ένα σύνολο έχει μία υψηλή κορυφή αυτοσυσχέτισης και χαμηλούς πλευρικούς λοβούς αυτοσυσχέτισης.
2. η συνάρτηση ετεροσυσχέτισης μεταξύ μιας κωδικής λέξης και κάθε άλλης κωδικής λέξης στο ίδιο σύνολο κωδικών λέξεων διεύθυνσης είναι χαμηλή.

Από τα μέσα της δεκαετίας του 1980, μελετήθηκαν και αναπτύχτηκαν σε βάθος η θεωρία κωδικοποίησης και η τεχνολογία κωδικοποίησης των OCDMA. Από τότε, πολλά ερευνητικά επιτεύγματα έχουν καταγραφεί [1]. Οι προσεγγίσεις κωδικοποίησης των OCDMA μπορούν να διαιρεθούν σε επτά κατηγορίες, με βάση την επιλογή διάφορων πηγών φωτός , διαφόρων συστημάτων ανίχνευσης και προσεγγίσεις κωδικοποίησης.

Μπορεί να διαπιστωθεί ότι, σύμφωνα με το οπτικό σήμα που χρησιμοποιούν οι πηγές (σύμφωνες οπτικές πηγές ή ασύμφωνες οπτικές πηγές) και τις διαφορετικές μορφές των σημάτων, τα OCDMA συστήματα μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες:

i. τα συνεκτικά συστήματα OCDMA
ii. τα μη - συνεκτικά συστήματα OCDMA.

Τα συνεκτικά συστήματα OCDMA κάνουν χρήση της συνεκτικής ιδιότητας των οπτικών σημάτων και εφαρμόζουν τη διπολική κωδικοποίηση δεδομένων με την κωδικοποίηση των οπτικών σημάτων. Τα μη συνεκτικά συστήματα OCDMA χρησιμοποιώντας ή όχι σήματα φωτός, λαμβάνουν τις τιμές του δυαδικού συστήματος "1" και "0", και εφαρμόζουν μονοπολική κωδικοποίηση σημάτων στα δεδομένα. Χρησιμοποιούνται ανιχνευτές για την ανίχνευση οπτικών σημάτων σε τερματικούς σταθμούς υποδοχής. Επειδή, τα συνεκτικά συστήματα OCDMA χρησιμοποιούν διπολική κωδικοποίηση, οι διπολικοί κώδικες των ασύρματων CDMA, μπορούν άμεσα να αναπτυχθούν, όπως m-ακολουθίες, Gold κώδικες, Walsh-Hadamard κώδικες.

Λόγω της παρουσίας αρνητικών στοιχείων στους διπολικούς κώδικες, η συνάρτηση ετεροσυσχέτισης μεταξύ δύο κωδικών λέξεων μπορεί να είναι κοντά στο μηδέν, γεγονός που καθιστά την MAI πολύ μικρή. Γι' αυτό το λόγο, η απόδοση του συστήματος μπορεί να βελτιωθεί πολύ, και ο αριθμός των κόμβων του δικτύου μπορεί να αυξηθεί. Ωστόσο, ο φασματικός παλμός κωδικοποίησης σε διπολικούς κώδικες προϋποθέτει βραχύ παλμό συνεκτικών οπτικών πηγών, οι οποίες είναι ευπαθείς στη μη γραμμικότητα και στη σκέδαση των οπτικών ινών. Όσον αφορά το φασματικό πλάτος και τη φάση κωδικοποίησης, ο αριθμός των συνδρομητών σε ένα σύστημα και οι επιδόσεις του συστήματος περιορίζονται από την ανάλυση των οπτικών πλεγμάτων και σκιών [1]. Επιπλέον, το φασματικό πλάτος κωδικοποίησης απαιτεί ένα ζευγάρι συμπληρωματικών σημάτων στα άκρα πηγής και διαφορετικούς ανιχνευτές στα άκρα λήψης.

Τα μη συνεκτικά συστήματα OCDMA χρησιμοποιώντας ή όχι ενέργεια από σήματα του φωτός, λαμβάνουν τις τιμές του δυαδικού συστήματος "1" και "0" και δεν μπορούν να ανιχνεύσουν τα αρνητικά στοιχεία στους διπολικούς κώδικες. Συνεπώς, οι διπολικοί κώδικες εφαρμόζονται σε ασύρματο CDMA ενώ δεν μπορούν να εφαρμοστούν σε μη συνεκτικά OCDMA συστήματα, τα οποία μπορεί να χρησιμοποιούν μόνο μονοπολικούς κώδικες. Αυτός είναι ο λόγος για τον οποίο πρέπει να αναπτυχθούν μονοπολικοί κώδικες που ταιριάζουν κατάλληλα σε μη συνεκτικά συστήματα OCDMA. Αυτοί οι μονοπολικοί κώδικες θα πρέπει να έχουν πολύ μεγάλη πληθικότητα και πολύ καλή αυτοσυσχέτιση και ετεροσυσχέτιση. Για να εξασφαλιστεί ότι τα συστήματα μπορούν να συγχρονιστούν βολικά όταν γίνεται η πρόσβαση των χρηστών στο δίκτυο, κάθε κωδική λέξη ενός μονοπολικού κώδικα πρέπει να διαθέτει κορυφές αυτοσυσχέτισης όσο πιο υψηλές γίνεται, και πλευρικούς λοβούς αυτοσυσχέτισης όσο το δυνατόν χαμηλότερους. Ταυτόχρονα, οι συναρτήσεις ετεροσυσχέτισης πρέπει να έχουν όσο το δυνατόν χαμηλότερες τιμές για να μειώνεται η MAI. Συνεπώς, οι μονοπολικοί κώδικες θα πρέπει να είναι κώδικες σποραδικοί "1", δηλαδή, στους κώδικες ο αριθμός "0" πρέπει να είναι πολύ μεγαλύτερος από τον αριθμό "1".

Επιπλέον, σε αντίθεση με τους διπολικούς κώδικες των οποίων οι πλευρικοί λοβοί αυτοσυσχέτισης και οι συναρτήσεις ετεροσυσχέτισης πλησιάζουν το μηδέν, οι μονοπολικοί κώδικες έχουν τους καλύτερους πλευρικούς λοβούς αυτοσυσχέτισης και οι συναρτήσεις ετεροσυσχέτισής τους ισούνται με 1. Έτσι, οι καλύτεροι μονοπολικοί κώδικες μπορούν να είναι σχεδόν ορθογώνιοι αλλά, σύμφωνα με τα θετικά συστήματα δεν μπορούν να θεωρηθούν ως αληθινοί ορθογώνιοι. Ωστόσο, αυτοί οι μονοπολικοί κώδικες αποκαλούνται επίσης οπτικοί ορθογώνιοι κώδικες (OOCs).

Για λόγους υλοποίησης της μη συνεκτικότητας των OCDMA, οι μονοδιάστατοι μονοπολικοί κώδικες και οι μονοδιάστατοι κώδικες προέρχονται κυρίως από ΟΟC και αλγεβρικούς κώδικες αντιστοιχία. Οι τελευταίοι χωρίζονται σε πρώτους κώδικες ακολουθίας (prime codes PC, linear congruence codes - γραμμικοί κώδικες αναλογίας), τετραγωνικούς κώδικες αναλογίας (quadratic congruence codes QCC), κυβικούς κώδικες αναλογίας (cubic congruence codes - CCC), υπερβολικούς κώδικες αναλογίας (hyperbolic congruence codes - HCC). Οι κατασκευές των αλγεβρικών κωδίκων αναλογίας είναι σχετικά απλές αλλά η πληθικότητα τους και οι ιδιότητες αυτοσυσχέτισης και ετεροσυσχέτισης τους δεν είναι τόσο καλές όσο των ΟΟC. Η πληθικότητα ενός ΟΟC είναι μεγαλύτερη σε μονοδιάστατούς κώδικες, αλλά η κατασκευή ενός ΟΟC είναι σχετικά περίπλοκη. Επιπλέον, αν γενικευτεί ο ορισμός του ΟΟC, ο αλγεβρικός κώδικας αναλογίας μπορεί επίσης να θεωρηθεί ως ένα είδος ΟΟCs με την ευρεία έννοια του όρου.

Επειδή η πληθικότητα των μονοδιάστατων κωδίκων είναι ανάλογη με το μήκος του κώδικα, δηλαδή, τη συχνότητα εξάπλωσης του μήκους, η οποία περιορίζεται από το πλάτος του οπτικού παλμού και την καθυστέρηση που έχουν οι γραμμές της οπτικής ίνας, καθυστέρηση προετοιμασία με ταχύτητες δεδομένων των χρηστών. Συνεπώς, η πληθικότητα (που αντιστοιχεί στον αριθμό των χρηστών) των μονοδιάστατων μονοπολικών κωδίκων που μπορεί να υλοποιηθεί, είναι σχετικά μικρή με βάση την τρέχουσα κατάσταση, και γι’ αυτό, απαιτούνται μονοπολικοί κώδικες με μεγαλύτερη πληθικότητα και καλύτερες επιδόσεις, ώστε τα OCDMA δίκτυα να μπορούν να υποστηρίξουν μεγαλύτερο αριθμό ταυτόχρονων χρηστών.

Σημειώνει μεγάλη ερευνητική προσπάθεια η ανάπτυξη 2-D οπτικών ορθογώνιων κωδίκων. Οι 2-D οπτικοί ορθογώνιοι κώδικες δεν αυξάνουν το μήκος του κώδικα (μπορούν δε να το μειώνουν) και την ίδια στιγμή μεγεθύνουν το μέγεθος των κωδίκων χωρίς να υποβαθμίζουν την απόδοση τους. 2-D κώδικες (όπως, τα πολλαπλά μήκη κύματος ή οι πολλαπλές οπτικές ίνες) μπορούν να σχηματιστούν αν μια διάσταση κωδικοποίησης συνδυαστεί με τη διάσταση του χρόνου. Άλλοι τύποι κωδίκων, είναι οι 3-D κώδικες, οι οποίοι σχηματίζονται με την πρόσθεση κάποιας διάστασης κωδικοποίησης στους 2-D κώδικες.

Είναι δύσκολο να χρησιμοποιηθούν μονοδιάστατοι κώδικες για να επιτευχθεί υψηλή ταχύτητα δεδομένων επικοινωνίας και για να υπάρξουν στην πράξη μονοδιάστατα συστήματα κωδικοποίησης, λόγω των περιορισμών της τρέχουσας κατάστασης. Παρόλα αυτά, η αλγεβρική μεθοδολογία κωδικοποίησης για τις κατασκευές των μονοδιάστατων κωδίκων, ιδιαίτερα των ΟΟCs, παρέχει έρευνες με διορατικότητα για πολυδιάστατους κώδικες. Οι πληθικότητες των πολυδιάστατων κωδίκων έχουν βελτιωθεί σημαντικά, σε σχέση με εκείνες που έχουν οι μονοδιάστατοι ΟΟCs, και γι’ αυτό είναι κατάλληλοι για μη συνεκτικά συστήματα OCDMA.

Λαμβάνοντας υπόψιν, ότι υπάρχει πολύ υλικό για την κωδικοποίηση OCDMA δικτύων, στην εργασία αυτή, θα παρουσιαστούν μόνο οι μονοδιάστατοι οπτικοί ορθογώνιοι κώδικες.

Βιβλιογραφία

[1] P. R. Prucnal, et. al.: Optical code division multiple access: fundamentals and application. CRC Press, Taylor &Francis Group, 2006, pp55

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

2ο Μέρος : Οπτικοί Ορθογώνιοι Κώδικες

1ο Κεφάλαιο
Βασικές Έννοιες

Αριθμοί

Ορισμός

Πρώτος αριθμός (ή απλά πρώτος) είναι ένας φυσικός αριθμός μεγαλύτερος της μονάδας με την εξής ιδιότητα: οι μόνοι φυσικοί διαιρέτες του να είναι η μονάδα και ο εαυτός του. Το μηδέν και το ένα δεν είναι πρώτοι αριθμοί. Η ακολουθία των 10 πρώτων αριθμών είναι η εξής: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Ο αριθμός 2 είναι ο μοναδικός άρτιος (ζυγός) πρώτος αριθμός. Όλοι οι άλλοι πρώτοι είναι περιττοί (μονοί).

Ορισμός

Πρώτος του Mersenne ονομάζεται κάθε αριθμός που έχει τη μορφή $2^p - 1$, όπου p είναι πρώτος.

Ορισμός

Πρώτος του Fermat ονομάζεται κάθε αριθμός που έχει τη μορφή $p_i = 2^{(2^k)} + 1$. Ο Fermat υπέθεσε ότι οι αριθμοί $2^{(2^k)} + 1$ είναι πρώτοι για όλους τους μη αρνητικούς ακέραιους k.

Ο Euler έδειξε ότι , για $k = 0, 1, 2, 3 \; και \; 4$ οι αριθμοί που προκύπτουν είναι πρώτοι Fermat, δηλαδή,

$p_0 = 2^{(2^0)} + 1 = 3, \; p_1 = 2^{(2^1)} + 1 = 5, \; p_2 = 2^{(2^2)} + 1 = 17,$

$p_3 = 2^{(2^3)} + 1 = 257 \;\; και \;\; p_4 = 2^{(2^4)} + 1 = 65537.$

Έχει αποδειχθεί ότι, για $5 \leq k \leq 19$ όπως και για $k > 20$ οι αριθμοί $2^{(2^k)} + 1$ είναι σύνθετοι. Είναι άγνωστο αν το πλήθος των πρώτων αριθμών του Fermat είναι πεπερασμένο ή άπειρο.

Ορισμός

Δύο αριθμοί x και y ονομάζονται «σχετικά πρώτοι» ή «πρώτοι προς αλλήλους» αν ο μέγιστος κοινός διαιρέτης τους είναι η μονάδα. Δεν έχουν άλλο κοινό διαιρέτη πλην της μονάδας. Για παράδειγμα οι αριθμοί 12 και 25 είναι σχετικά πρώτοι.

Θεμελιώδες Θεώρημα της Αριθμητικής

Είναι ένα από τα πιο σημαντικά θεωρήματα της θεωρίας αριθμών στα μαθηματικά. Σύμφωνα με αυτό, κάθε φυσικός αριθμός μεγαλύτερος της μονάδας αναλύεται σε γινόμενο πρώτων παραγόντων κατά ένα και μοναδικό τρόπο. Δεν λαμβάνεται υπόψιν η σειρά των παραγόντων στο γινόμενο.

Για παράδειγμα: $3.640 = 2^3 \times 5 \times 7 \times 13$.

Ορισμός

Έστω D μία ακέραια περιοχή και $a, b \in D$. Αν υπάρχει $c \in D$ τέτοιο ώστε $b = ac$, τότε το a διαιρεί το b (ή το a είναι παράγοντας του b), και συμβολίζεται a/b.

Ο Gauss στο πρώτο μεγάλο και μνημειώδες επιστημονικό του έργο με τίτλο «Αριθμητικές έρευνες» (1801), περιλαμβάνει το λεγόμενο «χρυσό θεώρημα», που σήμερα ονομάζεται «νόμος της τετραγωνικής αντιστροφής». Ολόκληρο, το έργο θεωρείται η ληξιαρχική πράξη γέννησης της σύγχρονης αριθμοθεωρίας.

Νόμος Τετραγωνικής Αντιστροφής

Έστω q, p είναι περιττοί πρώτοι, διαφορετικοί μεταξύ τους. Τότε ,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu}, \mu = \frac{1}{2}(p-1)(q-1).$$

Αλγεβρικές Δομές

Ορισμός

Το ζεύγος $< G, * >$ μ' ένα σύνολο G και μια διμελή πράξη $*$ στο G ονομάζεται ομάδα όταν ικανοποιούνται τα ακόλουθα αξιώματα:

i. Η διμελής πράξη $*$ είναι προσεταιριστική, δηλαδή $\forall\, \alpha, \beta, \gamma \in G$ ισχύει $\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma$.
ii. Υπάρχει ένα στοιχείο e στο G τέτοιο ώστε, $e * x = x * e = x$ για κάθε $x \in G$. (Το στοιχείο e λέγεται ταυτοτικό στοιχείο για την $*$ στο G) .

iii. Για κάθε α στο G υπάρχει ένα στοιχείο α′ στο G με την ιδιότητα $\alpha' * \alpha = \alpha * \alpha' = e$.
(Το στοιχείο α′ λέγεται αντίστροφο του α ως προς την πράξη $*$) .

Παραδείγματα

Το $< \mathbb{Z}^+, + >$ δεν είναι ομάδα, γιατί δεν υπάρχει ταυτοτικό στοιχείο για την $+$ στο $\mathbb{Z}^+$.
Το $< \mathbb{Z}^+, * >$ δεν είναι ομάδα, γιατί παρόλο που υπάρχει ταυτοτικό στοιχείο για το 1, δεν υπάρχουν αντίστροφοι.

Ορισμός

Αν ένα υποσύνολο Η μιας ομάδας G είναι κλειστό ως προς τη διμελή πράξη της G και αν το Η είναι και αυτό ομάδα, τότε το Η θα λέγεται υποομάδα της G.

Κάθε ομάδα έχει ως υποομάδες την ίδια την G και το $\{e\}$, όπου το e είναι το ταυτοτικό στοιχείο της G.

Ορισμός

Έστω μια πεπερασμένη ομάδα G , τότε η τάξη της, συμβολίζεται $|G|$, είναι το πλήθος των στοιχείων της G.

Γενικά, για πεπερασμένο σύνολο S, $|S|$ είναι το πλήθος των στοιχείων του.

Ορισμός

Η ομάδα G λέγεται κυκλική αν υπάρχει κάποιο στοιχείο α στην G που παράγει την G. Αυτό το στοιχείο λέγεται γεννήτορας της G, και συμβολίζεται $< \alpha > = G$.

Ορισμός

Μια ομάδα $< A , * >$ λέγεται αβελιανή ομάδα αν η διμελής πράξη $*$ είναι αντιμεταθετική, δηλαδή $\forall\, \alpha, \beta \in G$ ισχύει $\alpha * \beta = \beta * \alpha$.

Παραδείγματα

1ο. Το σύνολο των πραγματικών αριθμών $\mathbb{Z}$ εφοδιασμένο με την πράξη της πρόσθεσης είναι ομάδα.

2ο. Το σύνολο των θετικών πραγματικών αριθμών $\mathbb{Z}^+$ εφοδιασμένο με την πράξη της πρόσθεσης δεν είναι ομάδα.

Ορισμός

Μια απεικόνιση $\varphi : G \to G'$ λέγεται ομομορφισμός αν $\varphi(ab) = \varphi(\alpha)\varphi(b)$ για κάθε $a, b \in G$.

Ορισμός

Ένας ισομορφισμός $\varphi : G \to G'$ είναι ένας ομομορφισμός «ένα προς ένα» και «επί» επί της G'. Ο συνήθης συμβολισμός είναι ο $G \simeq G'$.

Ορισμός

Έστω ομάδα G . Κάθε ισομορφισμός $\varphi : G \to G$ λέγεται αυτομορφισμός της ομάδας G.

Ορισμός

Ένας δακτύλιος $< R, +, \cdot >$ είναι ένα σύνολο R με δύο διμελείς πράξεις, την πρόσθεση $(+)$ και τον πολλαπλασιασμό $(\cdot)$, οι οποίες είναι ορισμένες στο R έτσι ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

i. $< R, + >$ είναι μια αβελιανή ομάδα.
ii. Ο πολλαπλασιασμός είναι προσεταιριστικός.
iii. Για κάθε $a, b, c \in R$, ισχύουν ο αριστερός επιμεριστικός νόμος: $a(b + c) = (ab) + (ac)$, και ο δεξιός επιμεριστικός νόμος: $(a + b)c = (ac) + (bc)$.

Παραδείγματα

$< Z, +, \cdot >, < Q, +, \cdot >, < R, +, \cdot >$ είναι δακτύλιοι.

Ορισμός

Έστω R *και* R' δύο δακτύλιοι. Μια απεικόνιση $\varphi : R \to R'$ λέγεται ομομορφισμός αν οι παρακάτω δύο ιδιότητες ικανοποιούνται για κάθε $a, b \in R$:

$$\varphi(\alpha + b) = \varphi(\alpha) + \varphi(b)$$

$$\varphi(ab) = \varphi(\alpha)\varphi(b)$$

Ορισμός

Ένας ισομορφισμός $\varphi : R \to R'$ από ένα δακτύλιο R σ' έναν δακτύλιο R' είναι ένας ομομορφισμός «ένα προς ένα» και «επί» επί του R'. Οι δακτύλιοι R, R'είναι ισόμορφοι.

Σημείωση:

Σε οποιοδήποτε είδος μαθηματικής δομής, η έννοια δύο συστημάτων με ταυτόσημες δομές (δεν λαμβάνονται υπόψιν τα ονόματα των στοιχείων) μαρτυρά ότι τα δύο συστήματα είναι όμοια. Στην άλγεβρα, η έννοια αυτή λέγεται ισομορφισμός.

Ορισμοί

Ένας δακτύλιος R, στον οποίο ο πολλαπλασιασμός είναι αντιμεταθετική πράξη, λέγεται αντιμεταθετικός δακτύλιος. Ένας δακτύλιος με πολλαπλασιαστικό ταυτοτικό στοιχείο το 1, $(1x = x1 = x, \forall x \in R)$ λέγεται δακτύλιος με μοναδιαίο στοιχείο. Κάθε ουδέτερο στοιχείο του πολλαπλασιασμού λέγεται μοναδιαίο στοιχείο.

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο u του R λέγεται μονάδα του R αν έχει πολλαπλασιαστικό αντίστροφο στο R.

Αν κάθε μη μηδενικό στοιχείο του R είναι μονάδα, τότε ο R λέγεται δακτύλιος διαίρεσης. Σώμα λέγεται ένας αντιμεταθετικός δακτύλιος διαίρεσης.

Παραδείγματα

Το $\mathbb{Z}$ δεν είναι σώμα, αφού το 2 δεν έχει πολλαπλασιαστικό αντίστροφο, δηλαδή το 2 δεν είναι μονάδα του $\mathbb{Z}$..

Το $\mathbb{Q}$ και το $\mathbb{R}$ είναι σώματα.

Ορισμός

Για κάθε πρώτο p και για κάθε ακέραιο $m \geq 1$ υπάρχει ακριβώς ένα πεπερασμένο σώμα τάξης p^m. Αυτό το σώμα $GF(p^m)$ αναφέρεται συνήθως ως το σώμα Galois (Galois fields) τάξης p^m, και διαβάζεται σώμα Galois τάξης q, όπου $q = p^m$.

Θεωρία Σχεδιασμών

Ορισμός

Ένας ισορροπημένος, μη – πλήρης σχεδιασμός κατά μπλοκ (balanced incomplete block design) γράφεται BIBD , είναι ο σχηματισμός b μπλοκ από v διακριτά στοιχεία, έτσι ώστε κάθε μπλοκ να περιέχει ακριβώς k στοιχεία, κάθε στοιχείο να ανήκει σε ακριβώς r μπλοκ και κάθε ζευγάρι στοιχείων να ανήκει σε ακριβώς λ μπλοκ. Οι αριθμοί v, b, r, k, λ είναι παράμετροι του σχεδιασμού.

Ο BIB – σχεδιασμός συμβολίζεται με τη διατεταγμένη πεντάδα (v, b, r, k, λ).

Παράδειγμα

Έστω ένας (7,7,3,3,1) BIB – σχεδιασμός.

Σχεδιασμός με 7 στοιχεία, τα 1,2,3,4,5,6,7, δηλαδή $v = 7$, τα οποία σχηματίζουν 7 block (τριάδες), $(b = 7)$ τέτοια ώστε κάθε block να περιέχει ακριβώς τρία στοιχεία $(k = 3)$.

Κάθε στοιχείο ανήκει σε ακριβώς τρία block ($r = 3$) και κάθε ζευγάρι στοιχείων ανήκει σε ακριβώς ένα block ($\lambda = 1$). Μία λύση του προβλήματος θα μπορούσε να είναι η εξής: $\{123, 145, 167, 246, 257, 347, 356\}$

Για τις παραμέτρους (v, b, r, k, λ) ισχύουν τα ακόλουθα θεωρήματα.

Θεώρημα

Σε κάθε (v, b, r, k, λ) BIB – σχεδιασμό ισχύει: $bk = vr$.

Θεώρημα

Σε κάθε (v, b, r, k, λ) BIB – σχεδιασμό ισχύει: $\lambda(v - 1) = r(k - 1)$.

Σημειώσεις:

1) Εφόσον ο BIB – σχεδιασμός είναι μη - πλήρης ισχύει ότι $k < v$, δηλαδή το πλήθος των στοιχείων σε κάθε block είναι μικρότερο από το πλήθος των στοιχείων.
2) Αν $b = v$, τότε θα είναι και $k = r$. Δηλαδή αν το πλήθος των μπλοκ ισούται με το πλήθος των στοιχείων, τότε η επαναληπτικότητα κάθε στοιχείου r, θα ισούται με το πλήθος των στοιχείων σε κάθε μπλοκ.
   Ένας τέτοιος σχεδιασμός λέγεται συμμετρικός (symmetric) μη – πλήρης σχεδιασμός κατά μπλοκ SBIB και συμβολίζεται με 3 μόνο παραμέτρους (v, k, λ).
3) Κάθε BIB – σχεδιασμός μπορεί να θεωρηθεί σαν διμελής σχέση μεταξύ του συνόλου των στοιχείων του $S = \{1,2, \dots , v\}$ και του συνόλου των μπλοκ $B = \{B_1, B_2, \dots , B_b\}$, δηλαδή το στοιχείο t του S αντιστοιχεί στο μπλοκ B_i του B όταν $t \in B_i$.

Ορισμός

Έστω t, v, k, λ ακέραιοι με $v \geq k \geq t$ και $\lambda > 0$. Ένας $t - (v, k, \lambda)$ t − σχεδιασμός είναι μια συλλογή D από $k -$ υποσύνολα ενός $v -$ συνόλου S έτσι ώστε κάθε $t -$ υποσύνολο του S να περιέχεται σε ακριβώς λ blocks.

Κάθε $t -$ σχεδιασμός με $t \geq 2$ είναι ένας BIB – σχεδιασμός.

Ένα σύστημα Steiner είναι απλά ένας $t -$ σχεδιασμός με $\lambda = 1$.

Ορισμός

Ένα σύστημα Steiner $S(t, k, v)$ είναι μία συλλογή από $k -$ υποσύνολα (blocks) ενός $v -$ συνόλου S έτσι ώστε κάθε $t -$ υποσύνολο του S να περιέχεται σε ακριβώς ένα από τα blocks.

Σημείωση

Το $S(t,k,v)$ είναι σαν ισοδύναμο του $t-(v,k,1)$ και τα συστήματα Steiner $S(2,k,v)$ είναι ακριβώς $(v,k,1)$ BIB – σχεδιασμοί.

Λήμμα

Ένα σύστημα Steiner $S(t,k,v)$ έχει $\binom{v}{t}/\binom{k}{t}$ blocks.

Απόδειξη:

Ο αριθμός των blocks στον $t-$ σχεδιασμό είναι:

$b = \lambda \binom{v}{t}/\binom{k}{t}$ στην περίπτωση που $\lambda = 1$.

Θεωρία Κωδίκων

Ορισμός

Αλφάβητο πηγής F^n καλείται μία πεπερασμένη ακολουθία συμβόλων $f_1, f_2, \dots, f_q$. Ένας q - αδικός κώδικας C είναι το υποσύνολο του συνόλου $(F_q)^n$ και τα στοιχεία του ονομάζονται κωδικές λέξεις.

Ορισμός

Η απόσταση Hamming μεταξύ δύο κωδικών λέξεων $\tilde{x}, \tilde{y}$ συμβολίζεται $d(\tilde{x}, \tilde{y})$ και είναι το πλήθος των ψηφίων στα οποία οι κωδικές λέξεις διαφέρουν.

Ορισμός

Ελάχιστη απόσταση $d(C)$ ενός κώδικα ορίζεται να είναι η μικρότερη από τις αποστάσεις μεταξύ των διακεκριμένων κωδικών λέξεων, συμβολίζεται:

$$d(C) = \min\{d(\tilde{x}, \tilde{y}) \,|\tilde{x}, \tilde{y} \in C, \tilde{x} \neq \tilde{y}\}.$$

Η ελάχιστη απόσταση είναι μια σημαντική παράμετρος για έναν κώδικα C. Δίνει ένα μέτρο του πόσο καλός είναι ο κώδικας στη διόρθωση σφαλμάτων. Ένας κώδικας C που έχει ελάχιστη απόσταση d, μπορεί να ανιχνεύσει μέχρι $d-1$ σφάλματα και να διορθώσει μέχρι και $\frac{d-1}{2}$ σφάλματα σε κάθε κωδική λέξη.

Ορισμός

Βάρος Hamming $w(\tilde{x})$ μιας κωδικής λέξης $\tilde{x} = x_1, x_2, \dots, x_n \in F^n$ είναι το πλήθος των μη – μηδενικών ψηφίων της κωδικής λέξης $\tilde{x}$.

Οπτικοί Ορθογώνιοι Κώδικες

Ορισμός

Ένας $(n, w, \lambda_\alpha, \lambda_c)$ οπτικός ορθογώνιος κώδικας (optical orthogonal code) OOC, C είναι μια οικογένεια $(0, 1)$ - ακολουθιών, μήκους n , με βάρος Hamming w (ο αριθμός "1"σε κάθε κωδική λέξη).

Η περιοδική συνάρτηση αυτοσυσχέτισης για κάθε $X = (x_0, x_1, \dots, x_{n-1}) \in C$ και η περιοδική συνάρτηση ετεροσυσχέτισης μεταξύ δύο κωδικών λέξεων $X = (x_0, x_1, \dots, x_{n-1})$ $και$ $Y = (y_0, y_1, \dots, y_{n-1})$ ικανοποιούν τις ακόλουθες ιδιότητες αντίστοιχα:

$$\theta_{XX}(\tau) = \sum_{i=0}^{n-1} x_i \cdot x_{i\oplus\tau} = \begin{cases} w, & \tau = 0 \\ \leq \lambda_\alpha, & 1 \leq \tau \leq n-1 \end{cases}$$

$$\theta_{XY}(\tau) = \sum_{i=0}^{n-1} x_i \cdot y_{i\oplus\tau} \leq \lambda_c \quad 0 \leq \tau \leq n-1$$

Για $x_i, y_i \in \{0,1\}$, όλοι οι ακέραιοι $\tau \neq 0 \ (mod\ n)$ $και$ $X \neq Y$, όπου OOC ορίζονται σύμφωνα με τις περιοδικές συναρτήσεις συσχέτισης, και γι' αυτό , "$\oplus$" υποδηλώνει πρόσθεση $modulo\ n$.

Από σύνολο – θεωρητική προοπτική, ένας $(n, w, \lambda_\alpha, \lambda_c) - OOC$, C, μπορεί εναλλακτικά να θεωρηθεί ως μια οικογένεια συνόλων w – ακεραίων, $modulo\ n$ [1], στην οποία κάθε w αντιστοιχεί σε μια κωδική λέξη και οι ακέραιοι w προσδιορίζουν τις θέσεις των μη μηδενικών chips (δηλαδή, "1" chip) της κωδικής λέξης. Τότε, οι ιδιότητες συσχέτισης μπορούν να αναδιατυπωθούν ως εξής:

1. Ιδιότητα αυτοσυσχέτισης:

$$|(X + \alpha) \cap (X + b)| \leq \lambda_\alpha \ , για\ κάθε\ X \in C\ και\ \ a \neq b\ (mod\ n)$$

2. Ιδιότητα ετεροσυσχέτισης

$$|(X + \alpha) \cap (Y + b)| \leq \lambda_c \ , για\ κάθε\ X, Y \in C\ , X \neq Y\ και\ \ κάθε\ a\ , b\ \in \mathbb{Z}_n$$

$όπου$ $X + \alpha = \{x \oplus a \mid x \in X\}$.

Από τώρα και στο εξής, σημειώνεται ότι, θα χρησιμοποιείται ο συμβολισμός $(n, w, \lambda_\alpha, \lambda_c) - OOC$ για έναν οπτικό ορθογώνιο κώδικα, εάν δεν διευκρινίζεται διαφορετικά.

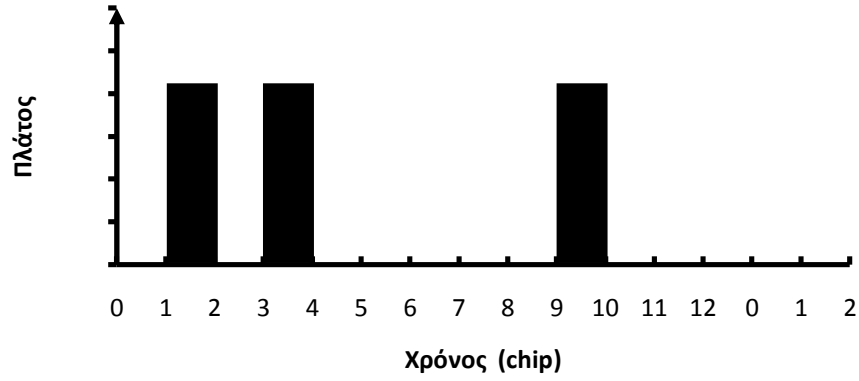
Ορισμός

Ο αριθμός των κωδικών λέξεων (δηλαδή, $|C|$) ενός $(n, w, \lambda_\alpha, \lambda_c) - OOC$ καλείται πληθικότητα του κώδικα. Η μεγαλύτερη πιθανή πληθικότητα συμβολίζεται ως $\Phi(n, w, \lambda_\alpha, \lambda_c)$, δηλαδή, $|C|_{max} = \Phi(n, w, \lambda_\alpha, \lambda_c)$.

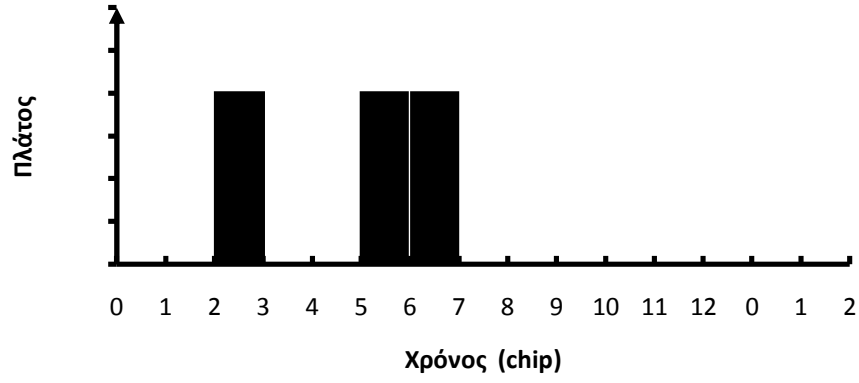
Παράδειγμα

Έστω $X_1 = \{1100100000000\}$ $και$ $X_2 = \{1010000100000\}$ οι δύο κωδικές λέξεις του $(n, w, \lambda_\alpha, \lambda_c) = (n, w, \lambda) = (13, 3, 1) - OCC$. Τότε συμβολίζονται $X_1 = \{(1,3,9)\ mod\ 13\}$ $και$ $X_2 = \{(2,5,6)\ mod\ 13\}$. Η κυματομορφή αυτών των δύο κωδικών λέξεων παρουσιάζεται στο ακόλουθο σχήμα:

Κωδική λέξη {1,3,9}



Κωδική λέξη {2,5,6}



Οι $OOCs$ χωρίζονται σε κώδικες σταθερού βάρους και σε κώδικες μεταβλητού βάρους. Οι κώδικες σταθερού βάρους υποδιαιρούνται σε συμμετρικούς και μη συμμετρικούς κώδικες σταθερού βάρους.

Βιβλιογραφία

«Εισαγωγή στην άλγεβρα» του John B. Fraleigh

«Θεωρία πληροφοριών και κωδίκων» - Χ.Κουκουβίνος, Α.Παπαϊωάννου

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

[1]. Jawad. A. Salehi, F. R. K. Chung, and V. K. Wei: Optical orthogonal codes: Design, analysis, and applications. IEEE Trans. on Information theory, Vol.35, Nol.3, May 1989, pp595-605

2ο Κεφάλαιο
Σταθερού βάρους Συμμετρικοί OOCs

Ορισμός

Ένας $(n, w, \lambda_\alpha, \lambda_c) - OOC$ καλείται σταθερού βάρους συμμετρικός OOC (constant-weight symmetric OOC) όταν $\lambda_\alpha = \lambda_c = \lambda$. Εν συντομία χρησιμοποιείται ο συμβολισμός (n, w, λ) για τον κώδικα, και $\Phi(n, w, \lambda)$ για τη μεγαλύτερη δυνατή πληθικότητα.

Πληθικότητα Σταθερού βάρους Συμμετρικών $OOCs$

Θεώρημα (φράγμα Johnson)

Το φράγμα Johnson ενός κώδικα διόρθωσης σφαλμάτων σταθερού βάρους, μπορεί να χρησιμοποιηθεί ώστε να βρεθεί ένα γενικό άνω φράγμα για την πληθικότητα $|C|$ *ενός* $(n, w, \lambda_\alpha, \lambda_c) - OOC$, το οποίο είναι το εξής:

$$\Phi(n, w, \lambda_\alpha, \lambda_c) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \right\rfloor \dots \left\lfloor \frac{n-\lambda+1}{w-\lambda+1} \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor$$

Συγκεκριμένα, στον $(n, w, 1) - OCC$ ισχύει

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{n-1}{w(w-1)} \right\rfloor$$

όπου $\lfloor x \rfloor$ υποδηλώνει τον μεγαλύτερο ακέραιο από τον μικρότερο ή ίσο με τον x.

Αν $w = 3, \lambda = 1$,

$$\Phi(n, 3, 1) \leq \left\lfloor \frac{n-1}{6} \right\rfloor$$

Όταν n είναι ζυγός, ισχύει το ελαφρώς ισχυρότερο άνω φράγμα

$$\Phi(n, w, 1) \leq \left\lfloor \frac{n-2}{w(w-1)} \right\rfloor$$

Θεώρημα

Έστω n, w, λ ακέραιοι, $n > 1,\ 1 \leq w \leq n,\ 0 \leq \lambda \leq w$.

Τότε θα ισχύουν:

1) $\Phi(n, w, \lambda) \leq 1,\ \alpha\nu\ w^2 > \lambda_c n$
2) $\Phi(n, w, \lambda) = 0,\ \alpha\nu\ w(w-1) > \lambda_\alpha(n-1)$

Απόδειξη:

1) Υποθέτοντας το αντίθετο.

   Για δύο διακεκριμένες κωδικές λέξεις $x, y,\ 0 \leq k \leq n-1$, θα ισχύει

$$\sum_{\tau=0}^{n-1}\sum_{i=0}^{n-1} x_i \cdot y_{i\oplus\tau} = w^2$$

   και

$$\sum_{i=0}^{n-1} x_i \cdot y_{i\oplus\tau} \leq \lambda_c \ \gamma\iota\alpha\ \kappa\acute{\alpha}\theta\varepsilon\ \tau$$

   δηλαδή

$$w^2 \leq \lambda_c n$$

   που είναι άτοπο.

   Άρα, $w^2 > \lambda_c n$.

2) Ομοίως, εφόσον,

$$\sum_{\tau=1}^{n-1}\sum_{i=0}^{n-1} x_i x_{i\oplus\tau} = w(w-1)$$

   πρέπει να ισχύει $w(w-1) > \lambda_\alpha(n-1)$ για να είναι $x(\cdot)$ έγκυρη κωδική λέξη.

▪

Ορισμός

Αν για την πληθικότητα $|C|$ του $(n, w, \lambda) - OOC$, C, ισχύει $|C| = \Phi(n, w, \lambda)$, τότε ο OOC, C καλείται βέλτιστος. Αν η $|C|$ πλησιάζει την $\Phi(n, w, \lambda)$, τότε ο C καλείται σχεδόν βέλτιστος.

Για $\lambda = 1$, παρατίθεται ο ακόλουθος πίνακας για την πληθικότητα ορισμένων βέλτιστων $OOCs$.

Η πληθικότητα ορισμένων βέλτιστων $OOCs$

w	n	$\|C\|$	w	n	$\|C\|$
3	31	5	5	85	4
3	63	10	5	341	17
3	127	21	5	1365	68
4	40	3	6	156	5
4	121	10	6	631	21
4	364	30	6	3156	105

Κατασκευές για Σταθερού βάρους Συμμετρικούς $OOCs$

Η κατασκευή ενός OOC είναι ισοδύναμη με το σχεδιασμό ενός μπλοκ μιας κωδικής λέξης. Η κατασκευή ενός μπλοκ μιας κωδικής λέξης επιτυγχάνεται, αν χρησιμοποιηθεί αρχική θεωρία αριθμών, πεπερασμένη προβολική γεωμετρία, πεπερασμένα σώματα, αλγεβρική θεωρία κωδικοποίησης και διάφοροι άλλοι συνδυαστικοί κλάδοι.

Οι κατασκευές θα κατηγοριοποιηθούν σε τέσσερις μεγάλες κατηγορίες. Στις συνδυαστικές κατασκευές, στις κατασκευές που βασίζονται στις θεωρίες της προβολικής γεωμετρίας, στις αλγεβρικές κατασκευές, και στις επαναληπτικές κατασκευές.

Συνδυαστικές κατασκευές

Οι οπτικοί ορθογώνιοι κώδικες μπορούν να κατασκευαστούν από διάφορες συνδυαστικές μεθόδους. Για $\lambda = 1$, το πρόβλημα της κατασκευής των $OOCs$ είναι ισοδύναμο με το πρόβλημα ομαδοποίησης των συνόλων διαφορών.

i. Κατασκευές για $(n, 2, 1) - OOCs$
$\{(0,1), (0,2), \dots, (0, \varphi)\}$ $(mod\ n)$ είναι βέλτιστος $(n, 2, 1) - OOC$

- όταν n περιττός, τότε $\varphi = \frac{n-1}{2}$
- όταν n άρτιος, τότε $\varphi = \frac{n}{2} - 1$

ii. Κατασκευές για $(n, 3, 1)$ βελτιστοποιημένους και βέτλιστους $OOCs$

Υποθέτοντας ότι $n = 6l + v'$ $για$ $1 \leq v' \leq 6$

- $l \equiv 0\ (mod\ 4)$

  Υποθέτοντας $l = 4u \geq 8$, οι ακόλουθοι l σχηματισμοί με 3 στοιχεία, σχηματίζουν έναν $(n, 3, 1)$ βελτιστοποιημένο OOC ως εξής:

  $\{0, 4u + i, 8u - i\}$ $\quad 1 \leq i \leq 2u - 1$

  $\{0, 8u - 1 + i, 12u - i\}$ $\quad 1 \leq i \leq u$

  $\{0, 9u + 1 + i, 11u - i\}$ $\quad 1 \leq i \leq u - 2$

  και $\{0, 6u, 10u\}, \{0, 9u, 9u + 1\}, \{0, 10u + 1, 12u\}$.

  Παράδειγμα

  Η κατασκευή του $(49,3,1) - OOC$

  Υποθέτοντας ότι $l = 8, \mathrm{u} = 2$ και $n = 6l + v' = 48 + v'$ για $1 \leq v' \leq 6$, μπορεί να επιτευχθεί ο OOC με τις εξής κωδικές λέξεις: (0,9,15), (0,10,14), (0,11,13), (0,16,23), (0,17,22) και (0,12,20), (0,18,19), (0,21,24), δηλαδή $|C| = 8$.

- $l \equiv 1\ (mod\ 4)$

  Υποθέτοντας $l = 4u + 1 \geq 9$, ο βελτιστοποιημένος $(n, 3, 1) - OOC$ μπορεί να κατασκευαστεί από l σχηματισμούς με 3 στοιχεία, ως εξής:

  $\{0, l + i, 2l + 1 - i\}$ $\quad 1 \leq i \leq 2u$

  $\{0, 2l + i, 3l - i\}$ $\quad 1 \leq i \leq u$

  $\{0, 2l + u + 2 + i, 3l - u - i\}$ $\quad 1 \leq i \leq u - 2$

  και $\{0, l + 2u + 1, 2l + 2u + 1\}, \{0, 2l + u + 1, 2l + u + 2\}, \{0, 2l + 2u + 2, 3l\}$.

Παράδειγμα

Η κατασκευή του $(55,3,1)-OOC$

Υποθέτοντας ότι $l=9,\mathrm{u}=2$ και $n=6l+v'=54+v'$ για $1\le v'\le 6$, μπορεί να επιτευχθεί ο OOC με τις εξής κωδικές λέξεις: (0,10,18), (0,11,17), (0,12,16), (0,13,15), (0,19,26), (0,20,25) και (0,14,23), (0,21,22), (0,24,27) δηλαδή $|C|=9$.

- $l\equiv 2\ (mod\ 4)$

Υποθέτοντας $l=4u+2\ge 6$, οι ακόλουθοι l σχηματισμοί με 3 στοιχεία , σχηματίζουν έναν $(n,3,1)$ βελτιστοποιημένο OOC ως εξής:

$\{0,l+i,2l-i\}$ $\quad 1\le i\le l/2-1$

$\{0,2l-1+i,3l-i\}$ $\quad 1\le i\le u$

$\{0,2l+u+1+i,3l-u-i\}$ $\quad 1\le i\le u-1$

και $\{0,\frac{3}{2}l,\frac{5}{2}l\},\{0,2l+u,2l+u+1\},\{0,\frac{5}{2}l+1,3l+1\}$.

Παράδειγμα

Η κατασκευή του $(37,3,1)-OOC$

Υποθέτοντας ότι $l=6,\mathrm{u}=1$ και $n=6l+v'=36+v'$ για $1\le v'\le 6$, μπορεί να επιτευχθεί ο OOC με τις εξής κωδικές λέξεις: (0,7,11), (0,8,10), (0,12,17), και (0,9,15), (0,13,14), (0,16,19) δηλαδή $|C|=6$.

- $l\equiv 3\ (mod\ 4)$

Υποθέτοντας $l=4u+3\ge 7$, τότε όταν $n\ne 2\ (mod\ 6)$ οι ακόλουθοι l σχηματισμοί με 3 στοιχεία , σχηματίζουν έναν $(n,3,1)$ βελτιστοποιημένο OOC ως εξής:

$\{0,l+i,2l+1-i\}$ $\quad 1\le i\le 2u+1$

$\{0,2l+i,3l+1-i\}$ $\quad 1\le i\le u+1$

$\{0,2l+u+3+i,3l-u-1-i\}$ $\quad 1\le i\le u-2$

και $\{0,l+2u+2,2l+2u+2\},\{0,2l+u+2,3l+3\},\{0,2l+2u+3,3l+1\}$.

iii. Κατασκευές για $(n,4,1)-OOCs$.

Κατασκευές Βασισμένες στην Πεπερασμένη Προβολική Γεωμετρία

Ορισμός

Στο διανυσματικό χώρο $V(r,q) = \{(a_1,\ a_2, \dots\ , a_r) \mid a_i \in GF(q)\}$ αντιστοιχεί μία συνδυαστική δομή $PG(r-1,q)$ που αποτελείται από σημεία και ευθείες που ορίζονται ως εξής:

i. Τα σημεία της $PG(r-1,q)$ είναι μονοδιάστατοι υπόχωροι του $V(r,q)$.
ii. Οι ευθείες της $PG(r-1,q)$ είναι διδιάστατοι υπόχωροι του $V(r,q)$.
iii. Το σημείο P ανήκει (ή βρίσκεται) στην ευθεία L αν και μόνον αν το P είναι ένας υπόχωρος του L.

Η $PG(r-1,q)$ ονομάζεται προβολική γεωμετρία (projective geometry) διάστασης $r-1$ πάνω στο $GF(q)$.

Η πεπερασμένη γεωμετρία υπακούει στο Ευκλείδειο αίτημα ότι οι παράλληλες ευθείες δεν έχουν κοινό σημείο. Από τις αρχές του 19ου αιώνα μελετήθηκαν διαφορές γεωμετρίες. Ένα αίτημα της γεωμετρίας είναι ότι «κάθε δύο ευθείες έχουν ένα κοινό σημείο» . Η προβολική γεωμετρία το δέχεται.

Έστω μία κυκλική μετατόπιση της ευθείας L στην $PG(r-1,q)$ για να δημιουργηθεί ένα σύνολο από σημεία

$$\{p : log\, p = 1 + logp'(mod\ n)\ \text{, για κάποια σημεία } p' \text{ στην } L\},$$

τότε, η κυκλική μετατόπιση της ευθείας εξακολουθεί να παραμένει ευθεία στην $PG(r-1,q)$.

Ορισμός

Τροχιά είναι ένα σύνολο ευθειών στην $PG(r-1,q)$, οι οποίες είναι κυκλικές μετατοπίσεις. Ο αριθμός των ευθειών σε μία τροχιά είναι το μέγεθος της, το οποίο είναι απαραίτητα διαιρέτης του n. Μια τροχιά είναι πλήρης αν το μέγεθος της είναι n, αλλιώς είναι ατελής.

Ερώτηση:

Πως κατασκευάζεται ένας $(n,w,1)$ – OOC από την πεπερασμένη προβολική γεωμετρία $PG(r-1,q)$, όπου $n = \frac{q^{d+1}-1}{q-1}$ και $w = q+1$;

Υποτίθεται ότι υπάρχουν m πλήρεις τροχιές στην $PG(r-1,q)$ και λαμβάνεται υπόψιν μία ευθεία - εκπρόσωπος από κάθε πλήρη τροχιά και μία απεικόνιση κάθε ευθείας

ενός συνόλου ακεραίων $modulo\ n$ για $log(\cdot)$. Τα m σύνολα που προκύπτουν, έχουν w στοιχεία και αποτελούν έναν OOC , με τις παραμέτρους που τον περιγράφουν και τις επιθυμητές ιδιότητες συσχέτισης. Δύο ευθείες τέμνονται όχι σε περισσότερα από ένα σημεία και επομένως, δύο διαφορετικές μετατοπίσεις μιας κωδικής λέξης τέμνονται το πολύ μία φορά. Ακόμη και αυθαίρετες μετατοπίσεις δύο κωδικών λέξεων τέμνονται το πολύ μία φορά.

Εφαρμογή μ' ένα παράδειγμα.

Παράδειγμα

Η κατασκευή του $(7, 3, 1) - OOC$ για το προβολικό επίπεδο $PG(2, 2)$ και την επέκταση του σώματος Galois $GF^*(2^{2+1})$.

Πρώτα απ 'όλα, είναι απαραίτητο όλα τα μη μηδενικά διανύσματα και οι διακεκριμένοι λογάριθμοι τους να βρίσκονται στο $GF^*(2^{2+1})$. Επιλέγεται ένα αρχικό ανάγωγο πολυώνυμο βαθμού 3 πάνω στο $GF(2)$, $το\ f(x) = x^3 + x + 1$ και έστω α ένα αρχικό στοιχείο.

Τότε, οι δυνάμεις του α είναι:

$\alpha^0 = (0, 0, 1), \alpha^1 = (0, 1, 0), \alpha^2 = (1, 0, 0), \alpha^3 = (0, 1, 1), \alpha^4 = (1, 1, 0), \alpha^5 = (1, 1, 1),$
$\alpha^6 = (1, 0, 1).$

Οι αντίστοιχες σχέσεις μεταξύ των διαφορετικών λογαρίθμων και των διανυσμάτων είναι: $0 \to (0, 0, 1),\ 1 \to (0, 1, 0), 2 \to (1, 0, 0),\ 3 \to (0, 1, 1),\ 4 \to (1, 1, 0),\ 5 \to (1, 1, 1),$
$6 \to (1, 0, 1).$

Για τη δυϊκή σχέση μεταξύ του προβολικού επιπέδου και των ευθειών της προβολικής γεωμετρίας, επιτυγχάνεται η δυϊκή ισότητα:

$$X_0x_0 + X_1x_1 + X_2x_2 = 0$$

Τα επτά διανύσματα (που αντιστοιχούν στις συντεταγμένες σημείου) που ήδη προαναφερθήκαν, θεωρούνται ως συντελεστές της εξίσωσης αντίστοιχα. Κατόπιν, οι εξισώσεις για τις επτά ευθείες είναι:

$0 \to (0, 0, 1) \to l_0 : x_0 = 0 \to (0, 1, 0), (0, 1, 0), (0, 1, 1)$ στη γραμμή l_0 , της οποίας ο αύξοντας αριθμός είναι $(0, 1, 3)$

$1 \to (0, 1, 0) \to l_1 : x_1 = 0 \to (0, 0, 1), (1, 0, 0), (1, 0, 1)$ στη γραμμή l_1 , της οποίας ο αύξοντας αριθμός είναι $(0, 2, 6)$

$2 \to (1, 0, 0) \to l_2 : x_2 = 0 \to (0, 1, 0), (1, 0, 0), (1, 1, 0)$ στη γραμμή l_2 , της οποίας ο αύξοντας αριθμός είναι $(1, 2, 4)$

$3 \to (0, 1, 1) \to l_3 : x_1 + x_0 = 0 \to (0, 1, 0), (0, 1, 1), (1, 1, 1)$ στη γραμμή l_3 , της οποίας ο αύξοντας αριθμός είναι $(0, 4, 5)$

$4 \to (1,1,0) \to l_4 : x_2 + x_1 = 0 \to (1,0,0), (0,1,1), (1,1,1)$ στη γραμμή l_4, της οποίας ο αύξοντας αριθμός είναι $(2,3,5)$

$5 \to (1,1,1) \to l_5 : x_2 + x_1 + x_0 = 0 \to (0,1,1), (1,1,0), (1,0,1)$ στη γραμμή l_5, της οποίας ο αύξοντας αριθμός είναι $(3,4,6)$

$6 \to (1,0,1) \to l_6 : x_2 + x_0 = 0 \to (0,1,0), (1,1,1), (1,0,1)$ στη γραμμή l_6, της οποίας ο αύξοντας αριθμός είναι $(1,5,6)$.

Οι επτά ευθείες αντιστοιχούν σε επτά κωδικές λέξεις του $(7,3,1) - OOC$, οι οποίες είναι: $(0,1,3), (0,2,6), (1,2,4), (0,4,5), (2,3,5), (3,4,6), (1,5,6)$. Ωστόσο, δεδομένου ότι αυτές περιλαμβάνουν έξι κυκλικές μετατοπίσεις, τότε, θα υπάρχει μόνο $7/7 = 1$ κωδική λέξη στον $(7,3,1) - OOC$. Επομένως, κάθε μία που θα επιλέγεται από αυτές, θα είναι κατασκευασμένη κωδική λέξη του $(7,3,1) - OOC$.

Με μια παρόμοια προσέγγιση, ο $(n,w,1) - OOC$, όπου $n = \frac{q^{d+1}-1}{q-1}$ και $w = q+1$ με αυθαίρετες τιμές μπορεί να κατασκευαστεί στο προβολικό χώρο $PG(d,q)$ επί του σώματος Galois.

Παράδειγμα

Δεκαεπτά κωδικές λέξεις μπορούν να επιτευχθούν για τον $(341,5,1) - OOC$, χρησιμοποιώντας την $PG(4,2^2)$, οι οποίες δίνονται στον παρακάτω πίνακα.

Οι κωδικές λέξεις του $(341,5,1) - OOC$

S_1	{0,1,85,21,5}
S_2	{0,2,170,10,42}
S_3	{0,3,111,104,53}
S_4	{0,6,222,106,208}
S_5	{0,9,268,151,105}
S_6	{0,11,45,76,198}
S_7	{0,12,103,75,212}
S_8	{0,13,305,227,43}
S_9	{0,15,107,146,164}
S_{10}	{0,17,264,203,165}
S_{11}	{0,19,88,267,220}
S_{12}	{0,22,90,55,152}

S_{13} {0,23,293,252,118}

S_{14} {0,24,206,83,150}

S_{15} {0,25,54,169,221}

S_{16} {0,26,269,86,113}

S_{17} {0,37,147,217,81}

▪

Παρατίθεται ο ακόλουθος πίνακας για την πληθικότητα ορισμένων $(n, w, 1) - OOCs$, καθώς και οι παράμετροι που χρησιμοποιούνται d και q .

$(n, w, 1) - OOCs$ της πεπερασμένης προβολικής γεωμετρίας $PG\ (d, q)$

w	n	$\|C\|$	d	q	w	n	$\|C\|$	d	q
3	31	5	4	2	5	85	4	3	4
3	63	10	5	2	5	341	17	4	4
3	127	21	6	2	5	1365	68	5	4
4	40	3	3	3	6	156	5	3	5
4	121	10	4	3	6	631	21	4	5
4	364	30	5	3	6	3156	105	5	5

Ο αριθμός των ευθειών στην προβολική γεωμετρία $PG\ (d, q)$, είναι:

$$\frac{(q^{d+1}-1)(q^{d+1}-q)}{(q^2-1)(q^2-q)} = \frac{(q^{d-1}-1)n}{(q^2-1)} = \frac{n(n-1)}{w(w-1)}$$

Όταν d – ζυγός, το q^2-1 διαιρεί το $q^{d-1}-1$ χωρίς η διαίρεση να αφήνει υπόλοιπο. Επιπλέον, όλες οι τροχιές είναι πλήρης και το αποτέλεσμα είναι ένας βέλτιστος OOC.

Όταν d – περιττός, το q^2-1 δεν διαιρεί το $q^{d-1}-1$ ακριβώς και υπάρχει μονό μία ατελής τροχιά, και όλες οι υπόλοιπες είναι πλήρεις. Τότε ο αριθμός για τις πλήρεις τροχιές είναι

$$\left\lfloor \frac{(n-1)}{w(w-1)} \right\rfloor = \frac{q^d - q}{q^2 - 1}$$

που ικανοποιεί το άνω φράγμα του Johnson, και συνεπώς, ο OOC που προκύπτει θα είναι επίσης βέλτιστος.

Λόγω του φράγματος Johnson, οι OOCs με $\lambda = 1$ έχουν μικρότερο αριθμό κωδικών λέξεων και επομένως, μερικοί χρήστες μπορεί να φιλοξενηθούν στα αντίστοιχα δίκτυα OCDMA. Κατ' επέκταση, οι OOCs με $\lambda_\alpha, \lambda_c > 1$ έχουν περισσότερες κωδικές λέξεις. Μερικές φορές αυτοί οι OOCs καλούνται γενικευμένοι οπτικοί ορθογώνιοι κώδικες (generalized OOCs), και έχουν μελετηθεί για τα συστήματα OCDMA.

Παράδειγμα

Σε 50 χρήστες, ο $(1000, 12, 2) - \text{OOC}$ έχει καλύτερη απόδοση από τον $(1000, 5, 1) - \text{OOC}$. Σε αυτό το σημείο αποδεικνύεται ότι οι OOCs με $\lambda = 2, 3$ μπορούν να έχουν καλύτερη απόδοση από τους κώδικες με $\lambda = 1$. Συνεπώς, οι μέθοδοι κατασκευής των γενικευμένων OOCs έχουν σημασία.

Ορισμός

Ένας συμμετρικός μη – πλήρης σχεδιασμός κατά μπλοκ SBIB με παραμέτρους $(q^2 + q + 1, q + 1, 1)$ ονομάζεται πεπερασμένο προβολικό επίπεδο (projective plane) επί του $GF(q)$.

Στους κώνους του πεπερασμένου προβολικού επιπέδου της προβολικής γεωμετρίας $PG(3, q)$ έχει επιτευχθεί ο ασυμπτωματικός βέλτιστος $(q^3 + q^2 + q + 1, q + 1, 2) - OOC$ με $q^3 - q^2 + q$ κωδικές λέξεις.

Παράδειγμα

Ο $(40,4,2) - OOC$, για $q = 3$, έχει 21 κωδικές λέξεις.

Βιβλιογραφία

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

«Θεωρία σχεδιασμών» - Χ.Κουκουβίνος, Α.Παπαϊωάνου

Αλγεβρικές κατασκευές

Σύντομες κατασκευές

1η Κατασκευή (Πεπερασμένη θεωρία σωμάτων)

Υποτίθεται ότι α είναι αρχικό στοιχείο του πεπερασμένου σώματος $GF(p^{2m})$, όπου p είναι ένας πρώτος αριθμός και το m είναι ένας θετικός ακέραιος αριθμός, μεγαλύτερος ή ίσος με τη μονάδα. Ορίζεται, $q = p^m + 1$ και $\beta = \alpha^q$.

Έστω f η αλγοριθμική απεικόνιση του $GF(p^{2m})\backslash\{0\}$ για το σύνολο ακεραίων $\{0, 1, \dots, p^{2m-1}\}$, δηλαδή,

$$f(\alpha^t) = t$$

Τότε, η χαρακτηριστική συνάρτηση των υποσυνόλων S_i, δίνεται από την ακόλουθη σχέση:

$$S_i = \{f(x) \mid (x-1)^{p^m+1} = \beta^i\}, 1 \le i \le p^m - 2$$

Αλλιώς, η χαρακτηριστική συνάρτηση των S_i οδηγεί σε μια απεικόνιση $g(x)$ από το $\{0, 1, \dots, p^{2m-1}\}$ στο $\{0, 1\}$, η οποία δίνεται ως:

$$g(x) = \begin{cases} 1 & \alpha\nu \ x \in S_i \\ 0 & \alpha\nu \ x \in \{0, 1, \dots, p^{2m-1}\} \setminus S_i \end{cases}$$

Άρα, μπορούν να επιτευχθούν $p^m - 2$ κωδικές λέξεις με αυτή τη μέθοδο, η οποία ικανοποιεί την ισότητα του φράγματος Johnson και γι' αυτό ο κατασκευασμένος ΟΟC είναι βέλτιστος ΟΟC.

Παράδειγμα

Η κατασκευή του $(63, 9, 2) - OCC$.

Ο $(63, 9, 2) - OCC$ επιτυγχάνεται για $p = 2$ $και$ $m = 3$.

Δηλαδή, $(63, 9, 2) = (2^6 - 1, 2^3 + 1, 2)$ και $q = 9$.

Το α είναι αρχικό στοιχείο του πεπερασμένου σώματος $GF(p^{2m}) = GF(2^{2\cdot 3}) = GF(2^6)$. Διαλέγοντας το ανάγωγο πολυώνυμο βαθμού 6, $x^6 + x + 1$, στο $GF(p) = GF(2)$. Η ισότητα

$$S_i = \{ f(x): (x-1)^{p^m+1} = \beta^i\}, \ 1 \le i \le p^m - 2$$

είναι ισοδύναμη με την ισότητα $(\alpha^y + 1)^9 = a^{9i}$, $1 \le i \le 6$, οι τιμές του y ικανοποιούν τη σχέση $1 \le y \le p^m - 2$ και συνεπώς, το y έχει πέντε τιμές για κάθε τιμή i.

Για παράδειγμα, όταν $i = 1, y = 6$ (τετριμένη τιμή) ισχύει $(\alpha^y + 1)^9 = a^9$, διότι $\alpha^y + 1 = \alpha^6 + 1 \xrightarrow{mod\ 5} \alpha^6 + 1 = (\alpha + 1) + 1 \xrightarrow{mod\ 5} \alpha^6 + 1 = a$.

Μπορούν να βρεθούν οχτώ άλλες λύσεις χρησιμοποιώντας παρόμοιες μεθόδους, και τελικά επιτυγχάνεται το μπλοκ της κωδικής λέξης του οπτικού ορθογώνιου κώδικα, δηλαδή το $S_1 = \{6,22,23,39,48,50,54,58,60\}$.

Ομοίως, για $i = 2$ ισχύει $(\alpha^y + 1)^9 = a^{18}$ με $S_2 = \{12,15,33,37,44,45,46,53,57\}$

Ομοίως, για $i = 3$ ισχύει $(\alpha^y + 1)^9 = a^{27}$ με $S_3 = \{4,9,14,20,32,34,47,49,61\}$.

Ομοίως, για $i = 4$ ισχύει $(\alpha^y + 1)^9 = a^{36}$ με $S_4 = \{3,11,24,25,27,29,30,43,51\}$.

Ομοίως, για $i = 5$ ισχύει $(\alpha^y + 1)^9 = a^{45}$ με $S_5 = \{2,7,10,16,17,36,55,56,62\}$.

Ομοίως, για $i = 6$ ισχύει $(\alpha^y + 1)^9 = a^{54}$ με $S_6 = \{1,5,8,18,28,31,35,40,59\}$.

Με αυτόν τον τρόπο, ο $(63, 9, 2)$ – OCC έχει κατασκευαστεί.

2η Κατασκευή (Wilson)

Υποτίθεται ότι $w = 2m + 1$, $n = w(w-1)r + 1$, όπου m και r είναι ακέραιοι έτσι ώστε ο n να είναι πρώτος αριθμός.

Έστω ότι α είναι αρχική ρίζα και το σύνολο $c = (w-1)r$. Για $1 \le i \le c-1$, το σύνολο S_i είναι το εξής:

$$S_i = \{\alpha^{i+jc} | 0 \le j \le w-1\}$$

όπου i είναι ο δείκτης του συνόλου S_i και έστω $i = i_k$ για κάθε $1 \le k \le m$. Αν και μόνο εάν $(a^{kc} - 1) \in S_i$, τότε οι χαρακτηριστικές συναρτήσεις των υποσυνόλων $S_0, S_m, S_{2m}, \dots, S_{(r-1)m}$ μπορούν να χρησιμοποιηθούν ως κωδικές λέξεις ενός βέλτιστου $(n, w, 1) - OOC$, εφόσον, όλοι οι δείκτες $i_1, i_2, \dots, i_m$ είναι διακεκριμένοι $modulo\ n$. Όλες οι αριθμητικές πράξεις είναι $modulo\ n$.

Παράδειγμα

Η κατασκευή του $(n, w, 1) = (61, 5, 1)$ βέλτιστου OOC.

Ο $n = 61$ είναι πρώτος αριθμός και έτσι $m = 2, r = 3, c = 12$. Επιλέγοντας, $a = 2$ ως αρχική ρίζα του $GF(61)$, προκύπτουν τα εξής υποσύνολα:

$S_0 = \{1,9,20,58,34\}$

$S_2 = \{4,36,19,49,14\}$

$S_4 = \{16,22,15,13,56\}$

τα οποία είναι όλα κωδικές λέξεις του $(61, 5, 1) - OOC$. Όλες οι αριθμητικές πράξεις είναι $modulo\ 61$.

3η Κατασκευή (Wilson)

Υποθέτοντας $w = 2m$, $n = w(w-1)r + 1$, όπου m και r είναι ακέραιοι έτσι ώστε ο n να είναι πρώτος αριθμός. Υποτίθεται ακόμη ότι, β είναι αρχική ρίζα $modulo\, n$ του $GF(n)$ και $c = wr$. Για $0 \le i \le c-1$, συμβολίζεται T_i το σύνολο

$$T_i = \{\beta^{i+jc} : 0 \le j \le w-2\} \cup \{0\}$$

όπου i είναι ο δείκτης του T_i και τότε $i_0, i_1, i_2, \dots, i_{m-1}$ είναι οι δείκτες του T_i οι οποίοι περιλαμβάνουν $1, \beta^c - 1, \beta^{2c} - 1, \dots, \beta^{(m-1)c} - 1$ αντίστοιχα. Αν $i_0, i_1, i_2, \dots, i_{m-1}$ είναι διακεκριμένα $modulo\, m$, τότε οι χαρακτηριστικές συναρτήσεις των υποσυνόλων μπορούν να θεωρηθούν κωδικές λέξεις του βέλτιστου $(n, w, 1) - OOC$. Όλες οι αριθμητικές πράξεις είναι $modulo\, n$.

Παράδειγμα

Η κατασκευή του $(n, w, 1) = (181, 6, 1) - OOC$.

Εφόσον, $n = 181$ και $w = 6$, υποτίθεται ότι $m = 3, r = 6, c = 36$. Επιλέγοντας, $\beta = 2$ την αρχική ρίζα του $GF(181)$, προκύπτουν τα υποσύνολα:

$T_0 = \{0,1,42,59,125,135\}$

$T_3 = \{0,8,95,110,155,175\}$

$T_6 = \{0,36,64,133,154,156\}$

$T_9 = \{0,107,146,150,159,162\}$

$T_{12} = \{0,5,29,82,114,132\}$

$T_{15} = \{0,7,40,51,113,151\}$

τα οποία είναι όλα κωδικές λέξεις του $(181, 6, 1) - OOC$. Όλες οι αριθμητικές πράξεις είναι $modulo$ 181.

Βιβλιογραφία

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

Σύνολα διαφορών, OOCs και σύγχρονοι OOCs

Ορισμός

Έστω ένα σύνολο k υπολοίπων $(mod\ v)$, $D = \{d_1, d_2, \dots, d_k\}$. Αν για κάθε υπόλοιπο $a \neq 0\ (mod\ v)$ η ισοδυναμία $d_i - d_j \equiv a\ (mod\ v)$ έχει ακριβώς λ ζεύγη λύσεων (d_i, d_j) όπου d_i, d_j ανήκουν στο D, τότε το σύνολο D ονομάζεται (v, k, λ) σύνολο διαφορών - difference set (DS).

Οι αριθμοί v, k, λ ονομάζονται παράμετροι του συνόλου διαφορών. Για το σύνολο διαφορών $D = \{d_1, d_2, \dots, d_k\}$ ισχύει $0 \leq d_1 \leq d_2 \leq \cdots \leq d_k < v$.

Παράδειγμα

Το σύνολο $D = \{1, 2, 4\}$ είναι ένα σύνολο διαφορών με παραμέτρους $(7, 3, 1)$; Σχηματίζοντας όλες τις ανά 2-διαφορές των στοιχείων του D προκύπτει ότι :

$1 - 2 = -1 \equiv 6\ (mod\ 7)$ $\quad$ $2 - 1 = 1 \equiv 1\ (mod\ 7)$
$1 - 4 = -3 \equiv 4\ (mod\ 7)$ $\quad$ $4 - 1 = 3 \equiv 3\ (mod\ 7)$
$2 - 4 = -2 \equiv 5\ (mod\ 7)$ $\quad$ $4 - 2 = 2 \equiv 2\ (mod\ 7)$

Με αυτόν τον τρόπο έχει σχηματιστεί το σύνολο των ανά 2-διαφορών των στοιχείων του D: $L = \{1, 2, 3, 4, 5, 6\}$.

Άρα, κάθε ένα από τα μη – μηδενικά υπόλοιπα $mod\ 7$ εμφανίζεται ακριβώς μία φορά $(\lambda = 1)$, και συνεπώς αποδεικνύεται το ζητούμενο.

Από τον ορισμό του συνόλου διαφορών, προκύπτει το ακόλουθο θεώρημα.

Θεώρημα

Μια αναγκαία και ικανή συνθήκη για την ύπαρξη ενός (v, k, λ) συνόλου διαφορών είναι η σχέση $\lambda(v - 1) = k(k - 1)$.

Απόδειξη:

Το πλήθος των δυνατών διαφορών ανά 2 των k στοιχείων του συνόλου $D = \{d_1, d_2, \dots, d_k\}$ είναι $k(k - 1)$. Επειδή κάθε υπόλοιπο από τα $1, 2, \dots, \mathrm{v} - 1$ πρέπει να προκύπτει με λ διαφορές, το πλήθος των δυνατών διαφορών ανά 2 των k στοιχείων του συνόλου D είναι $\lambda(v - 1)$. Συνεπώς, προκύπτει η ζητούμενη σχέση.

Ορισμός

Για κάθε θετικό ακέραιο v ορίζονται τα ακόλουθα σύνολα διαφορών $(mod\ v)$:

i. Το κενό σύνολο $D = \emptyset$

ii. $D = \{i\},\ 0 \le i \le v-1$
iii. $D = \{0, 1, \dots\ , v-1\}$
iv. $D = \{0, 1, \dots, i-1, i+1, \dots\ , v-1\}, 0 \le i \le v-1$
με παραμέτρους αντίστοιχα $(v, 0, 0),\ (v, 1, 0),\ (v, v, v), (v, v-1, v-2)$ ονομάζονται τετριμμένα και δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον.

Ενδιαφέρον παρουσιάζουν τα σύνολα διαφορών για τα οποία ισχύει $n \ge 2$, $όπου$ $n = k - \lambda.$

Κατασκευή συνόλων διαφορών

Για να κατασκευαστεί ένα (v, k, λ) σύνολο διαφορών πρέπει να σχηματιστούν $\binom{v}{k} = \frac{v!}{k!\cdot(v-k)!}$ υποσύνολα του συνόλου $V = \{0, 1, 2, \dots\ , v-1\}$ και να ελεγχθεί ποιο από αυτά ικανοποιεί τον ορισμό.

Παράδειγμα

Η τριάδα $(13, 4, 1)$ ικανοποιεί τη συνθήκη $\lambda(v-1) = k(k-1)$. Αυτό δεν αποκλείει την ύπαρξη ενός $(13, 4, 1)$ συνόλου διαφορών. Για να κατασκευαστεί αυτό το σύνολο διαφορών πρέπει να σχηματιστούν $\binom{13}{4} = 715$ υποσύνολα του συνόλου $V = \{0, 1, 2, \dots\ , 12\}$ και να ελεχθεί ποιο από αυτά ικανοποιεί τον ορισμό. Δηλαδή, για κάθε υποσύνολο του V πρέπει να σχηματιστούν όλες οι ανά 2 διαφορές των στοιχείων $(mod\ 13)$, τα υπόλοιπα των οποίων θα εμφανίζονται ακριβώς μία φορά.

Συνεπώς, η κατασκευή ενός συνόλου διαφορών με παραμέτρους (v, k, λ) είναι δύσκολο πρόβλημα.

Θεώρημα

Αν $D = \{d_1, d_2, \dots\ , d_k\}$ είναι ένα σύνολο διαφορών με παραμέτρους (v, k, λ) τότε και τα σύνολα:

i. $D + s = \{d_1 + s, d_2 + s, \dots\ , d_k + s\}\ (mod v),\ 0 \le s < v-1$
ii. $tD = \{td_1, td_2,\ \dots\ , td_k\}\ (mod v)\ ,\ (t, v) = 1$

είναι επίσης σύνολα διαφορών με τις ίδιες παραμέτρους. Το σύνολο $D + s$ λέγεται μετατόπιση – shift του D.

Κατασκευές από PDS και MG

Μια χρήσιμη μέθοδος για το σχεδιασμό OOCs, η οποία χρησιμοποιεί δύο μαθηματικές κατασκευές, δηλαδή το τέλειο σύνολο διαφορών - perfect difference set (PDS) και την πεπερασμένη γεωμετρία Möbius - finite Möbius geometry (MG), παρουσιάζεται στο [1].

Ένα k - υποσύνολο $D = \{d_1, d_2, \dots, d_k\}$ του $Z_n = \{0, 1, \dots, n-1\}$ καλείται $(n, k, \lambda) - PDS$ όποτε για κάθε $\alpha \not\equiv 0 \ (mod\ n)$ υπάρχουν ακριβώς λ διατεταγμένα ζεύγη (d_i, d_j), i ≠ j , έτσι ώστε $d_i - d_j \equiv a \ (mod\ n)$.

Η πεπερασμένη γεωμετρία Möbius $MG(q, r)$ όπου q είναι δύναμη πρώτου και r θετικός ακέραιος αριθμός, εκτεταμένο σώμα Galois $GF(q^r) \cup \{\infty\}$ με όλους τους κύκλους σε αυτό.

Με βάση την ένα προς ένα αντιστοιχία μεταξύ του $(q^{2r} + q^r + 1, q^r + 1, 1) - PDS$ και της $MG(q, r)$, ένας οπτικός ορθογώνιος κώδικας με παραμέτρους $(q^{2r} + q^r + 1, q^r + 1, 1, 2)$ και μέγεθος $2q^{r-1} \ \frac{q^{2r}-1}{q^2-1}$ μπορεί να επιτευχθεί.

Παράδειγμα

Εάν $q = 2, r = 2$ και ένας $(21, 3, 1, 2) - OOC$ με 20 κωδικές λέξεις. Το πλεονέκτημα αυτής της μεθόδου είναι η δυνατότητά του να παραγάγει μεγάλο αριθμό κωδικών λέξεων, αλλά η προϋπόθεση μικρού βάρους είναι ένα σημαντικό μειονέκτημα για αυτήν την κατασκευή.

Κυκλοτομικές Κατασκευές

Ορισμός

Έστω x μια πρωταρχική ρίζα του σώματος Galois $F = GF(q)$ όπου $q = ef + 1$ είναι μία δύναμη πρώτου αριθμού. Οι κυκλοτομικές κλάσεις (cyclotomic classes) ή σύμπλοκα (cosets) C_i στο σώμα είναι $C_i = \{x^{es+i} : s = 0,1, \dots, f-1\}, \ i = 0, \ 1, \ \dots, e-1.$

Τα C_i είναι ανά δύο ξένα μεταξύ τους και η ένωση τους δίνει το G, όπου $G = < x > -\{0\}$.

Ορισμός

Για σταθερά i, j ο κυκλοτομικός αριθμός (i, j) (cyclotomic number) ορίζεται να είναι ο αριθμός των λύσεων της εξίσωσης $z_i + 1 = z_j \ (z_i \in C_i, z_j \in C_j)$ όπου $1 = x^0$ να είναι η πολλαπλασιαστική μονάδα του F . Δηλαδή ο αριθμός (i, j) είναι ο αριθμός των διατεταγμένων ζευγών s, t τέτοιων ώστε $x^{es+i} + 1 = x^{et+j} \ (0 \le s, \ t \le f-1)$. Ο αριθμός $x^{es+i} - x^{et+k} \in C_j$ και είναι ο κυκλοτομικός αριθμός $(k - j, i - j)$.

Οι κυκλοτομικές κλάσεις και αριθμοί όσον αφορά το πεπερασμένο σώμα $GF(q)$ είναι μαθηματικές κατασκευές που μπορούν να χρησιμοποιηθούν για να κατασκευαστούν OOCs. Χρησιμοποιώντας αυτήν την μέθοδο, οι Ding και Xing παρουσίασαν διάφορες κατηγορίες $(2^m - 1, w, 2) - OOCs$ [2]. Επίσης, πέντε κατηγορίες $(q - 1, w, 2)$ – $OOCs$, όπου q είναι δύναμη περιττού πρώτου έχουν παραχθεί χρησιμοποιώντας κυκλοτομία.

Ορισμός

Το όριο του Johnson για $\lambda = 1$ δίνει το ακόλουθο άνω όριο στην Φ του κώδικα:

$$\Phi(n, w, 1) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \right\rfloor \right\rfloor.$$

Οι οπτικοί ορθογώνιοι κώδικες που ικανοποιούν το όριο Johnson καλούνται βέλτιστοι OOCs.

Υπάρχουν πολλές κατασκευές για τους OOCs με $\lambda = 1$.

Κατασκευές βέλτιστων OOCs

Στο επόμενο θεώρημα παρουσιάζεται μια νέα βέλτιστη κατασκευή για τους OOCs γενικεύοντας την κατασκευή Bose $(q^2 - 1, q, 1)$ [3] για διακεκριμένα σύνολα διαφορών, όπου q είναι δύναμη πρώτου.

Θεώρημα

Έστω F_{q^α} , $\alpha \geq 3$ είναι ένα πεπερασμένο σώμα με q^α στοιχεία. Έστω πολυώνυμα της μορφής: $P_{l,i}(\theta) = \theta^i + l_{i-1}\theta^{\alpha-1} + \ldots + l_1\theta$, $1 \leq i \leq (\alpha - 1)$ όπου $l \in F_q$ και θ είναι το πρώτο στοιχείο του F_{q^α}. Για κάθε τέτοιο πολυώνυμο δίνεται κωδική λέξη του OOC που έχει ακριβώς «μία» αντιστοιχία στο συνδυασμό $log_\beta (P_{l,i}(\theta) + u)$ για κάθε μη μηδενικό $u \in F_q$, όπου β είναι ένα άλλο πρώτο στοιχείο του F_{q^α}. Αυτό οδηγεί στην κατασκευή $(q^\alpha - 1, q, 1) - OOC$ με $\Phi = q^{\alpha-2} + q^{\alpha-3} + \cdots + 1$.

Κατασκευές DDS και DTS

Οι οπτικοί ορθογώνιοι κώδικες για $\lambda = 1$ συμπίπτουν με τα διακεκριμένα σύνολα διαφορών - distinct difference sets (DDS), και μπορούν να χρησιμοποιηθούν για να κατασκευαστούν τριγωνικά σύνολα διαφορών - difference triangle sets (DTS).

Ορισμός

Το (v, k, t) διακεκριμένο σύνολο διαφορών (DDS) τάξης v , είναι μια οικογένεια $(B_i \mid i \in I, t = |I|)$ του υποσυνόλου $\mathbb{Z}_v$ πληθικότητας - k, έτσι ώστε κάθε μη μηδενικό στοιχείο $g \in \mathbb{Z}_v$ να εμφανίζεται το πολύ μια φορά μεταξύ των διαφορών $(\alpha - b \mid \alpha, b \in B_i ; \alpha \neq b; i \in I)$.

Ορισμός

Ένα (I, J) τριγωνικό σύνολο διαφορών είναι ένα σύνολο $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_I\}$, όπου $\Delta_i = \{ a_{ij} \mid 0 \leq j \leq J \}$ για $1 \leq i \leq I$ είναι σύνολα ακεραίων έτσι ώστε οι διαφορές $a_{ij} - a_{ij'}$ να είναι διαφορετικές με $1 \leq i \leq I$ και $0 \leq j' \neq j \leq J$.

Θεώρημα

Ένας οπτικός ορθογώνιος κώδικας έχοντας τη μορφή $(n, w, 1)$ είναι ένα (v, k, t) διακεκριμένο σύνολο διαφορών με $n = v,\ k = w,\ \Phi(n, w, 1) = t$. Και επιπλέον, κάθε $(n, w, 1)$ οπτικός ορθογώνιος κώδικας με Φ κωδικές λέξεις ή ένα (n, w, Φ) διακεκριμένο σύνολο διαφορών δίνει ένα (I, J) τριγωνικό σύνολα διαφορών με $J = w - 1$, $I = \Phi$.

Θεώρημα

Έστω ένας $(n, w, 1)$ οπτικός ορθογώνιος κώδικας μεγέθους $\Phi(n, w, 1)$ και $n \neq 0\ (mod\ w)$, για κάθε r , ο μέγιστος κοινός διαιρέτης του $(r, (w-1)!)$ ισούται με 1, και έστω ένας άλλος $(nr, w, 1)$ οπτικός ορθογώνιος κώδικας μεγέθους

$$\Phi(nr, w, 1) = r\,\Phi(nr, w, 1).$$

Επιπλέον, εάν υπάρχει ένας $(r, w, 1)$ οπτικός ορθογώνιος κώδικας μεγέθους $\Phi'(r, w, 1)$, τότε θα υπάρχει και ένας $(nr, w, 1)$ οπτικό ορθογώνιο κώδικα μεγέθους

$$\Phi(nr, w, 1) = r\,\Phi(n, w, 1) + \Phi'(r, w, 1).$$

Ορισμός

Ένας (n, w, λ) σύγχρονος οπτικός ορθογώνιος κώδικας – synchronous optical orthogonal codes $(SOOC)$ είναι μια οικογένεια από {0,1} ακολουθίες μεγέθους n, με βάρος Hamming w και συντελεστή συσχέτισης λ που ικανοποιεί τη σχέση:

$$C_{x,y}(0) \leq \lambda, \qquad \forall \mathrm{x} \neq \mathrm{y}$$

Ορισμός

Ένας (n, w, λ) κυκλικός σύγχρονος οπτικός ορθογώνιος κώδικας - cyclic synchronous optical orthogonal codes $(CSOOC)$ είναι ένας σύγχρονος οπτικός ορθογώνιος κώδικας στον οποίο όλες οι n κυκλικές μετατοπίσεις κάθε κωδικής λέξης είναι διαφορετικές κωδικές λέξεις μέσα στον κώδικα.

Θεώρημα

Κάθε (n, w, λ) οπτικός ορθογώνιος κώδικας μεγέθους Φ δίνει (n, w, λ) έναν κυκλικό σύγχρονο οπτικό ορθογώνιο κώδικα μεγέθους $n\Phi$.

Βιβλιογραφία

[1] C.S. Weng and J. Wu, “Optical orthogonal codes with nonideal cross-correlation,” Journal of Lightwave Technology, vol. 19, no. 12, pp. 1856-1863, December 2001.

[2] C. Ding and C. Xing, “Several classes of (2m−1,w ,2) optical orthogonal codes,” Discrete Applied Mathematics 128 (2003) 103-120.

[3] R.C.Bose, “An affine analogue of Singer’s theorem,” J. Ind, Math. SOC., vol. 6, pp. 1-15, 1942.

Οικογένειες διαφορών και βέλτιστοι OOCs

Το κύριο αποτέλεσμα της εργασίας του RM Wilson, που δημοσιεύθηκε στην εφημερίδα «Θεωρία Αριθμών» το 1972, είναι το θεώρημα ασυμπτωτικής ύπαρξης (ένα ορόσημο στη θεωρία σχεδιασμού). Στην συγκεκριμένη εργασία, παρουσιάστηκαν επίσης κάποιες βασικές κατασκευές για τις απλές οικογένειες διαφορών (και κατά συνέπεια 2-σχέδιασμών Steiner) οι οποίες είναι αξιοσημείωτες. Τέλος, ο Wilson καταλήγει στο συμπέρασμα ότι η θεωρία πεπερασμένων σωμάτων διευκολύνει το έργο της κατασκευής στις οικογένειες διαφορών.

Αυτή η ενότητα, θα αξιοποιήσει με επιτυχία αυτές τις δυνατότητες, προκειμένου να δημιουργηθούν οικογένειες διαφορών και βέλτιστοι οπτικοί ορθογώνιοι κώδικες. Θα αναλύσει τον τρόπο με τον οποίο επιτυγχάνεται η δημιουργία μιας οικογένειας διαφορών από πεπερασμένο σώμα, σύμφωνα με τον Wilson, και θα παρουσιάσει ένα θεώρημα (με πορίσματα όλες τις γνωστές και άμεσες τεχνικές που στηρίζονται στο σώμα Galois) το οποίο χρησιμοποιείται σαν μια πολύ αποτελεσματική μέθοδος για να κατασκευαστούν πολλές οικογένειες διαφορών, αλλά και βέλτιστοι οπτικοί ορθογώνιοι κώδικες. Αρχικά, όμως, θα προηγηθεί κάποιο υπόβαθρο.

I. Εισαγωγή

Ορισμός

Έστω G μια ομάδα με πράξη την πρόσθεση και έστω $\mathcal{F} = \{B_1, \dots, B_t\}$ μια οικογένεια από k – υποσύνολα του $G : B_i = \{B_{i1}, B_{i2}, \dots, B_{ik}\}$, $i = 1, 2, \dots t$. Μια τέτοια οικογένεια καλείται (G, k, λ) οικογένεια διαφορών (difference family) ή εν συντομία $(v, k, \lambda) - DF$, όταν ισχύουν οι ακόλουθες συνθήκες:

σε κάθε μη μηδενικό στοιχείο της G, υπάρχει ακριβώς λ φορές στις λίστες διαφορών

(1) $(b_{ij} - b_{ih} \mid 1 \le i \le t, 1 \le j \ne h \le k)$
(2) $[B_i + g = B_i \iff g = 0]$ $\gamma\iota\alpha$ $i = 1, 2, \dots t$

Ορισμοί

Τα μέλη μιας οικογένειας συνόλων καλούνται blocks βάσης (base blocks). Μια οικογένεια συνόλων μ' έναν ενιαίο block βάσης καλείται σύνολο διαφορών. Μια $(G, k, \lambda) - DF$ λέγεται απλή όταν $\lambda = 1$. Μια $(\mathbb{Z}_v, k, \lambda) - DF$ καλείται κυκλική και συμβολίζεται $(v, k, \lambda) - DF$.

Έστω $\mathcal{F} = \{B_1, \dots, B_t\}$ μια οικογένεια μη κενών υποσυνόλων μιας προσθετικής ομάδας G. Το ανάπτυγμα της $\mathcal{F}$ έχει ως συχνότερη δομή την εξής: $\mathcal{F} = (G, \mathcal{B}, \varepsilon)$ με $\mathcal{B} := \{ B_i + g \mid i = 1, 2, \dots t ; g \in G \}$.

Η ακόλουθη πρόταση εξηγεί το λόγο για τον οποίο οι οικογένειες συνόλων έχουν μεγάλο ενδιαφέρον στη θεωρία σχεδιασμών:

Πρόταση 1

Έστω G μια ομάδα με πράξη την πρόσθεση τάξης v και με κλάση που έχει ως συχνότερη δομή το ανάπτυγμα κάποιας (G, k, λ) οικογένειας διαφορών. Μια τέτοια κλάση συμπίπτει με την κλάση $2 - (v, k, \lambda)$ σχεδιασμού που έχει την G ως ομάδα αυτομορφισμού που ενεργεί ομαλά ή κανονικά σ' ένα σημειοσύνολο και ημιομαλά ή ημικανονικά στο σύνολο των μπλοκ.

Συγκεκριμένα οι $(v, k, 1) - DFs$ δίνουν κυκλικούς σχεδιασμούς S $(2, k, v)$ χωρίς σύντομες τροχιές.

Ακολουθεί ο ορισμός της έννοιας του οπτικού ορθογώνιου κώδικα. Ο ορισμός αυτός είναι πιο γενικός από τον πρωτότυπο που αναφέρεται στο [1], αλλά συμπίπτει με αυτόν όταν η G είναι κυκλική ομάδα ενός ακέραιου αριθμού $modulo\ v$.

Ορισμός

Έστω G μια ομάδα με πράξη την πρόσθεση, και έστω C ένα υποσύνολο του $(\mathbb{Z}_2)^G$, του οποίου τα στοιχεία έχουν σταθερό βάρος Hamming k. Με άλλα λόγια, οποιοδήποτε στοιχείο του C ικανοποιεί την απεικόνιση $x : G \to \mathbb{Z}_2 : g \to x_g$ τέτοια ώστε $|g \in G : x_g = 1| = k$. Το σύνολο C λέγεται (G, k, λ) οπτικός ορθογώνιος κώδικας, εν συντομία (G, k, λ) - OOC, όταν για κάθε ζεύγος διακριτών στοιχείων $x\ και\ y$ του C ισχύουν οι ακόλουθες προϋποθέσεις:

$$\sum_{g \in G} x_{g+h} \cdot x_{g+h'} \leq \lambda \quad , \quad \forall\, h, h' \in G, h \neq h'$$

$$\sum_{g \in G} x_{g+h} \cdot y_{g+h'} \leq \lambda \quad , \quad \forall\, h, h' \in G$$

(3a), (3b) αντίστοιχα.

Ορισμοί

Το πλήθος των στοιχείων και τα στοιχεία του C ονομάζονται μέγεθος και κωδικές λέξεις του C αντίστοιχα.
Ένας $(G, k, \lambda) - OOC$ καλείται βέλτιστος οπτικός ορθογώνιος κώδικας (optimal optical orthogonal code - OOOC) , όταν δεν υπάρχει $(G, k, \lambda) - OOC$ που να έχει μεγαλύτερο μέγεθος.

Ένας $(G, k, \lambda) - OOC$ καλείται απλός (simple) ορθογώνιος κώδικας όταν λ=1.

Ένας $(\mathbb{Z}_v, k, \lambda) - OOC$ καλείται κυκλικός (cyclic) και συμβολίζεται ως $(v, k, \lambda) - OOC$.

Όταν $G = \mathbb{Z}_v$ οι σχέσεις (3a), (3b) υποδηλώνουν ότι το εσωτερικό γινόμενο μεταξύ δύο διακεκριμένων κυκλικών μετατοπίσεων μιας κωδικής λέξης (δύο κυκλικές μετατοπίσεις των διακεκριμένων κωδικών λέξεων αντίστοιχα) είναι το πολύ λ.

Έστω C ένας $(G, k, \lambda) - OOC$ μεγέθους t. Κάθε κωδική λέξη x του C, μπορεί να προσδιοριστεί από ένα υποσύνολο B της G, με k-στοιχεία, του οποίου η χαρακτηριστική συνάρτηση για το x είναι:

$$B := \{ g \in G \mid x_g = 1\}.$$

Ο C μπορεί να οριστεί ως μια οικογένεια $\mathcal{F} = \{\mathrm{B}_1, \dots, \mathrm{B}_t\}$ k-υποσυνόλων της G (σύνολα κωδικών λέξεων) ικανοποιώντας τις εξής συνθήκες:

$|(B_i + h) \cap (B_i + h')| \leq \lambda, \forall\, i \in \{1, 2, \dots, t\}\ ,\ \forall\, h \neq h' \in G$ (4a)

$|(B_i + h) \cap (B_i + h')| \leq \lambda, \forall\, i \neq j \in \{1, 2, \dots, t\}\ ,\ \forall\, h, h' \in G$ (4b)

Οι σχέσεις (4a) και (4b) είναι ισοδύναμες με τις ακόλουθες:

Κάθε μη μηδενικό στοιχείο της G εμφανίζεται το πολύ λ φορές στις λίστες διαφορών $(b - b' \mid b, b' \in \mathrm{B_i}, 1 \leq i \leq t)$ (4c)

Κάθε μη μηδενικό στοιχείο της G εμφανίζεται το πολύ λ φορές στις λίστες διαφορών $(b - b' \mid b \in B_i, b' \in B_j, 1 \leq i \neq j \leq t)$ (4d)

Άρα, ένας $(G, k, \lambda) - OOC$ θεωρείται οικογένεια $\{B_i\}$ k-υποσυνόλων της G αν ικανοποιεί τις (4c), (4d). Υπό αυτές τις συνθήκες, εύκολα γίνεται αντιληπτό ότι κάθε $(G, k, 1)$ οικογένεια διαφορών μπορεί να αντιμετωπιστεί σαν ένας $(G, k, 1)$ οπτικός ορθογώνιος κώδικας.

Η μελέτη του (v, k, λ) οπτικού ορθογώνιου κώδικα αρχικά υποκινήθηκε από μια εφαρμογή στην πολλαπλή προσπέλασης διαίρεσης κώδικα σε οπτικά συστήματα επικοινωνιών. Ο κύριος λόγος που προκλήθηκε η γενίκευση της έννοιας $(v, k, \lambda) - OOC$ με εκείνη της $(G, k, \lambda) - OOC$ είναι χάρη της ομοιομορφίας της γλώσσας. Από την άλλη πλευρά, πιστεύεται ότι, αυτή η γενίκευση είναι δικαιολογημένη και συγκεκριμένα για $\lambda = 1$. Διαπίστωση που προκύπτει από την επόμενη πρόταση (ανάλογη της πρότασης 1).

Πρόταση

Η κλάση με κατασκευή αντιστοιχίας, που είναι το ανάπτυγμα κάποιων $(G, k, 1)$– OOC, συμπίπτει με την κλάση του k-ομοιόμορφου ημιγραμμικού χώρου επιτρέποντας στη G, ως ομάδα αυτομορφισμού, να ενεργεί ομαλά ή κανονικά σ' ένα σημειοσύνολο και ημιομαλά ή ημικανονικά σ' ένα γραμμικό σύνολο.

Σημείωση

Για ένα υποσύνολο B μιας προσθετικής ομάδας G, αποδεικνύεται από το ΔB ότι το σύνολο (όχι η λίστα) από όλες τις μη μηδενικές διαφορές στο B είναι:

$$\Delta B := \{ b - b' \mid b, b' \in B, b \neq b' \}$$

Χρησιμοποιείται η ακόλουθη πρόταση για απλούς OOCs:

Πρόταση

Έστω G μια ομάδα με πράξη την πρόσθεση και $\mathcal{F} = \{\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_t\}$ οικογένεια k–υποσυνόλων της G. Για να είναι $\mathcal{F}$ ένας $(G, k, \lambda)-OOC$ αρκεί:

$|\Delta B_i| = k(k-1)$ για $1 \leq i \leq t$

$\Delta B_i \cap \Delta B_j = \emptyset$ για $1 \leq i < j \leq t$

Αν επιπλέον ισχύει $t = \left\lfloor \frac{v-1}{k^2-k} \right\rfloor$ (δηλαδή το ακέραιο μέρος του $\frac{v-1}{k^2-k}$) τότε ο κώδικας είναι βέλτιστος.

Οι οικογένειες συνόλων και οι οπτικοί ορθογώνιοι κώδικες θεωρούνται απλές και απλοί έχοντας οριστεί από προσθετική ομάδα πεπερασμένου πεδίου.

Σημείωση

Έστω q δύναμη πρώτου και έστω d οποιοσδήποτε διαιρέτης του $q-1$. Ορίζονται:

$GF(q)$: Galois field – σώμα Γκαλουά τάξης q

$EA(q)$: στοιχειώδη αβελιανή ομάδα - elementary abelian q τάξης,
δηλαδή το $GF(q)$ είναι ομάδα εφοδιασμένη με την πρόσθεση

$\omega :=$ σταθερό πρωτογενή στοιχείο του $GF(q)$

$H^d :=$ ομάδα του $GF(q)$ δύναμης d

Συγκεκριμένα, $H^1 = H$ είναι πολλαπλασιαστική ομάδα του $GF(q)$.
Αν $q-1 = d \cdot n$, τότε η H^d θεωρείται n-οστη ρίζα της μονάδας στο $GF(q)$.

II. Οικογένειες διαφορών μέσω Πεπερασμένων πεδίων

Σε αυτή την παράγραφο, θα εξεταστούν τα θεωρήματα που οδηγούν στις γνωστές και άμεσες κατασκευές απλών DFs των πεδίων Galois. Για λόγους συντομίας δεν προσδιορίζονται οι κατασκευές με εντολές.

Θεώρημα 2.1 (Bose)

Αν $q = 12t + 1$ είναι δύναμη πρώτου έτσι ώστε $\omega^{4t} - 1$ να μην είναι τέλειο τετράγωνο του $GF(q)$ (ισοδύναμα, το -3 δεν είναι 4η δύναμη), τότε θα υπάρχει μία $(EA(q), 4, 1)$ – DF.

Θεώρημα 2.2 (Bose)

Αν $q = 20t + 1$ είναι δύναμη πρώτου έτσι ώστε $\omega^{4t} + 1$ να μην είναι τέλειο τετράγωνο του $GF(q)$ (ισοδύναμα, το 5 δεν είναι 4η δύναμη), τότε θα υπάρχει μία $(EA(q), 5, 1)$ – DF.

Τα Θεωρήματα 2.1 και 2.2 έχουν βελτιωθεί και διατυπώνονται ως εξής:

Θεώρημα 2.3 (Buratti)

Εστω ότι $q = 12t + 1$ είναι δύναμη πρώτου και έστω 2^n είναι η μεγαλύτερη δύναμη του 2 στο t. Αν $\omega^{4t} - 1 \notin H^{2^{n+1}}$ (ισοδύναμα, το -3 δεν ανήκει στην $H^{2^{n+2}}$), τότε θα υπάρχει μία $(EA(q), 4, 1)$ – DF.

Θεώρημα 2.4 (Buratti)

Έστω ότι $q = 20t + 1$ είναι δύναμη πρώτου και έστω 2^n είναι η μεγαλύτερη δύναμη του 2 στο t. Αν $\omega^{4t} + 1 \notin H^{2^{n+1}}$ (ισοδύναμα, $(11 + 5\sqrt{5})$ / 2 δεν ανήκει στην $H^{2^{n+1}}$), τότε θα υπάρχει μία $(EA(q), 5, 1)$ – DF.

Το Θεώρημα 2.3 ισχύει για δυνάμεις πρώτων $p \equiv 2\ (mod\ 3)$ και το Θεώρημα 2.4 ισχύει για δυνάμεις πρώτων $p \equiv \pm 2\ (mod\ 5)$.

Τα Θεωρήματα 2.3 και 2.4 παρέχουν ικανές και αναγκαίες συνθήκες για την ύπαρξη οικογένειας συνόλων αποτελούμενων από κατάλληλα σύμπλοκα του $GF(q)$, ενώ οι συνθήκες των θεωρημάτων του Bose είναι μόνο επαρκής γι 'αυτό.

Θεώρημα 2.5 (Wilson)

Έστω $q = k\ (k-1)t + 1$ δύναμη πρώτου και $k -$ περιττός.

Αν το σύνολο $\{\omega^{i(k-1)t} - 1 \mid 1 \leq i \leq \frac{1}{2}\ (k-1)\}$ είναι ένα πλήρες σύστημα αντιπροσώπων για το σύμπλοκο $H^{(k-1)/2}$, τότε θα υπάρχει μία $(EA(q), k, 1)$ – DF.

Θεώρημα 2.6 (Wilson)

Έστω $q = k\,(k-1)\,t\,+1$ δύναμη πρώτου και k – ζυγός.

Αν το σύνολο $\{\omega^{ikt} - 1 \mid 1 \leq i \leq \frac{1}{2}\,k\,-1\} \cup \{1\}$ είναι ένα πλήρες σύστημα αντιπροσώπων για το σύμπλοκο $H^{k/2}$, τότε θα υπάρχει μία $(EA(q), k, 1) - DF$.

Τα παραπάνω θεωρήματα του Wilson, παρέχουν επαρκείς προϋποθέσεις για να υπάρχουν ριζικές οικογένειες διαφορών - radical difference families (RDF), δηλαδή οι οικογένειες διαφορών DFs αποτελούν κατάλληλα σύμπλοκα για $GF(q)$, και είναι γενικεύσεις των θεωρημάτων Bose, οι οποίες αντιστοιχούν σε περιπτώσεις $k = 4$ και $k = 5$.

Οι όροι των επόμενων δύο θεωρημάτων είναι επαρκής για την ύπαρξη των RDF, βελτιώνουν τους όρους των θεωρημάτων Wilson, επειδή είναι πιο αδύναμοι και είναι αναγκαίοι τουλάχιστον για k ≤ 7.

Θεώρημα 2.7 (Buratti)

Έστω $q = k\,(k-1)\,t + 1$ δύναμη πρώτου και k – περιττός.
Έστω $d_1 \mid d_2 \mid \ldots \mid d_{2s}$ σύνολο με διαιρέτες του $\frac{1}{2}(k-1)t$ τέτοιο ώστε:

i. $\prod_{1\leq a\leq s} d_{2a}/d_{2a-1} = \frac{1}{2}(k-1)$
ii. Για κάθε ζεύγος διακεκριμένων στοιχείων x, y στο σύνολο $\{\omega^{i(k-1)t} - 1 \mid 1 \leq i \leq \frac{1}{2}\,(k-1)\}$ θα υπάρχει κατάλληλο $\alpha \in \{1, \ldots, s\}$ τέτοιο ώστε x, y να ανήκουν σε διακεκριμένα σύμπλοκα του $H^{d_{2a-1}}$ modulo$(H^{d_{2a}})$, δηλαδή $x^{-1}y \in H^{d_{2a-1}} \backslash H^{d_{2a}}$

Τότε, θα υπάρχει μία $(EA(q), k, 1) - DF$.

Θεώρημα 2.8 (Buratti)

Έστω $q = k\,(k-1)\,t + 1$ δύναμη πρώτου και k – ζυγός.
Έστω $d_1 \mid d_2 \mid \ldots \mid d_{2s}$ σύνολο με διαιρέτες του $\frac{1}{2}k$ τέτοιο ώστε:

i. $\prod_{1\leq a\leq s} d_{2a}/d_{2a-1} = \frac{1}{2}k$
ii. Για κάθε ζεύγος διακριτών στοιχείων x, y στο σύνολο $\{\omega^{ikt} - 1 \mid 1 \leq i \leq \frac{1}{2}\,k\,-1\} \cup \{1\}$ θα υπάρχει κατάλληλο $\alpha \in \{1, \ldots, s\}$ τέτοι ώστε x, y να ανήκουν σε διακεκριμένα σύμπλοκα της $H^{d_{2a-1}}$ $modulo(H^{d_{2a}})$, δηλαδή $x^{-1}y \in H^{d_{2a-1}} \backslash H^{d_{2a}}$

Τότε, θα υπάρχει μία $(EA(q), k, 1) - DF$.

Το επόμενο θεώρημα, εκτός του ότι είναι πολύ χρήσιμο για την κατασκευή DFs με "μικρό" μέγεθος block, αξίζει της προσοχής κυρίως επειδή οδηγεί προς το θεώρημα Wilson ασυμπτωτικής ύπαρξης, ένα από τα πιο σημαντικά αποτελέσματα στη θεωρία σχεδιασμού, που αναφέρεται στο [2].

Θεώρημα 2.9 (Λήμμα του Wilson σε block με ομοιόμορφα κατανεμημένες διαφορές)

Έστω $q = k\,(k-1)\,t+1$ δύναμη πρώτου, και έστω B ένα k – υποσύνολο του $GF(q)$ έτσι ώστε κάθε σύμπλοκο της $H^{k(k-1)t+1}$ να περιέχει ακριβώς δύο στοιχεία (αντίθετα μεταξύ τους) του ΔB. Τότε θα υπάρχει μία $(EA(q), k, 1)$ – DF.

Το Θεώρημα 2.9 είναι αποτελεσματικό για χαμηλές τιμές του k. Πολλές DFs με μέγεθος block 4 και 5 είναι εύκολο να επιτευχθούν. Ο Wilson αποδεικνύει ότι για ορισμένο αυθαίρετο k, η κατάσταση του Θεωρήματος 2.9 είναι ασυμπτωτικά επαληθεύσιμη. Αυτό, σε συνδυασμό με τις κατασκευές των αναδρομικών τύπων, σημαίνει ότι για επαρκώς μεγάλο v οι προϋποθέσεις $v-1 \equiv 0\,(mod\,k-1)$ και $v\,(v-1) \equiv 0\,(mod\,k\,(k-1))$ είναι απαραίτητες και επαρκείς για την ύπαρξη $S\,(2,k,v)$ σχεδιασμού.

Ο Wilson πραγματεύτηκε και το ακόλουθο θεώρημα, για απλές DFs με μέγεθος block 6.

Θεώρημα 2.10 (Wilson)

Έστω $q = 30t+1$ δύναμη πρώτου και υποθέτοντας ότι υπάρχει ένα στοιχείο b στο πεδίο Galois $GF(q)$, τέτοιο ώστε το σύνολο

$$\{\omega^{10t}-1, b(\,\omega^{10t}-1), b-1, b-\,\omega^{10t}, b-\,\omega^{20t}\}$$

να είναι ένα πλήρες σύστημα αντιπροσώπων για σύμπλοκα $5^{ης}$ τάξης.

Τότε, θα υπάρχει μία $(EA(q), 6, 1)$ – DF.

III. Κύρια κατασκευή

Σύμφωνα με τον Wilson, ένα πολύ χρήσιμο θεώρημα για να κατασκευαστούν όχι μόνο οικογένειες διαφορών αλλά και βέλτιστοι οπτικοί ορθογώνιοι κώδικες είναι το ακόλουθο. Αυτό το θεώρημα έχει μια ενωτική λειτουργία σε σχέση με όσα διατυπώθηκαν, τα οποία είναι απόρροια αυτού. Αναζητούνται οικογένειες από το $GF(q)$ των οποίων τα μέλη είναι ενώσεις συμπλόκων της πολλαπλασιαστικής υποομάδα του $GF(q)$ και ενδεχομένως του $\{0\}$.

Σκοπός του θεωρήματος είναι ο μετασχηματισμός κάποιων γνωστών κατασκευών των DFs μέσω $GF(q)$ για να κατασκευαστούν $OOOCs$.

Θεώρημα 3.1

Έστω $k = e \cdot f$ ή $k = e \cdot f + 1$, e - περιττός και στις δύο περιπτώσεις.
Έστω q δύναμη πρώτου έτσι ώστε η Ευκλείδεια Διαίρεση του $q - 1$ με το $k \cdot (k - 1)$ να είναι ο εξής τύπος:

$$q - 1 = k \cdot (k-1)t + r, 0 \le r < k(k-1) \text{ , το } r \text{ διαιρείται από το } 2et \quad (3.1.a)$$

Το σύνολο $\left\{\varepsilon = \omega^{\frac{q-1}{e}}\right\}$ συνδέεται με κάθε f – υποσύνολο $B = \{ b_1 = 1, b_2 , \dots , b_f \}$ της H και ο πίνακας L_B ορίζεται:

$$L_B := (b_i - b_j e^h \mid \left[1 \le i = j \ \le f, 1 \le h \le \frac{1}{2}(e-1)\right]$$

$$\text{ή} \qquad [1 \le i < j \le f, 1 \le h \ \le e] + L^*{}_B$$

Όπου $L^*{}_B$ είναι ο μηδενικός πίνακας για $k = e \cdot f$, ενώ $L^*{}_B$ είναι η λίστα $(b_1, b_2 , \dots , b_f)$ των στοιχείων του B για $k = e \cdot f + 1$.

Έστω $(H^{d_1} \supset \cdots \supset H^{d_{2s}})$ αλυσίδα υποομάδων μεταξύ H και $H^{(q-1)/(2e)}$ – συνεπώς $(\mathrm{d}_1, \dots, \mathrm{d}_{2s})$ αλυσίδα από διαιρέτες των $(q-1)/(2e)$ – και έστω $d_0 = 1$, $d_{2s+1} = (q-1)/(2e)$. Αν B είναι ένα f - υποσύνολο της H τέτοιο ώστε: το L_B είναι υποσύνολο της H, δηλαδή το L_B δεν έχει επαναλαμβανόμενο στοιχείο και δεν περιέχει το μηδέν. (3.1.b)

$\prod_{0 \le a \le s} \frac{d_{2a+1}}{d_{2a}} = t$ (3.1.c)

$xy^{-1} \in \bigcup_{1 \le a \le s} \left(H^{d_{2a-1}} \backslash H^{d_{2a}}\right) \cup \{1\} \ \forall \, x, y \in L_B$ (3.1.d)

Τότε, εάν οριστεί

$$I := \left\{ \sum_{a=0}^{s} d_{2a} i_a \ \middle| \ 0 \le i_a \le \frac{d_{2a+1}}{d_{2a}} \, ; a = 0, 1, \dots , s \right\}$$

Τότε, θα υπάρχει οικογένεια $\mathcal{F} := \left\{\omega^i B \cdot \ H^{(q-1)/e} \ \cup B^* \,\middle|\, i \in I \right\}$,

όπου $B^* = \emptyset$ ή $B^* = \{0\}$ σύμφωνα με $k = e \cdot f$ ή $k = e \cdot f + 1$ αντίστοιχα, που είναι

ένας $(EA(q), k, 1)$ – βέλτιστος οπτικός ορθογώνιος κώδικας - OOOC.

Συγκεκριμένα, αν $r = 0$ τότε, θα είναι μία $(EA(q), k, 1)$ – DF.

Παρατηρήσεις:

i. Ο λόγος για τον οποίο στη σχέση (3.1.a) το r απαιτείται να είναι διαιρέσιμο με $2et$ (αυτό σημαίνει ότι η μόνη διαιρετότητα με το $2e$ είναι απαραίτητη για να αποδειχθεί το Θεώρημα 3.1) είναι για να υπάρχει συμβατότητα με την (3.1.c). Αν ισχύει η (3.1.c) τότε λύνοντας την, για d_{2s+1} προκύπτει

$d_{2s+1} = \frac{(q-1)}{(2e)} = t \cdot (\prod_{1 \le a \le s} d_{2a} / d_{2a-1})$ και άρα, το $2et$ είναι διαιρέτης του $q - 1$ και συνεπώς του r.

ii. Το σύνολο $m = (q-1)/(2e)$. Ο πιο απλός τρόπος για να εφαρμοστεί το Θεώρημα (3.1), είναι να βρεθεί ένα f – υποσύνολο B της H έτσι ώστε κάθε δύο στοιχεία του L_B να είναι διακεκριμένα σύμπλοκα της H^m. (3.2.a) Αν ισχύει η (3.2.a) τότε οι συνθήκες (3.1.b,c,d) επαληθεύονται στην περίπτωση της τετριμμένης αλυσίδας $H \supseteq H^m$. Σε αυτήν την περίπτωση, η περιγραφή της οικογένειας διαφορών είναι ευκολότερη.

iii. Με τις εκτιμήσεις όπως έγιναν για τις ριζικές οικογένειες διαφορών, είναι πιθανόν να δειχθεί ότι οι συνθήκες (3.1.b,c,d) είναι ισοδύναμες με τη συνθήκη (3.2.a), όταν το m και το t είναι σχετικά πρώτοι. Όμως, όταν $MK\Delta(m,t) \neq 1$ οι συνθήκες (3.1.b,c,d) είναι σχετικά αδύνατες σε σχέση με την (3.2.a).

iv. Οποιοδήποτε θεώρημα της παραγράφου 2 μπορεί να ληφθεί ως πόρισμα του Θεωρήματος 3.1. Για παράδειγμα, για $e = 1$ και $r = 0$, η συνθήκη (3.2.a) συμπίπτει με το λήμμα Wilson στα block με τις ομοιόμορφα κατανεμημένες διαφορές.

v. Από την προηγούμενη παρατήρηση και χρησιμοποιώντας το θεώρημα Wilson ασυμπτωτικής ύπαρξης ισχύει ότι για οποιοδήποτε k- σταθερό το Θεώρημα 3.1 οδηγείται, τουλάχιστον θεωρητικά, σε μια άπειρη κατηγορία $(EA(q), k, 1) - DFs$. Αντιθέτως, για οποιοδήποτε k - σταθερό, το θεώρημα 3.1 οδηγεί σε έναν πεπερασμένο αριθμό $(EA(q), k, 1) - OOOCs$ που δεν είναι DFs. Στην πραγματικότητα, η (3.1.a) δίνει: $r \le k(k-1) - 2$, ($r \neq k(k-1) - 1$, επειδή r είναι άρτιος) και άρα όταν $r \neq 0$, δεδομένου ότι $2t$ διαιρεί το r, $t \le \frac{1}{2} r \le \frac{1}{2} k(k-1) - 1$. Συμπερασματικά, $q < \frac{1}{2}(k^2 - k)^2$.

vi. Φυσικά, ο αριθμός αντιπροσώπων ενός ακέραιου αριθμού k στη μορφή $k = e \cdot f$ ή $k = e \cdot f + 1$ με e περιττό, είναι το άθροισμα περιττών αριθμών που διαιρούν το k και οι περιττοί αριθμοί που διαιρούν το $k - 1$. Αυτό το άθροισμα είναι ελάχιστο και ίσο με 3 όταν το k είναι πρώτος Mersenne ή δύναμη του 2 που προηγείται από έναν πρώτο. Επομένως, μέγιστη δυσκολία υπάρχει στην εφαρμογή του Θεωρήματος 3.1 σε αυτές τις τιμές του k.

Βιβλιογραφία

[1] Chang, E R. K., Salehi, J. A., and Wei, V. K. 1989. Optical orthogonal codes: design, analysis and applications. IEEE Transactions of lnformation Theory 35(3):595-504.

[2] Wilson, R. M. 1972a. Cyclotomy and difference families in elementary abelian groups. J. Number Theory 4:17-42.

Αναδρομικές Κατασκευές

Σύντομες κατασκευές

Ένας $(v_1v_2, k, 1) - OOC$, C , μπορεί να κατασκευαστεί χρησιμοποιώντας έναν $(v_1, k, 1) - OOC$, C_1 και έναν $(v_2, k, 1) - OOC$, C_2. Ο C είναι βέλτιστος OOC αν οι C_1, C_2 είναι βέλτιστοι $OOCs$.

Ορισμός

Πίνακας διαφορών (difference array) $DA(s, n)$ ορίζεται ο πίνακας $M = [m_{ij}]$ διάστασης $s \times n$, τέτοιος ώστε $m_{ij} \in \{0, 1, 2, \dots, n-1\}$. Για κάθε δύο γραμμές ($M_u$ και M_w) του M και για κάθε ακέραιο i, θα υπάρχει μόνο μία στήλη που θα ικανοποιεί την εξής σχέση:

$$m_{uj} - m_{wj} \equiv i \ (mod\ n).$$

Έστω $C_1 = \{(a_{i0}, a_{i1}, \dots, a_{ik-1}) : 1 \le i \le l_1\}$ είναι ένας $(v_1, k, 1) - OOC$, ο οποίος έχει l_1 κωδικές λέξεις και $C_2 = \{(b_{i0}, b_{i1}, \dots, b_{ik-1}) : 1 \le i \le l_2\}$ είναι ένας $(v_2, k, 1) - OOC$, ο οποίος έχει l_2 κωδικές λέξεις.

Υποτίθεται ότι $M = DA(k, v_2)$ είναι πίνακας διαφορών διάστασης $k \times v_2$. Τότε, οι ακόλουθες οικογένειες υποσυνόλων k - στοιχείων σχηματίζουν έναν $(v_1v_2, k, 1) - OOC$, ο οποίος έχει $l_2 + v_2l_1$ κωδικές λέξεις.

Τύπος I : $\{v_1m_{0i} + a_{j0}, v_1m_{1i} + a_{j1}, \dots, v_1m_{(k-1)i} + a_{j(k-1)}\}, 1 \le i \le v_2, 1 \le j \le l_1$

Τύπος II : $\{v_1b_{i0}, v_1b_{i1}, \dots, v_1b_{i(k-1)}\}, 1 \le i \le l_2$

Για να αποδειχθεί η ορθότητα των προαναφερθέντων αναδρομικών κατασκευών, πρέπει να αποδειχτεί ότι δεν υπάρχουν επαναλαμβανόμενες διαφορές στις κωδικές λέξεις.

Λαμβάνοντας υπόψιν μια διαφορά $d\ mod\ (v_1v_2)$.

Αν $d \equiv 0\ mod\ (v_1)$, τότε, d μπορεί να παραχθεί από μία κωδική λέξη του Τύπου II. Αν $d' \equiv \frac{d}{v_1}$, τότε ο C_2 παράγει το πολύ μία d'. Έτσι, κάθε κωδική λέξη του Τύπου II παράγει στον C το πολύ μία d.

Αν $d \neq 0\ mod\ (v_1)$, τότε, υποθέτοντας ότι $d = v_1x + y,\ για\ 0 \le y < v_1$ η διαφορά $y\ (mod\ v_1)$ παράγεται το πολύ μία στον C_1. Άρα, $\alpha_{jw} - \alpha_{ju} \equiv y\ (mod\ v_1)$, $1 \le i \le l_1$, $0 \le w \neq u < k$, τότε η διαφορά $x\ (mod\ v_2)$ παράγεται από συγκεκριμένη στήλη i του πίνακα διαφορών M την $m_{wi} - m_{ui}$. Άρα, ο C παράγει το πολύ μία $d\ (mod\ v_1v_2)$.

Αν C_1 , C_2 είναι βέλτιστοι και υπάρχει πίνακας διαφορών $DA(k, v_2)$, τότε ο C θα είναι επίσης βέλτιστος. Οι C_1 , C_2 μπορούν να ανταλλαχτούν στις αναδρομικές κατασκευές. Επειδή η κατασκευή του πίνακα διαφορών διαδραματίζει σημαντικό ρόλο στις αναδρομικές κατασκευές των $OOCs$, στην συγκεκριμένη ενότητα θα παρουσιαστούν δύο μέθοδοι που παράγουν πίνακες διαφορών.

1η Κατασκευή (μέθοδος για πρώτους)

Όταν κάθε αριθμός από τους $1, 2, \dots, k-1$ είναι πρώτος με τον n, τότε ο πίνακας $M = m_{ij}$ διάστασης $k \times n$ είναι πίνακας διαφορών $M = DA(k, n)$, όπου $m_{ij} = ij(mod\ n)$ $0 \le i \le k-1, 0 \le j \le n-1$.

Όταν $k = 2, 3, 4, 6$ και C_2 είναι βέλτιστος OOC, τότε $v_2 = n_1 + l_2 k(k-1)$ είναι πρώτος με κάθε αριθμό από τους $1, 2, \dots, k-1$ και θα υπάρχει πίνακας διαφορών $M = DA(k, v_2)$. Αν C_1 είναι βέλτιστος, τότε ο C είναι επίσης βέλτιστος OOC.

1ο Παράδειγμα

Έστω $C_1 = C_2 = \{(0,1,3)\ mod\ 7\}$ και

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \end{bmatrix}$$

Τότε, βάση της αναδρομικής κατασκευής που αναφέρθηκε παραπάνω, μπορεί να κατασκευαστεί ένας νέος βέλτιστος OOC. Αυτός είναι ο εξής:

$$C = \{(0,1,3), (0,8,17), (015,31), (0,22,45), (0,29,10), (0,36,24), (0,43,38), (0,7,21)\ (mod\ 49)\}$$

και οι C_1 , C_2 και C είναι βέλτιστοι OOC.

▪

2ο Παράδειγμα

Χρησιμοποιώντας τους $(v_1, k, 1) = (7,3,1) : C_1 = \{(0,1,3)\ mod\ 7\}$ και $(v_2, k, 1) = (13,3,1) : C_2 = \{(0,1,4), (0,2,7)\ mod\ 13\}$ κατασκευάζεται ο πίνακας διαφορών

$$M = DA(k, v_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 2 & 4 & 6 & 8 & 10 & 12 & 1 & 3 & 5 & 7 & 9 & 11 \end{pmatrix} (mod\ 13)$$

Παράγεται ο $(91,3,1) - OOC$, ο οποίος είναι :

$$C = \{(0,1,3), (0,8,17), (0,15,31), (0,22,45), (0,29,59), (0,36,73), (0,43,87),$$

$$(0,50,10), (0,57,24), (0,64,38), (0,71,52), (0,78,66), (0,85,80), (0,7,28), (0,14,49)\ mod\ 91\}$$

Με πληθικότητα $|C| = 15$.

▪

2η Κατασκευή (μέθοδος ορθογώνιων σχηματισμών)

Οι πίνακες διαφορών μπορούν επίσης να επιτευχθούν χρησιμοποιώντας ορθογώνιους σχηματισμούς ή ορθογώνια λατινικά τετράγωνα.

Ορισμός

Λατινικό τετράγωνο ονομάζεται ο σχηματισμός που προκύπτει από την τοποθέτηση σε k - γραμμές και k - στήλες, τα k - πρώτα γράμματα του λατινικού αλφαβήτου με τέτοιο τρόπο ώστε, σε κάθε γραμμή και σε κάθε στήλη να εμφανίζονται όλα τα γράμματα από μία φορά. Δύο λατινικά τετράγωνα λέγονται (αμοιβαία) ορθογώνια (mutually orthogonal latin squares, MOLS), αν στις θέσεις όπου στο πρώτο τετράγωνο είναι ένα συγκεκριμένο γράμμα, στο δεύτερο βρίσκονται όλα τα γράμματα.

Ορισμός

Ένας ορθογώνιος σχηματισμός (orthogonal array) $OA(n, s)$ είναι ένας πίνακας, του οποίου τα στοιχεία λαμβάνουν τιμές από το $\mathbb{Z}_n = \{0,1, \dots, n-1\}$ και κάθε πιθανό ζεύγος (i, j) δεν επαναλαμβάνεται σε ανά δύο ευθείες. Όταν $s \geq 2$, κάθε πιθανό ζευγάρι θα εμφανίζεται μία φορά σε δύο επιλεγμένες γραμμές.

Εφόσον δίνονται, ένας ορθογώνιος σχηματισμός, $OA(k, k)$, $A = [a(i, j)]$ και ένας $(v, k, 1) - OOC$ με l κωδικές λέξεις, τότε η μέθοδος για να επιτευχθεί ο πίνακας διαφορών $B = DA(k, v)$ θα είναι η ακόλουθη :

Υποτίθεται ότι οι κωδικές λέξεις του C συμβολίζονται ως

$$\{C_{i0}, C_{i1}, \dots, C_{i(k-1)}\} \ (mod\ v)\ 1 \leq i \leq l.$$

Τότε, κάθε στήλη του πίνακα διαφορών B αντιπροσωπεύεται ως

$$< C_{sa(0,j)}, C_{sa(k-1,j)}, \dots, C_{sa(k-1,j)} >, 1 \leq s \leq l, 0 \leq j \leq k(k-1)$$

Επιπλέον, μία μη μηδενική στήλη μπορεί να προστεθεί στον B ώστε ο συνολικός αριθμός των στηλών του B να είναι $v = 1 + l(k-1)k$. Ο πίνακας B είναι πίνακας διαφορών $DA(k, v)$.

Αν $k = p^a$ είναι δύναμη πρώτου, τότε μπορούν να κατασκευαστούν ορθογώνιοι σχηματισμοί $OA(k, k+1)$ και $OA(k, k)$ μέσω των παράλληλων ευθειών της πεπερασμένης προβολικής γεωμετρίας. Οι ορθογώνιοι σχηματισμοί αντιστοιχούν σε ορθογώνια λατινικά τετράγωνα.

Παράδειγμα

Έστω $C_1 = C_2 = \{(0,1,3)\ mod\ 7\}$ και

$$A = \begin{bmatrix} 0 & 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 \end{bmatrix}$$

Από τον $C_1(c_{10} = 0, c_{11} = 1, c_{12} = 3)$ και τον A κατασκευάζεται ο

$$B = \begin{bmatrix} 0 & 1 & 3 & 0 & 1 & 3 & 0 \\ 3 & 0 & 1 & 1 & 3 & 0 & 0 \\ 1 & 3 & 0 & 3 & 0 & 1 & 0 \end{bmatrix}$$

Τότε, από τους C_1 , C_2 και B προκύπτει ο $(49, 3, 1) - OOC$, που είναι ο ακόλουθος:

$C = \{(0,10,22), (1,7,24), (3,8,21), (0,8,24), (3,7,22), (1,10,21), (0,1,3), (0,7,21)\ mod\ 49\}$

Η πληθικότητα του OOC είναι $|C| = 8$.

Μπορεί επίσης να δειχθεί ότι η αναδρομική κατασκευή είναι έγκυρη για $k = 2,3,4,5,6,7,8,9$ αν συνδυαστούν οι δύο μέθοδοι που προαναφέρθηκαν.

Για $k = 10, v = 91$ το σύνολο διαφορών $\{0,1,3,9,27,49,56,61,77,81\}$ $(mod 91)$ είναι ένας $(91, 10, 1) - OOC$.

Βιβλιογραφία

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

Άλλες Αναδρομικές κατασκευές για $OOCs$

I. Εισαγωγή

Η θεωρία κωδικοποίησης, η πεπερασμένη προβολική γεωμετρία, τα πεπερασμένα σώματα και η συνδυαστική θεωρία σχεδιασμού διαδραματίζουν σημαντικό ρόλο στις μελέτες των OOCs. Υπάρχουν άπειρες οικογένειες OOCs που έχουν κατασκευαστεί. Μεταξύ αυτών των οικογενειών, οι πιο ενδιαφέρουσες είναι οι βέλτιστοι OOCs και οι ασυμπτωτικά βέλτιστοι OOCs.

Ο ορισμός του ασυμπτωτικά βέλτιστου OOCs είναι η ακόλουθη.

Ορισμός 1.1

Έστω $\mathcal{F}$ μια άπειρη οικογένεια OOCs με $\lambda_\alpha = \lambda_c$. Κάθε $(n, w, \lambda) - OOC, C \in \mathcal{F}$ περιέχει μια τουλάχιστον κωδική λέξη, ο αριθμός των κωδικών λέξεων του C συμβολίζεται με $M_{(n,w,\lambda)}$, και το φράγμα του Johnson για τους $(n, w, \lambda) - OOCs$ συμβολίζεται με $J(n, w, \lambda)$. Η $\mathcal{F}$ λέγεται ασυμπτωτικά βέλτιστη με το φράγμα Johnson, εάν το ακόλουθο όριο υπάρχει και προσεγγίζει το 1:

$$\lim_{n\to\infty} \frac{M_{(n,w,\lambda)}}{J(n, w, \lambda)} = 1$$

Η κυκλική διαφορά ομαδοποίησης ή οι οικογένειες διαφορών είναι η κύρια μέθοδος που χρησιμοποιείται για την κατασκευή των $(n, w, 1) - OOCs$ και από αυτήν έχουν ληφθεί καρποφόρα αποτελέσματα. Σε αυτήν την ενότητα, θα δοθεί μια νέα αναδρομική κατασκευή (η Βασική Κατασκευή) η οποία μπορεί να εφαρμοστεί σε οποιουσδήποτε $(n, w, \lambda_\alpha, \lambda_c) - OOCs$, καθώς θα διατηρείται η ασυμπτωτική βέλτιστη ιδιότητα.

II. Αναδρομικές Κατασκευές

Στην παράγραφο αυτή, παρατίθενται μερικές αναδρομικές κατασκευές για τους οπτικούς ορθογώνιους κώδικες. Αρκετές αναδρομικές κατασκευές έχουν παρουσιαστεί για τους $(n, w, 1) - OOCs$, όμως πολύ λίγες είναι διαθέσιμες για OOCs με $\lambda > 1$.

Στο [1], παρουσιάζονται οι ακόλουθες κατασκευές.

Βασική Κατασκευή

Θεώρημα 2.1

1) Δίνεται ένας $(n, w, \lambda_\alpha, \lambda_c)$ κώδικας C, τότε ο C θα είναι επίσης ένας $(n, w, \lambda_\alpha', \lambda_c')$ κώδικας με $\lambda_\alpha' \geq \lambda_\alpha$ και $\lambda_c' \geq \lambda_c$.
2) Δίνεται ένας $(n, w, \lambda_\alpha, \lambda_c)$ κώδικας C με m κωδικές λέξεις, τότε θα υπάρχει ένας $(n, 2w - 2\lambda_c, 2\lambda_a + 2\lambda_c, w + 3\lambda_c)$ κώδικας C' με $\binom{m}{2}$ κωδικές λέξεις.

3) Δίνεται ένας $(n, w, \lambda_\alpha, \lambda_c)$ κώδικας C και t ένας θετικός ακέραιος, τότε θα υπάρχει ένας $(tn, tw, t\lambda_{\alpha,} t\lambda_c)$ C' κώδικας με τον ίδιο αριθμό κωδικών λέξεων.

Παρατήρηση 1

Όλες οι κατασκευές του Θεωρήματος 1 μεγεθύνουν τις τιμές λ_α, λ_c. Είναι πιθανό όταν δίνεται ένας $(n, w, \lambda_\alpha, \lambda_c)$ κώδικας C, οι αναδρομικές κατασκευές του να έχουν τις ακόλουθες ιδιότητες:

a) Οι κώδικες που προκύπτουν από τις αναδρομικές κατασκευές έχουν τις τιμές λ_α και λ_c όσο το δυνατόν μικρότερες. Ειδικότερα, οι αναδρομικές κατασκευές πρέπει να διατηρούν αυτές τις δύο τιμές αμετάβλητες.
b) Αν C είναι βέλτιστος, ο νέος κώδικας που προκύπτει από τις αναδρομικές κατασκευές πρέπει να είναι βέλτιστος, ή τουλάχιστον να πλησιάζει το βέλτιστο.

Στην ενότητα αυτή, κάνοντας χρήση των λεγόμενων $r-$απλών πινάκων, θα παρουσιαστούν διάφορες αναδρομικές κατασκευές που θα διατηρήσουν τις τιμές λ_α και λ_c αμετάβλητες, και θα δώσουν νέους κώδικες που θα πλησιάζουν την ιδανική περίπτωση ενός πρωτότυπου βέλτιστου κώδικα με $\lambda_\alpha = \lambda_c$.

Η έκφραση «ένας κώδικας C' πλησιάζει το βέλτιστο C» σημαίνει ότι ο κώδικας C' είναι ασυμπτωτικά βέλτιστός.

Ορισμός 2.2

Έστω G αβελιανή ομάδα μεγέθους n, και έστω r είναι ένας θετικός ακέραιος. Ένας $s \times t$ πίνακας $A = (a_{ij})$ της G ονομάζεται $r-$απλός, εάν η διαφορά που προκύπτει από δύο οποιεσδήποτε στήλες - διανύσματα του A, περιέχει κάθε στοιχείο της G περισσότερες από $r - 1$ φορές.

Στην εργασία αυτή, γίνεται χρήση μόνον των r - απλών πινάκων για μια κυκλική ομάδα G. Στις περισσότερες περιπτώσεις, ισχύει $G = \mathbb{Z}_g$.

Θεώρημα 2.2 (Βασική Κατασκευή)

Έστω C ένας $(n, w, \lambda_\alpha, \lambda_c) - OOC$. Εάν υπάρχει ένας $w \times N$, r – απλός πίνακας στο $\mathbb{Z}_g$, τότε θα υπάρχει ένας $(ng, w, \lambda_\alpha, \max\{\lambda_\alpha, \lambda_c, r-1\})$ – OOC, C′ με $|C'| = N|C|$, όπου $|C'|$ και $|C|$ δηλώνουν τον αριθμό των κωδικών λέξεων στους νέους και αρχικούς κώδικες αντίστοιχα.

Απόδειξη:

Έστω $C = \{C_i | 1 \leq i \leq |C|\}$ είναι η οικογένεια των κωδικών λέξεων με τις παραμέτρους $(n, w, \lambda_\alpha, \lambda_c)$, όταν $C_i = \{b_{i1}, b_{i2}, \dots, b_{iw}\}$ με $b_{ij} \in \mathbb{Z}_n$ $1 \leq i \leq |C|$, $1 \leq j \leq w$. Εδώ χρησιμοποιείται σύνολο - θεωρητική σημειογραφία.

Έστω $D = (d_{ij})$ $με$ $1 \leq i \leq w$ $και$ $1 \leq j \leq N$ είναι ένας r - απλός πίνακας στο $\mathbb{Z}_g$.

Έστω $C_i = \{b_{i1}, b_{i2}, \dots, b_{iw}\}$ είναι μια κωδική λέξη του C. Οι ακόλουθες N νέες κωδικές λέξεις σχεδιάζονται ως εξής:

$$F_{ij} = \{b_{ij} + nd_{jl} | 1 \leq j \leq w\} \text{ όπου } 1 \leq l \leq N$$

και η πρόσθεση λαμβάνεται στο $\mathbb{Z}_{ng}$.

Έστω $C' = \{F_{il} | 1 \leq i \leq |C|,\ 1 \leq l \leq N\}$.

Τότε, ο C' θα είναι ο επιθυμητός $(ng, w, \lambda_\alpha, max\{\lambda_\alpha, \lambda_c, r-1\}) - OOC$. Προς απόδειξη αυτού του ισχυρισμού, θα πρέπει να ελεγχθούν οι ιδιότητες αυτοσυσχέτισης και ετεροσυσχέτισης.

Για κάθε κωδική λέξη $C_i \in C$, κάθε ακέραιος $c \neq 0$ στο $\mathbb{Z}_n$ μπορεί να παρουσιαστεί ως η διαφορά $x - x'$, με $x, x' \in C_i$ το πολύ με λ_α τρόπους. Τώρα, για οποιαδήποτε κωδική λέξη F_{il} του C', οποιαδήποτε διαφορά $b_{ij1} + nd_{j1l} - b_{ij2} - nd_{j2l}$ μπορεί να εμφανιστεί περισσότερες από λ_α φορές, επειδή η διαφορά αυτή είναι σύμφωνη με την $b_{ij1} - b_{ij2}$ $modulo\ n$, που εμφανίζεται περισσότερες από λ_α φορές.

Για να ελεγχθεί η ιδιότητα της ετεροσυσχέτισης, χρειάζεται να επαληθευθούν οι δύο περιπτώσεις:

<u>1η Περίπτωση:</u> Πρώτα θα ελεγχθεί η ετεροσυσχέτιση μεταξύ $F_{i_1 l_1}$ και $F_{i_2 l_2}$ με $i_1 \neq i_2$. Αυτό σημαίνει ότι, αυτές οι δύο κωδικές λέξεις κατασκευάζονται βάσει διαφορετικών κωδικών λέξεων του C.

Υποθέτοντας ότι οι δύο κωδικές λέξεις είναι οι εξής:

$$F_{i_1 l_1} = \{b_{i_1 j} + nd_{j l_1} | 1 \leq j \leq w\}$$
$$F_{i_2 l_2} = \{b_{i_2 j} + nd_{j l_2} | 1 \leq j \leq w\}$$

Για κάθε διαφορά ισχύει:

$$(b_{i_1 j_1} + nd_{j_1 l_1}) - (b_{i_2 j_2} + nd_{j_2 l_2}) = b_{i_1 j_1} - b_{i_2 j_2}\ (mod\ n).$$

Συνεπώς, μπορεί να εμφανιστεί περισσότερες από λ_c φορές στο $\mathbb{Z}_{ng}$, δεδομένου ότι δεν μπορεί να εμφανιστεί περισσότερες από λ_c φορές στο $\mathbb{Z}_n$.

<u>2η Περίπτωση:</u> Η τιμή της ετεροσυσχέτισης μεταξύ των F_{il_1} και F_{il_2} ενδεχομένως να γίνει μεγαλύτερη από λ_c, όταν οι κωδικές λέξεις κατασκευάζονται βάσει μίας ίδιας κωδικής λέξης του C.

Υποθέτοντας ότι αυτές οι δύο κωδικές λέξεις είναι οι εξής:

$$F_{il_1} = \{b_{ij} + nd_{jl_1} | 1 \le j \le w\}$$
$$F_{il_2} = \{b_{ij} + nd_{jl_2} | 1 \le j \le w\}$$

Εξετάζεται κάθε διαφορά μεταξύ $(b_{ij_1} + nd_{j_1 l_1}) - (b_{ij_2} + nd_{j_2 l_2})$.

Αν $j_1 \neq j_2$, τότε το ίδιο το επιχείρημα δείχνει ότι μια τέτοια διαφορά δεν μπορεί να εμφανίζεται περισσότερες από λ_α φορές.

Αν $j_1 = j_2$, τότε η διαφορά

$$(b_{ij_1} + nd_{j_1 l_1}) - (b_{ij_2} + nd_{j_2 l_2}) = n(b_{i_1 l_1} - b_{i_2 l_2})$$

Με τη βοήθεια της υπόθεσης, ότι δηλαδή η διαφορά πίνακα D είναι $r -$ απλή, είναι γνωστό ότι η διαφορά αυτή δεν μπορεί να εμφανιστεί περισσότερες από $r - 1$ φορές. Συνδυάζοντας όλες τις περιπτώσεις, η τιμή της ετεροσυσχέτισης μεταξύ των F_{il_1} και F_{il_2} δεν είναι παρά η μέγιστη τιμή, δηλαδή $max\{\lambda_\alpha, \lambda_c, r - 1\}$.

Έτσι, έχει αποδειχτεί η Βασική Κατασκευή.

▪

Στην πραγματικότητα, η Βασική Κατασκευή μπορεί να γίνει λίγο καλύτερη με την προσθήκη περισσότερων κωδικών λέξεων στο νέο κώδικα, κάτω από ορισμένες συνθήκες.

Πόρισμα 2.1

Εκτός από τις προϋποθέσεις που ήδη ισχύουν στη Βασική Κατασκευή, αν επιπλέον υπάρχει ένας $(g, w, \lambda_\alpha, \lambda_c) - OOC$ με t κωδικές λέξεις, τότε θα υπάρχει και ένας $(ng, w, \lambda_\alpha, \max\{\lambda_\alpha, \lambda_c, \mathrm{r} - 1\}) - OOC$ με περισσότερες από t κωδικές λέξεις.

Απόδειξη:

Έστω $H = \{H_1, H_2, \dots, H_t\}$ είναι ένας $(g, w, \lambda_\alpha, \lambda_c) - OOC$.

Για οποιαδήποτε $H_i = \{h_{i1}, h_{i2}, \dots, h_{iw}\}$ κατασκευάζεται μία νέα κωδική λέξη, η

$$nH_i = \{nh_{i1}, nh_{i2}, \dots, nh_{iw}\} \ (mod\ ng).$$

Η προσθήκη των t νέων κωδικών λέξεων στον κώδικα C', δίνει έναν κώδικα με t περισσότερες κωδικές λέξεις.

Για να διαπιστωθεί ότι αυτός είναι ο επιθυμητός κώδικας, πρέπει να ελεγχθεί η ετεροσυσχέτιση μεταξύ των nH_i και πρέπει κάθε κωδική λέξη F_{jl} να έχει κατασκευαστεί σύμφωνα με τη Βασική Κατασκευή.

Έστω $nH_i = \{nh_1, nh_2, \dots, nh_w\}$ και $F_{jl} = \{b_1, b_2, \dots, b_w\}$. Υποθέτοντας ότι δύο διαφορές μεταξύ των nH_i και F_{jl} είναι ίσες, δηλαδή οι τιμές των $nh_{i1} - b_{j1} = nh_{i2} - b_{j2}$. Συνεπάγεται ότι $j_1 = j_2$ και $i_1 = i_2$. Έτσι, οποιαδήποτε διαφορά μεταξύ των nH_i και F_{jl} δεν μπορεί να εμφανιστεί περισσότερο από μία φορά.

▪

r – Απλοί Πίνακες

Για να χρησιμοποιηθεί η Βασική Κατασκευή, πρέπει να κατασκευαστούν κάποιοι r-απλοί πίνακες. Ακολουθεί μια κατασκευή που βασίζεται σε πεπερασμένα σώματα.

Λήμμα 2.1

Έστω p είναι πρώτος και $f(x)$ είναι ένα πολυώνυμο στο $GF(p)$[x]. Ορίζεται ένας $p \times p$ πίνακας $D = (d_{ij})$, με $d_{ij} = ij + f(i)$, $0 \le i,\ j \le p-1$.

Τότε, ο D είναι ένας 2 - απλός πίνακας στο $\mathbb{Z}_p$.

Απόδειξη:

Υποθέτοντας ότι $0 \le j_1 \ne j_2 \le p-1$. Πρέπει να αποδειχτεί ότι το πολύ – σύνολο $\{d_{ij1} - d_{ij2} | 0 \le i \le p-1\}$ περιέχει κάθε στοιχείο του $GF(p)$ όχι περισσότερο από μία φορά, δηλαδή, ακριβώς μια φορά. Σε αυτή την περίπτωση

$$d_{ij1} - d_{ij2} = ij_1 + f(i) - ij_2 - f(i) = (j_1 - j_2)i$$

Παρατηρείται ότι για $j_1 \ne j_2$ το σύνολο $\{(j_1 - j_2)i \,|0 \le i \le p-1\}$ περιέχει κάθε στοιχείο του $\mathbb{Z}_p$ ακριβώς μια φορά.

▪

Τώρα μπορεί να δοθεί μια κατασκευή ενός $p \times p^{r-1}$, r – απλού πίνακα στο $\mathbb{Z}_p$ για τυχόν πρώτο αριθμό p, με $r \ge 3$. Ξεκινά λοιπόν, η κατασκευή για $r = 3$, εφόσον για $r = 2$ η κατασκευή μπορεί να επιτευχθεί από το Λήμμα 2.1.

Θεώρημα 2.3

Έστω $3 \le r \le p$ είναι ένας ακέραιος, και p είναι ένας περιττός πρώτος.

Έστω

$$\mathcal{F} = \left\{ f(x) = \sum_{i=2}^{r-1} a_i x^i \,|\, a_i \in GF(p), 2 \le i \le r-1 \right\}$$

είναι μια οικογένεια p^{r-2} πολυώνυμων $GF(p)$. Ορίζεται $D_{f(x)} = ({d_{ij}}^{f(x)})$ με ${d_{ij}}^{f(x)} = ij + f(i)$, $(1 \le i, j \le p)$, για κάθε $f(x) \in \mathcal{F}$.

Τότε,

$$D = (D_{f(x)} | f(x) \in \mathcal{F})$$

είναι ένας r −απλός πίνακας στο $\mathbb{Z}_p$, όπου D είναι $p \times p^{r-1}$ πίνακας που αποτελείται από $D_{f(x)}$ με $f(x) \in \mathcal{F}$.

Απόδειξη:

Παρατηρείται ότι $|\mathcal{F}| = p^{r-2}$. Έτσι ο D είναι ένας $p \times p^{r-1}$ πίνακας. Για την απόδειξη του αποτελέσματος, θα πρέπει απλώς να δειχθεί ότι είναι r −απλός.

Με βάση τα παραπάνω λήμμα, $D_{f(x)}$ είναι 2-απλός, γι'αυτό το μόνο που χρειάζεται είναι έλεγχος σε κάθε ζεύγος στηλών των $D_{f(x)}$ και $D_{g(x)}$ με $f(x) - g(x) \neq 0$ στο $GF(p)[x]$. Για τη j_1 - οστη στήλη από το $D_{f(x)}$ και τη j_2 - οστη από το $D_{g(x)}$ θα εξεταστεί η διαφορά μεταξύ των i – στών στοιχείων τους

$$\begin{aligned} d^f_{ij1} - d^g_{ij2} &= ij_1 + f(i) - ij_2 - g(i) \\ &= i(j_1 - j_2) + f(i) - g(i) \end{aligned}$$

Σημειώνεται ότι $2 \leq deg(f(x) - g(x)) \leq r - 1$. Έτσι, για όλα τα $c \in GF(p)$, η εξίσωση

$$c = d^f_{ij1} - d^g_{ij2} = i(j_1 - j_2) + f(i) - g(i)$$

δεν έχει περισσότερες από $r - 1$ λύσεις.

▪

Συνδυάζοντας το Θεώρημα 2.3 και το Λήμμα 2.1, εξάγεται το ακόλουθο πόρισμα.

Πόρισμα 2.2

Για οποιονδήποτε πρώτο p και κάθε ακέραιο r με $2 \leq r \leq$ p, υπάρχει ένας $p \times p^{r-1}$, r −απλός πίνακας στο $\mathbb{Z}_p$.

Παράδειγμα 1

Έστω $p = 3$ και $r = 3$. Υπάρχει ένας 3-απλός πίνακας στο $\mathbb{Z}_3$ ως εξής:

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

▪

Για να υπάρξουν r −απλοί πίνακες σε άλλες διαστάσεις, χρειάζονται οι ακόλουθες κατασκευές γινομένου.

Θεώρημα 2.4 (Κατασκευή Γινόμενου)

Έστω $A = (a_{ij})$ ένας $m \times n$, r −απλός πίνακας στο $\mathbb{Z}_s$, και $B = (b_{ij})$ είναι ένας $m \times nk$, r −απλός πίνακας στο $\mathbb{Z}_t$.

Τότε θα υπάρχει ένας $m \times nk$, r −απλός πίνακας στο $\mathbb{Z}_{st}$.

Απόδειξη:

Για κάθε στήλη του A, έστω για την i –οστη στήλη $a_i = (a_{1i}, a_{2i}, \dots, a_{mi})^T$, κατασκευάζεται ο ακόλουθος $m \times k$ πίνακας :

$$H_i = \begin{pmatrix} a_{1i} + sb_{11} & a_{1i} + sb_{12} & \dots & a_{1i}+sb_{1k} \\ a_{2i}+sb_{21} & a_{2i}+sb_{22} & \dots & a_{2i}+sb_{2k} \\ & \dots & & \\ a_{mi}+sb_{m1} & a_{mi}+sb_{m2} & \dots & a_{mi}+sb_{mk} \end{pmatrix}$$

Έστω ο ισχυρισμός ότι

$$H = (H_1, H_2, \dots, H_t)$$

είναι ο επιθυμητός r −απλός πίνακας.

Για να αποδειχθεί ο ισχυρισμός, παρατηρούνται τα εξής δύο γεγονότα:

1) $\forall i, o\ H_i$ είναι ένας r-απλός πίνακας στο $\mathbb{Z}_{st}$, καθώς έχει παρατηρηθεί ότι η διαφορά μεταξύ δύο στηλών του H_i , είναι s φορές η διαφορά που αντιστοιχεί σε δύο στήλες του πίνακα B και η r-απλότητα του B εγγυάται την r-απλότητα του H_i.
2) έστω δύο στήλες H_i και H_j με $i \neq j$, αντίστοιχα. Το διάνυσμα διαφοράς των δύο αυτών στηλών $modulo\ s$ μετά από πράξεις είναι ίσο με τη διαφορά της i – οστης και της j – οστης στήλης. Τότε, η r-απλότητα του A εγγυάται ότι υπάρχουν το πολύ $r - 1$ επαναλαμβανόμενες τιμές στο διάνυσμα διαφοράς.

Με τον συνδυασμό αυτών των δύο γεγονότων, έχει αποδειχτεί το ζητούμενο.

▪

Οι r-απλοί πίνακες μπορεί να θεωρηθούν ως γενίκευση ενός άλλου καλά μελετημένου είδους των συνδυαστικών πινάκων, τους λεγόμενους πίνακες διαφορών. Έχει διαπιστωθεί ότι οι r-απλοί πίνακες έχουν άλλες εφαρμογές σε ακολουθίες σχεδιασμών για επικοινωνίες. Μια πιο λεπτομερή επεξεργασία για βασικές ιδιότητες, για όρια, για σχέσεις μεταξύ των πινάκων διαφορών και των ορθογώνιων πινάκων, για κατασκευές και για εφαρμογές γίνεται στο [2].

Ασυμπτωτικά Βέλτιστες Αναδρομικές Κατασκευές

Σε αυτό το σημείο θα παρουσιαστεί μία αναδρομική κατασκευή η οποία βασίζεται στη Βασική Κατασκευή και την Κατασκευή Γινομένου για r-απλούς πίνακες και για όλους τους OOCs με $\lambda_\alpha = \lambda_c = \lambda$.

Θεώρημα 2.5 (Κατασκευή Α)

Υποθέτοντας ότι υπάρχει ένας $(n, w, \lambda) - OOC$ με T κωδικές λέξεις. Έστω p είναι πρώτος, όχι μικρότερος από w.

Τότε, θα υπάρχει ένας $(np, w, \lambda) - OOC$ με Tp^{λ} κωδικές λέξεις.

Απόδειξη:

Σύμφωνα με το Θεώρημα 2.3 και τα συμπεράσματα αυτού, υπάρχει ένας $p \times p^{\lambda}(\lambda + 1)$ - απλός πίνακας D στο $\mathbb{Z}_p$. Λαμβάνοντας υπόψιν τις πρώτες w σειρές του D, θα υπάρχει ένας $w \times p^{\lambda}$ $(\lambda + 1)$ – απλός πίνακας στο $\mathbb{Z}_p$. Έτσι, το ζητούμενο συμπέρασμα προκύπτει από την Βασική Κατασκευή.

Πόρισμα 2.3

Υποθέτοντας ότι υπάρχει ένας $(n, w, \lambda) - OOC$ με T κωδικές λέξεις. Έστω $m = {p_1}^{r_1}{p_2}^{r_2} \dots {p_t}^{r_t}$ ένας θετικός ακέραιος, όπου p_i με $1 \le i \le t$ είναι πρώτος όχι μικρότερος από w. Τότε, θα υπάρχει ένας $(mn, w, \lambda) - OOC$ με Tm^{λ} κωδικές λέξεις.

Απόδειξη:

Η εφαρμογή της Κατασκευής Α σε $(n, w, \lambda) - OOC$ αρκετές φορές δίνει $(\lambda + 1)$ - απλούς πίνακες. Το ίδιο αποτέλεσμα επιτυγχάνεται, αν αρχικά κατασκευαστεί ένας $w \times m^{\lambda}$ $(\lambda + 1)$ - απλός πίνακας στο $\mathbb{Z}_m$ μέσω της Κατασκευής Γινομένων r-απλών πινάκων, και στη συνέχεια εφαρμοστεί η Βασική Κατασκευή για να προκύψει ο επιθυμητός OOC.

Παράδειγμα 2

Ο ακόλουθος κώδικας αποτελεί ένα $(63, 9, 2)$ βέλτιστο OOC.

{1	5	8	18	28	31	35	40	59}
{2	7	10	16	17	36	55	56	62}
{3	11	24	25	27	29	30	43	51}
{4	9	14	20	32	34	47	49	61}
{6	22	23	39	48	50	54	58	60}
{12	15	33	37	44	45	46	53	57}

Σύμφωνα με την Κατασκευή Α, μπορεί να κατασκευαστεί ένας $(63 \times 11, 9, 2) - OOC$ με $6 \times 121 = 726$ κωδικές λέξεις, από έναν 9×121 3-απλό πίνακα στο $\mathbb{Z}_{11}$. Το φράγμα Johnson για το $\Phi(63 \times 11, 9, 2)$ είναι 948.

▪

Αυτή η αναδρομική κατασκευή πληροί την πρώτη προϋπόθεση της παρατήρησης 1. Δυστυχώς όμως, σε γενικές γραμμές δεν δίνεται κανένας νέος βέλτιστος OOCs, ακόμη και αν ο αρχικός κώδικας είναι βέλτιστος. Είναι δυνατόν να προκύψουν βέλτιστοι OOCs υπό ορισμένες συνθήκες για $\lambda = 1$. Εντούτοις, διασφαλίζεται η διατήρηση της ασυμπτωτικής βέλτιστης ιδιότητας.

Θεώρημα 2.6

Έστω $\mathcal{F}$ μια άπειρη οικογένεια ασυμπτωτικά βέλτιστων OOCs για την οποία ισχύει το φράγμα Johnson. Τότε θα υπάρχει μία άπειρη $\mathcal{F}^*$ οικογένεια ασυμπτωτικά βέλτιστων OOCs με την ιδιότητα ότι για κάθε $(n, w, \lambda) - OOC, C \in \mathcal{F}$ με T κωδικές λέξεις, και για κάθε θετικό ακέραιο πρώτο m, ο οποίος δεν είναι μικρότερος από w, θα υπάρχει ένας $(n, w, \lambda) - OOC$, $C^* \in \mathcal{F}^*$ με Tm^λ κωδικές λέξεις.

Απόδειξη:

Η ύπαρξη της οικογένειας $\mathcal{F}^*$ προκύπτει από το Πόρισμα 2.3. Αρκεί να δειχτεί ότι η $\mathcal{F}$ είναι ασυμπτωτικά βέλτιστη σε σχέση με το φράγμα Johnson. Παρατηρείται ότι

$$\lim_{n\to\infty} \frac{Tm^\lambda}{J(mn, w, \lambda)} = \lim_{n\to\infty} \frac{m^\lambda T\, J(n, w, \lambda)}{J(mn, w, \lambda)\, J(n, w, \lambda)} = \lim_{n\to\infty} \frac{m^\lambda\, J(n, w, \lambda)}{J(mn, w, \lambda)} \lim_{n\to\infty} \frac{T}{J(n, w, \lambda)} = 1$$

Έτσι, το συμπέρασμα προκύπτει από τον ορισμό των ασυμπτωτικά βέλτιστων $OOCs$.

III. Οικογένειες Ασυμπτωτικά Βέλτιστων $OOCs$

Στην παράγραφο αυτή, θα εφαρμοστεί η Κατασκευή Α σε ορισμένες γνωστές οικογένειες ασυμπτωτικά βέλτιστων OOCs. Η πρώτη κατηγορία πραγματεύεται την περίπτωση με $\lambda = 1$, η δεύτερη κατηγορία είναι αφιερωμένη στην περίπτωση με $\lambda > 1$ και η τελευταία κατηγορία περιέχει κάποιες περαιτέρω συζητήσεις σχετικά με τη Βασική Κατασκευή και την Κατασκευή Α.

a) $OOCs$ με $\lambda = 1$

Οι $(n, w, 1) - OOCs$ έχουν πλέον μελετηθεί εκτενώς τις τελευταίες δεκαετίες. Πολλές άπειρες οικογένειες βέλτιστων $OOCs$ έχουν κατασκευαστεί, ιδίως για μικρές τιμές w.

Θεώρημα 3.7

Για κάθε δύναμη πρώτου q , υπάρχει ένας βέλτιστος $\left(q^2 + q + 1,\ q + 1, 1\right) - OOC$.

Παρατήρηση 2

Για την ακρίβεια, για κάθε δύναμη πρώτου q , ένας $\left(q^2 + q + 1,\ q + 1, 1\right) - OOC$ είναι ένας $\left(q^2 + q + 1,\ q + 1, 1, 0\right) - OOC$, καθώς έχει μόνο μία κωδική λέξη.

Η εφαρμογή της Κατασκευής Α οδηγεί στο ακόλουθο θεώρημα.

Θεώρημα 3.8

Για κάθε δύναμη πρώτου q, υπάρχει ένας $\left((m(q^2+q+1),\ q\ +\ 1,1\right)-OOC$, όπου m είναι θετικός ακέραιος, του οποίου οι πρώτοι διαιρέτες είναι μεγαλύτεροι από τον q. Αυτή η οικογένεια είναι ασυμπτωτικά βέλτιστη καθώς $q \to \infty$.

Στην πραγματικότητα, για κάποιες ειδικές τιμές του m, μπορεί να επιτευχθούν βέλτιστοι OOCs.

Πόρισμα 3.4

$$\Phi\left((m(q^2+q+1),\ q\ +\ 1,1\right) = m\ ,\ \alpha\nu\ \ q < m < q^2+q\ +1$$

όπου m είναι θετικός ακέραιος, με πρώτους διαιρέτες μεγαλύτερούς από q.

Επιπλέον, εάν εφαρμοστεί το αποτέλεσμα της Βασικής Κατασκευής (Πόρισμα 2.1), μπορεί να προκύψει μία άλλη βέλτιστη οικογένεια $OOCs$ υπό ορισμένες συνθήκες.

Πόρισμα 3.5

Έστω q οποιαδήποτε δύναμη πρώτου. Αν όλοι οι πρώτοι διαιρέτες του q^2+q+1 είναι μεγαλύτεροι από q, τότε θα υπάρχει ένας βέλτιστος $\left((q^2+q+1)^t,\ q+1,1\right)-OOC$ για κάθε θετικό ακέραιο t.

Απόδειξη:

Θα αποδειχθεί με επαγωγή.

Ισχύει για $t=1$.

Έστω ότι υπάρχει ένας βέλτιστος $\left((q^2+q+1)^t,\ q+1,1\right)-OOC$, C.

Μετρώντας τις κωδικές λέξεις του C, ισχύουν τα εξής:

$$|C| = \frac{(q^2+q+1)^t-1}{q(q+1)} = \sum_{i=0}^{t-1}(q^2+q+1)^i$$

Σύμφωνα με την παραγοντοποίηση του q^2+q+1, μπορεί να εφαρμοστεί η Κατασκευή Α στον C αρκετές φορές, με κατάλληλους 2-απλούς πίνακες, και να προκύψει ένας νέος OOC, C'. Εφόσον, υπάρχει ένας βέλτιστος $\left(q^2+q+1,\ q+1,1\right)-OOC$, μπορεί να γίνει περαιτέρω χρήση του Πορίσματος 2.1 και να προστεθεί ακόμη μία κωδική λέξη στον C'. Συνεπώς,

$$|C'| = |C|(q^2+q+1)+1 = \frac{(q^2+q+1)^{t+1}-1}{q(q+1)}$$

Είναι εύκολο να αποδειχτεί ότι $|C'|$ είναι ίσο με το φράγμα Johnson για τους $((q^2+q+1)^{t+1}, q\ +1,1)-OOCs$, οπότε ο C' είναι ένας βέλτιστος OOC.

b) $OOCs$ με $\lambda > 1$

Για την κατηγορία αυτή, θα ξαναειπωθούν κάποιες γνωστές οικογένειες ασυμπτωτικά βέλτιστων $(n, w, \lambda) - OOC$ με $\lambda > 1$, και θα επεκταθούν με την Κατασκευή Α.

Θεώρημα 3.9

Έστω p πρώτος αριθμός, και m ακέραιος ≥ 1.

Τότε θα υπάρχει ένας βέλτιστος $\left(p^{2m} - 1,\ p^m + 1, 2\right) - OOC$ με $(p^m - 2)$ κωδικές λέξεις.

Πόρισμα 3.6

Έστω p πρώτος αριθμός, και m ακέραιος ≥ 1, και t οποιοσδήποτε ακέραιος. Οι πρώτοι διαιρέτες των p, m, t υπερβαίνουν p^m. Τότε, θα υπάρχει ένας $\left(t(p^{2m} - 1),\ p^m + 1, 2\right) - OOC$ με $t^2(p^m - 2)$ κωδικές λέξεις. Αυτή η οικογένεια είναι ασυμπτωτικά βέλτιστη καθώς $p \to \infty$.

Θεώρημα 3.10

1. Έστω p οποιοσδήποτε πρώτος αριθμός, m κάθε διαιρέτης του $p - 1$, και t οποιοδήποτε ακέραιος, $1 \leq T \leq M$. Τότε θα υπάρχει ένας $(pm, m, t) - OOC$ με
$$\frac{1}{pm}\left(\sum_{d|(p-1)} \mu(d)\left(p^{\lceil (t+1)/d \rceil} - 1\right)\right)$$
κωδικές λέξεις. Αυτή η οικογένεια είναι ασυμπτωτικά βέλτιστη καθώς $m \to \infty$.

2. Έστω p οποιοσδήποτε πρώτος αριθμός και α, t να είναι φυσικοί αριθμοί, $a \geq 2,\ 1 \leq t < p - t$. Τότε θα υπάρχει ένας $(p(p^\alpha - 1), p - t, t) - OOC$ με $p^{\alpha-1}(p^{t\alpha-1} - 1)/\ (p^\alpha - 1)$ κωδικές λέξεις. Αυτή η οικογένεια είναι ασυμπτωτικά βέλτιστη καθώς $p \to \infty$ και t είναι σταθερό.

3. Έστω $q = p^s$ όπου $s \geq 1$ και p είναι κάθε πρώτος αριθμός. Έστω m και $q + 1$ είναι σχετικά πρώτοι, και t είναι ακέραιος αριθμός με $1 \leq t \leq \frac{m}{2}$. Τότε, θα υπάρχει ένας $\left((q + 1)m,\ m, 2t\right) - OOC$ με $\frac{M}{m(q+1)}$ κωδικές λέξεις, όπου M ορίζεται ως εξής:
$$M = \begin{cases} q^{2t+1} - q & , \quad t = 1,2,3,4,5,6 \\ \geq q^{2t+1} - \frac{1}{7}q^{2t+6} & , \quad t \geq 7 \end{cases}$$
Επιπλέον, αυτή η οικογένεια είναι ασυμπτωτικά βέλτιστη καθώς $m \to \infty$ και t είναι σταθερό.

Με βάση την Κατασκευή Α, μπορούν να κατασκευαστούν τρεις νέες οικογένειες ασυμπτωτικά βέλτιστων OOCs. Οι τρεις νέες οικογένειες είναι πολύ μεγαλύτερες από τις αρχικές και είναι ασυμπτωτικά βέλτιστες σύμφωνα με το φράγμα Johnson.

Η πρώτη άπειρη οικογένεια βέλτιστων OOCs με $\lambda > 2$ προήλθε από κατασκευή που παρουσιάστηκε στο [3].

c. Γενικά

Με τη Βασική Κατασκευή και την Κατασκευή Α, δεν είναι πλέον δύσκολο να προκύψουν κάποιες οικογένειες OOCs. Το ακόλουθο θεώρημα είναι ένα παράδειγμα.

Θεώρημα 3.11

Έστω q οποιοσδήποτε πρώτος αριθμός, n κάθε θετικός ακέραιος και m κάθε θετικός ακέραιος, οι πρώτοι διαιρέτες των οποίων δεν είναι μικρότεροι από το $\frac{q^n-1}{q-1}$.

Τότε, υπάρχει ένας

$$\left(m\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right) - OOC$$

με $m^{(q^{n-1}-1)/(q-1)}$ κωδικές λέξεις.

Απόδειξη:

Για κάθε πρώτο αριθμό q, υπάρχει ένας

$$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right) - OOC$$

με μία κωδική λέξη.

Το συμπέρασμα προκύπτει έπειτα, από την Κατασκευή Α.

▪

Αν εφαρμοστεί η Βασική Κατασκευή, άμεσα, μπορούν να προκύψουν μερικές οικογένειες OOCs με $\lambda_\alpha \neq \lambda_c$.

Παράδειγμα 3

Έστω q πρώτος αριθμός, και m είναι οποιοσδήποτε θετικός ακέραιος των οποίων οι πρώτοι διαιρέτες είναι μεγαλύτεροι από q.

Τότε, θα υπάρχει ένας $\left((m(q^2+q+1),\ q\ +\ 1, 2\right) - OOC$ με m^2 κωδικές λέξεις.

Απόδειξη:

Για κάθε πρώτο αριθμό q, υπάρχει ένας $\left(q^2+q\ +1,\ q+1, 1\right)\ -\ OOC$ με μια κωδική λέξη. Σύμφωνα με την παραγοντοποίηση m, εφαρμόζονται αντίστοιχα 3-απλοί πίνακες. Με τη Βασική Κατασκευή, επιτυγχάνεται ο επιθυμητός κώδικας.

Τα παραπάνω παραδείγματα δείχνουν ότι είναι εύκολο να προκύψουν κάποιες οικογένειες OOCs. Ωστόσο, σε κανένα από τα παραπάνω παραδείγματα, οι οπτικοί ορθογώνιοι κώδικες δεν είναι βέλτιστοι ή ασυμπτωτικά βέλτιστοι.

IV. Συμπέρασμα

Σε αυτή την ενότητα, παρουσιάστηκε μία νέα αναδρομική κατασκευή (η Βασική Κατασκευή) για OOCs. Από τη Βασική Κατασκευή, επιτυγχάνεται η Κατασκευή Α για $(n, w, \lambda) - OOCs$. Με την Κατασκευή Α, διευρύνονται ορισμένες γνωστές οικογένειες ασυμπτωτικά βέλτιστων $OOCs$, και ως αποτέλεσμα προκύπτουν νέες οικογένειες, που είναι πολύ μεγαλύτερες από τις αρχικές και εξακολουθούν να είναι και αυτές ασυμπτωτικά βέλτιστες.

Μια σημαντική ερώτηση σχετικά με τη Βασική Κατασκευή είναι πόσο μακριά είναι από το να προκύψουν νέοι βέλτιστοι OOCs από τις αρχικές οικογένειες. Στην πραγματικότητα, είναι δυνατό να προκύψουν κάποιες βέλτιστες οικογένειες, εφόσον, τροποποιηθεί η Βασική Κατασκευή υπό ορισμένες συνθήκες.

Βιβλιογραφία

[1] F. R. K. Chung, J. A. Salehi, and V. K. Wei, “Optical orthogonal codes: Design, analysis and applications,” IEEE Trans. Inform. Theory, vol. 35, pp. 595–604, May 1989.

[2] W. Chu, “Optical Orthogonal Codes and Cyclic t-designs,” Ph.D. dissertation, Univ. So. Calif., Los Angeles, 2002.

[3] H. Chung and P. V. Kumar, “Optical orthogonal codes–New bounds and an optimal construction,” IEEE Trans. Inform. Theory, vol. 36, pp. 866–873, July 1990.

Αναδρομικές κατασκευές για βέλτιστους $(n, 4, 2) - OOCs$

I. Εισαγωγή

Ένα δύσκολο πρόβλημα των OOCs είναι να επιτευχθούν βέλτιστοι OOCs, και ιδιαίτερα με $\lambda > 1$. Πρόσφατα αναπτύχθηκε ένας αλγοριθμικός σχεδιασμός βασισμένος στο μέγιστο πρόβλημα πλήρους γραφήματος - maximal clique problem (MCP) για να βρεθούν βέλτιστοι$(n, 4, 2) - OOCs$ τάξης μέχρι $n = 44$. Το επίκεντρο αυτής της ενότητας είναι οι αναδρομικές κατασκευές για βέλτιστους $(n, 4, 2) - OOCs$. Οι περισσότερες κωδικές λέξεις μπορούν να κατασκευαστούν από γενικές αναδρομικές τεχνικές, παρόλα αυτά, παραμένει το χάσμα που υπάρχει μεταξύ των αναδρομικών κατασκευών και των βέλτιστων OOCs. Σε μερικές περιπτώσεις, αυτό το χάσμα μπορεί να κλείσει, όταν δίνονται αναδρομικές κατασκευές για βέλτιστους $(n, 4, 2) - OOCs$.

Η αναγωγή από βέλτιστους $(n, 4, 2) - OOCs$ σε απλούς, μέσω μιας σειράς αναδρομικών κατασκευών, δηλώνεται ως πεπερασμένο μέγιστο πρόβλημα πλήρους γραφήματος (maximal clique problem).

Με την επίλυση αυτών των πεπερασμένων MCP προβλημάτων, μπορεί να επεκταθεί η γενική αναδρομική κατασκευή των OOCs και να επιτευχθούν νέες αναδρομικές κατασκευές που δίνουν βέλτιστους $(n \cdot 2^x,\ 4,\ 2) - OOCs$ για $x \geq 3$, εάν υπάρχει το $CSQS(n)$.

Υπάρχει μια στενή σχέση μεταξύ OOCs και (μερικών) κυκλικών t - σχεδιασμών. Γι' αυτό παρατίθενται οι ορισμοί των t - σχεδιασμών, των κυκλικών t - σχεδιασμών και των μερικών κυκλικών t - σχεδιασμών.

Ορισμός 1.1

Ένας (μερικός) $t - (v, k, \lambda)$ σχεδιασμός είναι ένα ζευγάρι (X, B) όπου X είναι ένα v – σύνολο (ή σημειοσύνολο), και B είναι μια οικογένεια k - υποσυνόλων του X (οικογένεια από blocks), έτσι ώστε κάθε t - υποσύνολο του X να εμφανίζεται ακριβώς (το πολύ) λ blocks.

Ορισμός 1.2

Ένας (μερικός) $t - (v, k, \lambda)$ σχεδιασμός είναι κυκλικός αν η ομάδα αυτομορφισμού περιέχει έναν κύκλο μήκους v. Επιπλέον, στο πλαίσιο δράσης του αυτομορφισμού, κάθε κυκλική τροχιά μήκους v είναι ένας αυστηρά κυκλικός (μερικός) σχεδιασμός. Ένας (αυστηρά) κυκλικός $t - (v, k, \lambda)$ μερικός σχεδιασμός καλείται επίσης (αυστηρά) κυκλική $t - (v, k, \lambda)$ ομαδοποίηση.

Μία $t - (v, k, \lambda)$ κυκλική ομαδοποίηση είναι βέλτιστη, εφόσον, περιέχει το μέγιστο δυνατό αριθμό blocks.

Η σχέση μεταξύ OOCs και κυκλικών t - σχεδιασμών συνοψίζεται στο Θεώρημα 1.1.

Θεώρημα 1.1

Κάθε $(v, w, \lambda) - OOC$ είναι ισοδύναμος με μία αυστηρά κυκλική $(\lambda + 1) - (v, w, 1)$ ομαδοποίηση, όπου $\lambda \geq 1$. Όμως, κάθε αυστηρά κυκλική $t - (v, k, 1)$ ομαδοποίηση ισοδυναμεί με έναν $(v, k, t - 1)$ – OOC, όπου $t \geq 2$. Εξάλλου, αν η ομαδοποίηση είναι βέλτιστη, τότε το αποτέλεσμα ενός OOC είναι επίσης βέλτιστο.

II. $(v, 4, 2) - OOCs$ και κυκλικά τετραπλά συστήματα Steiner

Σε αυτήν την παράγραφο, εξετάζονται κυρίως οι $(v, 4, 2) - OOCs$, οι οποίοι ισοδυναμούν με αυστηρά κυκλικές $3 - (v, 4, 1)$ ομαδοποιήσεις.

Ορισμός 2.1

Ένας $3 - (v, 4, 1)$ σχεδιασμός είναι ένα τετραπλό σύστημα Steiner (quadruple system Steiner), συμβολίζεται συχνά ως $SQS(v)$. Ένα αυστηρά κυκλικό $SQS(v)$ συμβολίζεται ως $sSQS(v)$, και ένα κυκλικό $SQS(v)$ συμβολίζεται ως $CSQS(v)$.

Ορισμός 2.2

Μια τετραπλή διαφορά – difference quadruple (DQ) είναι μία τετράδα (a, b, c, d) πάνω στο $\mathbb{Z}_v$ με $a + b + c + d \equiv 0 \ (mod\ v)$. Μια τριπλή διαφορά – difference triple (DT) είναι μια τριάδα (a, b, c) πάνω στο $\mathbb{Z}_v$ τέτοια ώστε $a + b + c \equiv 0 \ (mod\ v)$.

Κάθε DQ (a, b, c, d) περιλαμβάνει τέσσερις DTs, δηλαδή $(a, b, c + d)$, $(b, c, d + \alpha)$, $(c, d, a + b)$, $(d, a, b + c)$. Από οποιαδήποτε DQ (a, b, c, d), μπορεί να κατασκευαστεί ένα αρχικό block $S = \{0, a, a + b, a + b + c\}$.

Ορισμός 2.3

Έστω $A_i = (a_i, b_i, c_i, d_i)$, $i = 1, 2$ είναι δύο DQs στο $\mathbb{Z}_v$. Το A_1 είναι ισοδύναμο με το A_2 , συμβολίζεται $A_1 \sim A_2$, αν $B_i = \{0, a_i , a_i + b_i , a_i + b_i + c_i\}$, $i = 1, 2$ είναι στην ίδια τροχιά του $\mathbb{Z}_v$, δηλαδή, $B_1 \in {B_2}^{\mathbb{Z}_v}$.

Με παρόμοιο τρόπο έχει οριστεί η ισοδυναμία μεταξύ δύο DTs.

Μια DQ δεν χρειάζεται να περιέχει τέσσερις ανισότιμες DTs. Οι εξαιρέσεις μπορεί να χαρακτηριστούν ως εξής:

Μια DQ του τύπου $(i, \frac{v}{2} - i, i, \frac{v}{2} - i)$ δημιουργεί δύο ανισότιμες DTs αν $i \neq \frac{v}{4}$.

Μια DQ του τύπου $(\frac{v}{4}, \frac{v}{4}, \frac{v}{4}, \frac{v}{4})$ δημιουργεί μια μοναδική DT.

Στην πρώτη περίπτωση η DQ είναι το μισό της τετράδας και στην τελευταία είναι το ένα τέταρτο της τετράδας. Αυτές οι διαφορές δίνουν αντίστοιχα τις μισές και το εν τέταρτο των τροχιών όταν $\mathbb{Z}_v$ ενεργεί αντίστοιχα στα αρχικά blocks τους.

Ορισμός 2.4

Οποιαδήποτε DQ που περιείχε τέσσερις ανισότιμες DTs ονομάζεται πλήρης DQ.

Η ύπαρξη ενός $CSQS(n)$ είναι ισοδύναμη με την ύπαρξη ενός συνόλου DQs για το οποίο κάθε DT μέσω του $\mathbb{Z}_n$ περιέχεται σε ακριβώς μία από τις DQs.

Χρησιμοποιώντας αυτούς τους ορισμούς για την ισοδυναμία μεταξύ DQs και DTs, κάθε DT $(\text{ή } DQ)$ έχει διαφορετικές ισοδύναμες παραστάσεις πέρα από τις κυκλικές μετατοπίσεις της.

Οι DTs, ακολουθούν έξι διαφορετικές μορφές.

Λήμμα 2.1

Έστω (a, b, c) είναι DT στο $\mathbb{Z}_v$.
Τότε $(a, b, c) \sim (b, c, a) \sim (c, a, b) \sim (-b, -a, -c) \sim (-a, -c, -b) \sim (-c, -b, -a)$.

Απόδειξη:

Έστω ένα αντιπροσωπευτικό block της τροχιάς (a, b, c) , δηλαδή $\{0, a, a + b\}$. Παρότι τα σύνολα δεν έχουν διάταξη, υπάρχουν έξι τρόποι για να διαταχτούν. Αυτοί αντιστοιχούν στις έξι μορφές DTs.

Για οποιαδήποτε DT, υπάρχουν μόνο δύο ανεξάρτητες παράμετροι, έτσι ώστε η DT (a, b, c) να συμβολίζεται ως $[\alpha]_b$. Τότε, ξαναγράφοντας το Λήμμα 2.1 προκύπτει το ακόλουθο λήμμα.

Λήμμα 2.2

$$[\alpha]_b \sim [b]_{(-\alpha-b)} \sim [-\alpha - b]_\alpha \sim [-b]_{(-a)} \sim [-\alpha]_{(a+b)} \sim [\alpha + b]_{(-b)}$$

Μια πολύ χρήσιμη γενίκευση των CSQSs ορίζεται, ως εξής:

Ορισμός 2.4

Έστω $v \equiv 0\ (mod\ m)$. Ένας m - αποκομμένος $CSQS(v)$, συμβολίζεται $CSQS(v, -m)$, είναι μια συλλογή από DQs, με την ιδιότητα ότι κάθε DT των οποίων η είσοδος έχει κοινό παράγοντα $\frac{v}{m}$, δεν εμφανίζεται στο σύστημα, αλλά όλες οι υπόλοιπες DTs εμφανίζονται ακριβώς μία φορά.

Η σημασία της έννοιας αυτής στηρίζεται στο εξής απλό λήμμα.

Λήμμα 2.3

Αν υπάρχουν $CSQS(v, -m)$ και $CSQS(m)$, τότε θα υπάρχει και $CSQS(v)$.

III. Βασική Κατασκευή και $H - σχεδιασμοί$

Προτείνεται μία αναδρομική κατασκευή για τους γενικευμένους OOCs. Αυτή η κατασκευή εγγυάται ασυμπτωτική βελτιστότητα εάν η αρχική οικογένεια είναι ασυμπτωτικά βέλτιστη. Η αναδρομική κατασκευή ονομάζεται Βασική Κατασκευή.

Ορισμός 3.1

Έστω G μία αβελιανή ομάδα μεγέθους n, και r είναι ένας θετικός ακέραιος. Ένας $s \times t$ πίνακας $A = (\alpha_{ij})$ πάνω στη G είναι r - απλός, αν η διαφορά δύο οποιωνδήποτε διανυσμάτων της στήλης A περιέχει κάθε στοιχείο της G περισσότερες από $r - 1$ φορές.

Θεώρημα 3.1 (Βασική Κατασκευή)

Έστω C ένας $(n, w, \lambda) - OOC$. Εάν υπάρχει ένας $w \times N$ $(\lambda + 1)$ – απλός πίνακας στο $\mathbb{Z}_g$, τότε θα υπάρχει ένας $(ng, w, \lambda) - OOC$ C′ με $|C'| = N|C|$, όπου $|C'|$ και $|C|$, δηλώνουν τον αριθμό των κωδικών λέξεων στους νέους και αρχικούς κώδικες, αντίστοιχα.

Για να επιτευχθούν βέλτιστοι $(n, 4, 2) - OOCs$, η Βασική Κατασκευή εφαρμόζεται αρχικά σε $CSQSs$ για να εφοδιαστεί η πλειοψηφία των κωδικών λέξεων που χρειάζονται οι βέλτιστοι OOCs.

Η έρευνα για το υπόλοιπο μέρος περιορίζεται στο πρόβλημα MCP. Αν επιτευχθεί μια βέλτιστη λύση για το MCP, τότε μπορεί να κατασκευαστεί μια βέλτιστη οικογένεια OOCs.

Για να κατανοηθεί η δομή των αποτελεσμάτων των σχεδιασμών που προέρχονται από την Βασική Κατασκευή των $CSQSs$, έχουν εισαχθεί οι $H-\sigma\chi\varepsilon\delta\iota\alpha\sigma\mu o\acute{\iota}$.

Ορισμός 3.2

Ένας $H-\sigma\chi\varepsilon\delta\iota\alpha\sigma\mu\acute{o}\varsigma$, $H(m,r,k,t)$, είναι μία ταξινομημένη τριάδα $(X,\mathcal{G},\mathcal{T})$, όπου X είναι ένα σύνολο με $v=mr$ σημεία, $\mathcal{G}$ είναι μια συλλογή από m - ξένα r – υποσύνολα του X (που ονομάζονται ομάδες του $\mathcal{G}$), δηλαδή $\mathcal{G}$ είναι μια διαμέριση του X, και $\mathcal{T}$ είναι μια συλλογή k - εγκάρσιων στοιχείων της $\mathcal{G}$, που ονομάζεται blocks, έτσι ώστε κάθε εγκάρσιο t - στοιχείο να περιέχεται σε ένα ακριβώς block.

(Ένα εγκάρσιο στοιχείο της $\mathcal{G}$ είναι ένα υποσύνολο του X που ικανοποιεί κάθε ομάδα το πολύ μία φορά.)

Έστω X μία αβελιανή ομάδα με v στοιχεία. Ένας $H-\sigma\chi\varepsilon\delta\iota\alpha\sigma\mu\acute{o}\varsigma$ καλείται κυκλικός, εφόσον ο αυτομορφισμός της ομάδα περιέχει μια κυκλική υποομάδα τάξης v. Εάν η κυκλική υποομάδα περιέχει μόνο κύκλους μήκους v, ο $H-\sigma\chi\varepsilon\delta\iota\alpha\sigma\mu\acute{o}\varsigma$ ονομάζεται αυστηρά κυκλικός.

Σχετικά με τους $H-\sigma\chi\varepsilon\delta\iota\alpha\sigma\mu o\acute{\upsilon}\varsigma$, ισχύει το ακόλουθο θεώρημα.

Θεώρημα 3.2

Υποθέτοντας ότι υπάρχει ένας $(n,w,\lambda)-OOC$ που είναι ισοδύναμος με έναν αυστηρά κυκλικό $(n,w,1)$ $(\lambda+1)$-σχεδιασμό, και έστω ότι υπάρχει ένας $w\times g^{\lambda}$ $(\lambda+1)$-απλός πίνακας D στο $\mathbb{Z}_g$,.

Τότε θα υπάρχει ένας αυστηρά κυκλικός σχεδιασμός $H(n,g,w,\lambda+1)$ στο $\mathbb{Z}_{ng}$.

Απόδειξη:

Εφαρμόζοντας την Βασική Κατασκευή σ' έναν $(n,w,\lambda)-OOC$ C, επιτυγχάνεται ένας $(gn,w,\lambda)-OOC$ C′. Έστω $\mathcal{X}=\mathbb{Z}_{ng}$, $\mathcal{G}=\{\mathcal{G}_i \mid i\in\mathbb{Z}_n\}$, και $\mathcal{T}$ είναι το σύνολο όλων των πιθανών κυκλικών μετατοπίσεων των κωδικών λέξεων του C′, όπου $\mathcal{G}_i=\{i+kn|k\in\mathbb{Z}_g\}$ για $i\in\mathbb{Z}_n$. Έστω ότι ισχύει ο ισχυρισμός: $(\mathcal{X},\mathcal{G},\mathcal{T})$ είναι ένας κυκλικός $H(n,g,w,\lambda+1)$ σχεδιασμός στο $\mathbb{Z}_{ng}$. Για να αποδειχθεί ο ισχυρισμός, θα πρέπει ο πίνακας $O=(D,\ D+1,\ \ldots,D+g-1)$ να είναι ένας ορθογώνιος πίνακας δύναμης $\lambda+1$ στο $\mathbb{Z}_g$. Το γεγονός ότι κάθε $(\lambda+1)$ – εγκάρσια στοιχεία της $\mathcal{G}$ περιέχονται σε ακριβώς ένα block του $\mathcal{T}$, προκύπτει από το γεγονός ότι ο O είναι ένας ορθογώνιος πίνακας, και επειδή ο αρχικός OOC αντιστοιχεί σε ένα $\lambda+1$ σχεδιασμό.

▪

Το ακόλουθο θεώρημα για 3-απλούς πινάκες είναι ζωτικής σημασίας για τις κατασκευές.

Θεώρημα 3.3

Για κάθε $g\geq 2$, υπάρχει ένας $4\times g^2$ 3-απλός πίνακας στο $\mathbb{Z}_g$.

Πόρισμα 3.1

Αν υπάρχει ένας $sSQS(n)$, για κάθε $g \geq 2$, τότε θα υπάρχει και ένας αυστηρά κυκλικός $H(n, g, 4, 3)$ σχεδιασμός.

Απόδειξη:

Αυτό είναι ένα άμεσο αποτέλεσμα των Θεωρημάτων 3.2 και 3.3.

Λήμμα 3.1

Αν υπάρχει ένας $CSQS(n)$ με $n \equiv 2, 10 (mod\ 12)$, τότε για κάθε $g \geq 2$ και $g \equiv 0 (mod\ 2)$, θα υπάρχει ένας αυστηρά κυκλικός $H(n, g, 4, 3)$ σχεδιασμός.

Απόδειξη:

Επειδή $n \equiv 2,\ 10\ (mod\ 12)$, ο $CSQS(n)$ δεν διαθέτει το εν τέταρτο της τροχιάς. Εάν πρόκειται για αυστηρά κυκλικό SQS, τότε το συμπέρασμα προκύπτει από το Πόρισμα 3.1.
Εάν περιέχει τη μισή τροχιά, πρέπει πρώτα να εφαρμοστεί ο ακόλουθος 3-απλός πίνακας του $CSQS(n)$ στο $\mathbb{Z}_2$,

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

και να διαγραφούν τα διπλότυπα από το σύστημα που θα προκύψει. Σε αυτό το σημείο, οι περιττές επαναλήψεις προέρχονται από τους μισούς τετραπλασιασμούς. Για οποιαδήποτε μισό τετραπλασιασμό, π.χ. $\left\{0, i, \frac{n}{2}, \frac{n}{2} + i\right\}$, εάν εφαρμοστεί η διαφορά του παραπάνω πίνακα σύμφωνα με τη βασική κατασκευή, θα έχουν επιτευχθεί τέσσερα blocks:

$$\left\{0, i, \frac{n}{2}, \frac{n}{2} + i\right\}, \left\{0, i, \frac{3n}{2}, \frac{3n}{2} + i\right\}, \left\{0, v + i, \frac{n}{2}, \frac{3n}{2} + i\right\}, \left\{0, n + i, \frac{3n}{2}, \frac{n}{2} + i\right\}.$$

Τα δύο πρώτα blocks βρίσκονται στην ίδια τροχιά, όπως και τα δύο τελευταία. Είναι εύκολο να ελεγχθεί ότι αν απαλειφθούν οι περιττές επαναλήψεις, θα προκύψει ένας $(2n, 4, 2) - OOC$. Τέλος, εφαρμόζονται οι 3-απλοί πίνακες στο $\mathbb{Z}_{g/2}$ του τελικού συστήματος για να προκύψει ένας αυστηρά κυκλικός $H(n, g, 4, 3)$ σχεδιασμός.

▪

Για την πλήρη χρήση της κατασκευής των $CSQSs$, γενικεύεται η έννοια των m - αποκομμένων $H - σχεδιασμών$.

Ορισμός 3.3

Αν $m|v$ με $v = ng$. Ένας αυστηρά κυκλικός m - αποκομμένος $H-\sigma\chi\epsilon\delta\iota\alpha\sigma\mu\acute{o}\varsigma$ στο $\mathbb{Z}_v$, συμβολίζεται ως $H(n, g, 4, 3; -m)$, είναι μια συλλογή DQs ενός αυστηρά κυκλικού $H(n, g, 4, 3)$ σχεδιασμού, εξαιρώντας κάθε DT που έχει εισόδους με κοινό παράγοντα $\frac{v}{m}$, ο οποίος παραλείπεται.

Παρόμοιο με το Λήμμα 3.1, είναι το εξής.

Λήμμα 3.2

Αν υπάρχει ένας $CSQSs(v, -m)$ χωρίς τροχιά τετάρτων, τότε θα υπάρχει ένας $H(v, g, 4, 3; -mg)$ σχεδιασμός, για οποιονδήποτε θετικό ακέραιο $g \geq 2$.

IV. Προσαρμοσμένος παράγοντας συστήματος και MCP

Στόχος είναι η κατασκευή ενός $sSQS(gn, -2g)$ από $\acute{\epsilon}\nu\alpha\nu$ $CSQS(n)$, ή ενός $sSQS(gn, -mg)$ από έναν $sSQS(n, -m)$ χωρίς να διαιρούνται οι τροχιές στα τέσσερα. Χρησιμοποιώντας τα Λήμματα 3.1 και 3.2, μπορούν να προκύψουν ένας αυστηρά κυκλικός $H(n, g, 4, 3)$ σχεδιασμός ή ένας $H(n, g, 4, 3; -mg)$ σχεδιασμός αντίστοιχα. Η πρόσθεση περισσότερων DQs στους αντίστοιχους $H - \sigma\chi\epsilon\delta\iota\alpha\sigma\mu o\acute{\upsilon}\varsigma$, ολοκληρώνει τα $sSQS(gn, -2g)$ ή $sSQS(gn, -mg)$ αντίστοιχα.

Λήμμα 4.1

Έστω ότι υπάρχει ένας αυστηρά κυκλικός $H(n, g, 4,3)$ σχεδιασμός με $n, g \equiv 0\ (mod\ 2)$, και έστω ότι υπάρχει ένα πλήρες σύνολο DQs τέτοιο ώστε οι DTs

$$[i]_{kn}, i \in \mathbb{Z}_{gn}, \frac{n}{2} \nmid i, 1 \leq k \leq \frac{(g-2)}{2} \quad \kappa\alpha\iota \quad [i]_{gn/2}, 0 \leq i \leq \frac{gn}{2}, \frac{n}{2} \nmid i$$

να διαιρούνται κάθε μία, ακριβώς από μία DQ .

Τότε θα υπάρχει ένας $sSQS(gn, -2g)$.

Λήμμα 4.2

Έστω ότι υπάρχει ένας αυστηρά κυκλικός $H(n, g, 4,3; -mg)$ σχεδιασμός με $n, g \equiv 0\ (mod\ 2)$, και έστω ότι υπάρχει ένα πλήρες σύνολο DQs τέτοιο ώστε οι DTs

$$[i]_{kn}, i \in \mathbb{Z}_{gn}, \frac{n}{m} \nmid i, 1 \leq k \leq \frac{(g-2)}{2} \quad \kappa\alpha\iota \quad [i]_{gn/2}, 0 \leq i \leq \frac{gn}{2}, \frac{n}{m} \nmid i$$

να διαιρούνται κάθε μία, ακριβώς από μία DQ.

Τότε θα υπάρχει ένας $sSQS(gn, -mg)$.

Ο στόχος των Λημμάτων 4.1 και 4.2 ανάγεται σε πεπερασμένα προβλήματα υπολογισμού, όπως είναι για παράδειγμα το πρόβλημα του προσαρμοσμένου παράγοντα συστήματος.

Ορισμός 4.1

Έστω g ένας ζυγός θετικός ακέραιος, K_g είναι ένα πλήρες γράφημα με κορυφή $\mathbb{Z}_g$, και $K_{\frac{g}{2}}$ είναι ένα πλήρες γράφημα με κορυφή $\mathbb{Z}_{\frac{g}{2}}$. Έστω F_i με $1 \leq i \leq \frac{g}{2} - 1$ να είναι ο $1^{ος}$ – παράγοντας του K_g, και $F_{\frac{g}{2}}$ να είναι ο $1^{ος}$ – παράγοντας του $K_{\frac{g}{2}}$.

Τότε το $C = \{F_i \,|1 \leq i \leq \frac{g}{2}\}$ καλείται προσαρμοσμένος παράγοντας συστήματος (matched factor system), τάξης g αν ικανοποιούνται οι παρακάτω συνθήκες:

1. για $1 \leq k,\ l \leq \frac{g}{2} - 1,$ το όριο $(i, i+l) \in F_k$ ανν $(-l-k-1-i, -l-1-i) \in F_l$
2. για $1 \leq k \leq \frac{g}{2} - 1,$ το όριο $(i, i+\frac{g}{2}) \in F_k$ τότε $(-k-1-i, -1-i) \in F_{\frac{g}{2}}$

Παράδειγμα 4.1

Έστω $g = 8$. Οι ακόλουθοι τέσσερις $1^{οι}$ – παράγοντες διαμορφώνουν τον προσαρμοσμένο παράγοντα συστήματος τάξης 8.

$$F_1 = \{(1,2), (4,5), (6,0), (3,7)\}$$
$$F_2 = \{(6,7), (2,4), (1,3), (5,0)\}$$
$$F_3 = \{(5,7), (1,4), (0,3), (2,6)\}$$
$$F_4 = \{(0,3), (1,2)\}$$

Είναι εύκολο να εξακριβωθεί ότι:

$(1,2) \in F_1\ \alpha\nu\nu\ (4,5) \in F_1, (6,0) \in F_1\ \alpha\nu\nu\ (6,7) \in F_2$
$(3,7) \in F_1\ \tau\acute{o}\tau\varepsilon\ (3,0) \in F_4$
$(2,4) \in F_2\ \alpha\nu\nu\ (1,3) \in F_2, (5,0) \in F_2\ \alpha\nu\nu\ (5,7) \in F_3, (1,4) \in F_3\ \alpha\nu\nu\ (0,3) \in F_3$ και
$(2,6) \in F_3\ \tau\acute{o}\tau\varepsilon\ (2,1) \in F_4$.

▪

Για να συμπεριληφθούν όλες οι υπόλοιπες DTs στα Λήμματα 4.1 και 4.2, χρησιμοποιείται μόνο μία ενιαία μορφή DQs, η οποία αναφέρεται στο ακόλουθο λήμμα., στο οποίο χρησιμοποιείται ο ορισμός του προσαρμοσμένου παράγοντα συστήματος.

Λήμμα 4.3

Μία DQ $(in+j, -(l+i+1)n+n-j, (k+l+i)n+j, -(k+i+1)n+n-j)$ καλύπτει τις τέσσερις ακόλουθες DTs:

$[in+j]_{kn}, [(i+l)n+j]_{kn}, [(-i-k-l-1)n+(n-j)]_{ln}, [(-i-l-1)n+(n-j)]_{ln}.$

Απόδειξη:

Αυτό προκύπτει από τον ορισμό της DQ και το συμβολισμό που χρησιμοποιείται.

Μία DQ της παραπάνω μορφής καλύπτει δύο ζεύγη DTs, δηλαδή $[in+j]_{kn}$, $[(i+l)n+j]_{kn}$, $και$ $[(-i-k-l-1)n+(n-j)]_{ln}, [(-i-l-1)n+(n-j)]_{ln}$. Αυτή η παρατήρηση βοηθά για να συσχετιστεί ο προσαρμοσμένος παράγοντας συστήματος με το ακόλουθο λήμμα.

Λήμμα 4.4

Εάν υπάρχουν ο προσαρμοσμένος παράγοντας συστήματος τάξης g και ένας αυστηρά κυκλικός $H(n,g,4,3)$ σχεδιασμός, τότε θα υπάρχει ένας $sSQS(gn,-2g)$.

Απόδειξη:

Έστω $C=\{F_1,F_2,\dots,F_{\frac{g}{2}}\}$ είναι ο προσαρμοσμένος παράγοντας συστήματος τάξης g. Σύμφωνα με τον ορισμό του προσαρμοσμένου παράγοντα συστήματος ισχύει ότι, αν $(i,i+l)\in F_k$, τότε $(-l-k-1-i,-l-1-i)\in F_l$.

Με αυτά τα δύο όρια, κατασκευάζονται $(n-2)DQs$ σύμφωνα με τα ακόλουθα:

$$(in+j,-(l+i+1)n+n-j,(k+l+i)n+j,-(k+i+1)n+n-j)$$

$όπου$ $1\le j\le n-1, j\neq\frac{n}{2}$.

Τότε, τα $4(n-2)DTs$ καλύπτονται από:

$$[in+j]_{kn},[(i+l)n+j]_{kn},[(-i-k-l-1)n+(n-j)]_{ln},[(-i-l-1)n+(n-j)]_{ln}$$

όπου $1\le j\le n-1$, $j\neq\frac{n}{2}$.

Όταν κατασκευάζονται οι $\frac{g(g-1)}{8}$ DQs συναρτήσει του προσαρμοσμένου παράγοντα συστήματος τάξης g για κάθε $1\le \mathrm{k}\le\frac{g}{2}$, τότε καλύπτονται οι ακόλουθες συλλογές DTs

$$\{[in+j]_{kn},[(i+l)n+j]_{kn}|(i,i+l)\in F_k, 1\le j\le n-1, j\neq\frac{n}{2}\}$$

Εφόσον F_k είναι $1^{ος}$ – παράγοντας, το παραπάνω σύνολο είναι ισοδύναμο με

$\left\{[i]_{kn}\;\middle|\; i\in\mathbb{Z}_{gn}, \frac{n}{2}\nmid i\right\}$ $όταν$ $1\le k\le\frac{g}{2}-1$, και

$$\left\{[i]_{\frac{gn}{2}}\mid 0\le i\le\frac{gn}{2}, \frac{n}{2}\nmid i\right\}\ όταν\ k=\frac{g}{2}$$

Συνεπώς, οι ιδιότητες του προσαρμοσμένου παράγοντα συστήματος τάξης g καλύπτουν όλες τις DTs του Λήμματος 4.1.

▪

Λήμμα 4.5

Εάν υπάρχουν ο προσαρμοσμένος παράγοντας συστήματος τάξης g και ένας αυστηρά κυκλικός $H(n, g, 4,3; -m)$ σχεδιασμός, τότε υπάρχει $sSQS(gn, -mg)$.

Απόδειξη:

Είναι ακριβώς η ίδια απόδειξη όπως στο Λήμμα 4.4, επιβάλλοντας περισσότερους περιορισμούς στην τιμή j: $\frac{n}{m} \nmid j$.

▪

Για να υπάρξει ένας προσαρμοσμένος παράγοντας συστήματος κάποιας τάξης, πρέπει να μεταφραστεί η ύπαρξη του προβλήματος ενός MCP. Ορίζεται λοιπόν, τη γραφική παράσταση για το MCP.

Ορισμός 4.2

Έστω g ένας ζυγός ακέραιος, και έστω

$$\mathcal{V} = \{\big((i, i+l), k\big), ((-l-k-1-i, -l-1-i), l)\big\} \mid i \in \mathbb{Z}_g, 1 \leq l, k \leq \frac{g}{2}\}$$

είναι το σύνολο όλων των πιθανών προσαρμοσμένων ορίων. Έτσι, κάθε κορυφή στο $\mathcal{V}$ είναι ένα ζεύγος ορίων που ανήκουν σε ορισμένους $1^{ους}$ - παράγοντες. Για κάθε δύο κορυφές του $\mathcal{V}$, το ένα όριο προστίθεται στο σύνολο $\mathcal{E}$, είτε $k \neq l$ είτε $k = l$ με $\{i, i+1\} \cap \{-l-k-1-i, -l-1-i\} = \emptyset$.

Λήμμα 4.6

Εάν η γραφική παράσταση $(\mathcal{V}, \mathcal{E})$ που ορίζεται παραπάνω έχει πλήρες μέγεθος γραφήματος $\frac{g(g-1)}{8}$, τότε υπάρχει ένας προσαρμοσμένος παράγοντας συστήματος τάξης g.

Απόδειξη:

Απλή μέτρηση δείχνει το αποτέλεσμα.

Λήμμα 4.7

Υπάρχει ένας προσαρμοσμένος παράγοντας συστήματος τάξης g, με $g \in \{8, 16, 24\}$.

Απόδειξη:

Αν F_i είναι ο i - οστος $1^{ος}$ - παράγοντας με $1 \leq i \leq \frac{g}{2}$, τότε παρατίθενται τα όρια του κάθε $1^{ου}$ – παράγοντα.

- $g = 8$ στο παράδειγμα 4.1
- $g = 16$

$F_1 = \{(5,6),(8,9),(11,12),(2,3),(13,14),(0,1),(4,10),(7,15)\}$
$F_2 = \{(4,6),(7,9),(10,12),(1,3),(13,15),(14,0),(5,8),(11,2)\}$
$F_3 = \{(5,7),(1,4),(8,11),(15,2),(10,13),(0,3),(9,12),(6,14)\}$
$F_4 = \{(6,10),(1,5),(14,2),(9,13),(15,3),(8,12),(0,4),(7,11)\}$
$F_5 = \{(2,7),(3,8),(9,14),(12,1),(15,4),(6,11),(10,0),(5,13)\}$
$F_6 = \{(4,5),(10,15),(11,1),(8,14),(12,2),(7,13),(0,6),(3,9)\}$
$F_7 = \{(11,13),(2,9),(15,6),(14,5),(3,10),(0,7),(1,8),(4,12)\}$
$F_8 = \{(7,0),(6,1),(5,2),(4,3)\}$

- $g = 24$

$F_1 = \{(1,2),(4,5),(6,7),(8,9),(10,12),(11,23),$
$(13,14),(15,16),(17,18),(19,3),(20,21),(22,0)\}$
$F_2 = \{(0,2),(1,3),(4,6),(5,16),(7,9)(8,13),$
$(10,11),(12,14),(15,17),(18,20),(19,21),(22,23)\}$
$F_3 = \{(0,3),(1,4),(5,8),(6,9),(7,13),(10,22),$
$(11,14),(12,15),(16,19),(17,20),(18,21),(23,2)\}$
$F_4 = \{(3,7),(4,8),(5,14),(6,10),(9,13),(11,15),$
$(12,16),(17,21),(18,1),(19,23),(20,0),(22,2)\}$
$F_5 = \{(1,6),(2,7),(4,14),(5,13),(8,10),(9,21),$
$(11,16),(12,17),(15,20),(18,23),(19,0),(22,3)\}$
$F_6 = \{(0,6),(3,9),(7,10),(8,14),(11,17),(12,18),$
$(13,19),(15,21),(16,1),(20,2),(22,4),(23,5)\}$
$F_7 = \{(0,7),(3,10),(4,11),(5,12),(6,13),(8,20),$
$(9,16),(14,21),(15,23),(17,1),(18,22),(19,2)\}$
$F_8 = \{(1,9),(3,11),(4,12),(5,10),(6,14),(8,16),$
$(13,21),(15,22),(17,0),(18,2),(19,20),(23,7)\}$
$F_9 = \{(1,10),(4,13),(5,9),(6,15),(7,19),(11,20)$
$(12,21),(14,0),(16,22),(17,2),(18,3),(23,8)\}$
$F_{10} = \{(0,10),(3,13),(4,9),(7,17),(8,18),(11,21)$
$(12,22),(14,23),(15,1),(16,2),(19,5),(20,6)\}$
$F_{11} = \{(5,7),(6,18),(8,19),(9,20),(10,21),(11,22),$
$(12,23),(13,0),(14,1),(15,2),(16,3),(17,4)\}$
$F_{12} = \{(6,5),(7,4)(8,3),(9,2),(10,1),(11,0)\}$

V. Αναδρομικές κατασκευές για βέλτιστους $(v, 4, 2) - OOCs$

Θεώρημα 5.1

Εάν υπάρχει ένας $sSQS(gn, -mg)$ και ένας αυστηρά κυκλικός $3 - (mg, 4, 1)$ σχεδιασμός που αποτελείται από L DQs με $\frac{(mg-1)(mg-2)}{24} - L < 1$, τότε θα υπάρχει μία αυστηρά κυκλική βέλτιστη $3 - (gn, 4, 1)$ ομαδοποίηση, δηλαδή ένας βέλτιστος $(gn, 4, 2) - OOC$.

Απόδειξη:

Χρησιμοποιείται η κατασκευή του Λήμματος 2.3. Για οποιαδήποτε $DQ\ (a, b, c, d)$ μιας αυστηρά κυκλικής $3-(mg, 4, 1)$ ομαδοποίησης, κατασκευάζεται μία νέα $DQ\ (a \cdot \frac{n}{m}, b \cdot \frac{n}{m}, c \cdot \frac{n}{m}, d \cdot \frac{n}{m})$. Η ένωση των DQs και του $sSQS(gn, -mg)$ δίνει μια αυστηρά κυκλική και βέλτιστη $3-(mg, 4, 1)$ ομαδοποίηση σύμφωνα με τους όρους του λήμματος.

Η βελτιστότητα της ομαδοποίησης προκύπτει από την ανισότητα

$$\frac{(mg-1)(mg-2)}{24} - L < 1$$

η οποία εγγυάται ότι ο αριθμός των DTs στο $\mathbb{Z}_{gn}$, που δεν διαιρούνται με την προκύπτουσα $3-(mg, 4, 1)$ ομαδοποίηση, είναι λιγότερο από 4. Αυτό, ολοκληρώνει την απόδειξη.

Προτού αποδειχθεί το κύριο αποτέλεσμά, απαριθμούνται διάφορα λήμματα.

Λήμμα 5.1

Η ύπαρξη ενός $CSQS(2n, -2m)$ εγγυάται την ύπαρξη ενός $CSQS(4n, -4m)$ εφόσον, $n \equiv m(mod\ 2)$.

Πόρισμα 5.1

Αν υπάρχει ένας $CSQS(n)$ με $n \equiv 2, 10\ (mod\ 12)$, τότε θα υπάρχει για κάθε $x \geq 1$ ένας $CSQS(2^x \cdot n, -2^{x+1})$.

Απόδειξη:

Αν υπάρχει ένας $CSQS(n)$ $n \equiv 2, 10\ (mod\ 12)$, τότε θα υπάρχει ο $CSQS(2n)$. Ο $CSQS(2n)$ στην πραγματικότητα παράγει τον $CSQS(2n, -4)$, οπότε μπορεί να εφαρμοστεί το Λήμμα 5.1 για να αποδειχτεί το αποτέλεσμα.

Πόρισμα 5.2

Αν υπάρχει ένας $CSQS(n)$ με $4|n$, τότε θα υπάρχει ένας $CSQS(2^x \cdot n, -2^{x+2})$ για κάθε $x \geq 0$.

Απόδειξη:

Ένας $CSQS(n)$ με $4|n$ ισοδυναμεί μ' έναν $CSQS(n, -4)$. Με βάση το Λήμμα 5.1, θα υπάρχει ένας $CSQS(2^x \cdot n, -2^{x+2})$ για οποιαδήποτε $x \geq 1$.

Παρουσιάζεται η πρώτη άπειρη οικογένεια για βέλτιστους $(n, 4, 2) - OOCs$ με $n = 2^x$.

Λήμμα 5.2.

Για όλα τα $x \geq 4$, υπάρχει ένας $CSQS(2^x, -2^{x+1})$.

Το ακόλουθο αποτέλεσμα είναι γνωστό.

Λήμμα 5.3

Υπάρχει ένας $CSQS(2^x)$ αν και μόνο αν $x \neq 3, 4$.

Λήμμα 5.4

Υπάρχει ένας βέλτιστος $(n, 4, 2) - OOC$ για $n = 8, 16, 32$.

Λήμμα 5.5

Υπάρχει ένας βέλτιστος $(64, 4, 2) - OOC$.

Απόδειξη:

Έχει βρεθεί ότι ο βέλτιστος $(64, 4, 2) - OOC$ έχει 162 κωδικές λέξεις.

Θεώρημα 5.2

Υπάρχει ένας βέλτιστος $(2^x, 4, 2) - OOC$ για όλα τα $x \geq 3$.

Απόδειξη:

Δεν υφίσταται ένας $CSQS(16)$, αλλά υπάρχει ένας $CSQS(16, -8)$, ο οποίος σύμφωνα με το Λήμμα 5.2, δεν περιέχει τετραπλάσια τροχιά. Χρησιμοποιώντας το Λήμμα 3.2, αποδεικνύεται ότι υπάρχει ένας αυστηρά κυκλικός $H(16, 8,4,3; -64)$, ενώ από το Λήμμα 4.5, υπάρχει ένας $sSQS(128, -64)$. Τέλος, το Λήμμα 5.5 και το Θεώρημα 5.1 δίνουν την εγγύηση για την ύπαρξη ενός βέλτιστου $(128, 4, 2) - OOC$. Για $(2^x, 4, 2) - OOC$ με $x \geq 8$ και μεγαλύτερα, μπορούν να χρησιμοποιηθούν $CSQS(2^x)$ με $x \geq 5$. Η ύπαρξη $CSQS(2^x)$ συνεπάγει την ύπαρξη $CSQS(2^x, -4)$. Χρησιμοποιώντας τα Λήμματα 3.2, 4.5, 5.4 και το Θεώρημα 5.1, υπάρχει μία αυστηρά κυκλική $3 - (2^x, 4, 1)$ ομαδοποίηση, δηλαδή ένας βέλτιστος $(2^x, 4, 2)$ – OOC με $x \geq 8$.

Θεώρημα 5.3

Αν υπάρχει ένας $CSQS(n)$, τότε θα υπάρχει μία αυστηρά κυκλική και βέλτιστη $3 - (2^x \cdot n, 4, 1)$ ομαδοποίηση, ή ισοδύναμα ένας βέλτιστος $(2^x \cdot n, 4, 2) - OOC$ με $x \geq 3$.

Απόδειξη:

Εάν ένας $CSQS(n)$ δεν περιέχει τετραπλάσια τροχιά, τότε από το Λήμμα 3.1, υπάρχει αυστηρά κυκλικός $H(n,8,4,3)$ σχεδιασμός. Από τα Λήμματα 4.4 και 4.7, υπάρχει ένας s$SQS(8n-16)$. Δεδομένου ότι ο $CSQS(n)$ δεν περιέχει τετραπλάσια τροχιά, από το Πόρισμα 5.1, θα υπάρχει $CSQS(2^x n, -2^{x+1})$ για οποιαδήποτε $x \geq 1$. Χρησιμοποιώντας το Λήμμα 3.2, υπάρχει ένας αυστηρά κυκλικός $H(2^x n,8,4,3;-2^{x+1}\cdot 8)$. Ενώ, από τα Λήμματα 4.5 και 4.7, θα υπάρχει s$SQS(2^{x+3}n,-2^{x+4})$.

Εάν ο $CSQS(n)$ περιέχει τετραπλάσια τροχιά, τότε από το Πόρισμα 5.2, υπάρχει $CSQS(2^x\cdot n,-2^{x+2})$ για κάθε $x \geq 0$. Επομένως, θα υπάρχει ένας αυστηρά κυκλικός $H(2^x n,8,4,3;-2^{x+2}\cdot 8)$. Από τα Λήμματα 4.5 και 4.7, είναι γνωστό ότι υπάρχουν s$SQS(2^{x+3}\cdot n,-2^{x+5})$.

Τέλος, για αμφότερες τις περιπτώσεις, ισχύουν τα Θεωρήματα 5.1 και 5.2 για να ολοκληρωθεί η απόδειξη.

VI. Συμπέρασμα

Σε αυτή την ενότητα, παρουσιάστηκε μια αναδρομική κατασκευή για τους βέλτιστους $(n,4,2)-OOC$s. Αυτή η κατασκευή μπορεί γενικότερα να εφαρμοστεί σε οποιοδήποτε $CSQS(n)$ για να παραχθεί μία αυστηρά κυκλική βέλτιστη $3-(2^x\cdot n,4,1)$ ομαδοποίηση με $x \geq 3$, δηλαδή ένας βέλτιστος $(2^x\cdot n,4,2)-OOC$ με $x \geq 3$.

Ο προσαρμοσμένος παράγοντας συστήματος συμπληρώνει το κενό ανάμεσα σ' έναν αυστηρά κυκλικό $H-\sigma\chi\epsilon\delta\iota\alpha\sigma\mu\acute{o}$ και σ' ένα βέλτιστο $(n,4,2)-OOC$. Βρέθηκε ότι ο προσαρμοσμένος παράγοντας συστήματος έχει πολλές διαφορετικές τάξεις, όπως $g=8,16,24,32$. Ο προσαρμοσμένος παράγοντας συστήματος τάξης 24 μπορεί να χρησιμοποιηθεί για την κατασκευή ενός s$SQS(24n,-48)$, αν υπάρχει ένας $CSQS(n)$ χωρίς το εν τέταρτο της τροχιάς. Δυστυχώς όμως, δεν έχει ακόμα βρεθεί ο βέλτιστος $(48,4,2)-OOC$.

Τέλος, πιστεύεται ότι $8|g$ αποτελεί αναγκαία και ικανή προϋπόθεση για την ύπαρξη ενός προσαρμοσμένου παράγοντα συστήματος τάξης g.

Σύνοψη

Οι κατασκευές των σταθερού βάρους συμμετρικών OOCs περιλαμβάνουν τις συνδυαστικές κατασκευές, τις κατασκευές που βασίζονται στην προβολική γεωμετρία τις αλγεβρικές κατασκευές και τις αναδρομικές κατασκευές.

Οι συνδυαστικές κατασκευές πραγματεύονται τη σχέση μεταξύ OOCs και οικογένειες διαφορών. Μία $(n, w, 1)$ οικογένεια διαφορών είναι ακριβώς ένας $(n, w, 1) - OOC$, και συνεπώς, οι συνδυαστικές κατασκευές είναι κατάλληλες μόνο για την κατασκευή των $(n, w, 1) - OOC$s.

Όταν $w \leq 3$ ένας οπτικός ορθογώνιος κώδικας μπορεί εύκολα να κατασκευαστεί με βέλτιστη πληθικότητα. Αν και ένας οπτικός ορθογώνιος κώδικας μπορεί να κατασκευαστεί για $w = 4$, η πληθικότητα του δεν είναι βέλτιστη και η κατασκευή του είναι περίπλοκη. Όταν $w \geq 5$, είναι δύσκολο να κατασκευαστούν οι $(n, w, 1) - OOC$s. Η απόδοση (BER bit error rate – ρυθμός σφαλμάτων) των OCDMA συστημάτων μειώνεται δραματικά καθώς μειώνεται το w, δηλαδή όταν αριθμός των ταυτόχρονων χρηστών σε ένα δίκτυο, είναι πολύ περιορισμένος.

Οι κατασκευές της προβολικής γεωμετρίας για OOCs βασίζονται στην πεπερασμένη προβολική γεωμετρία. Οι ευθείες στην πεπερασμένη προβολική γεωμετρία αντιστοιχούν σε κωδικές λέξεις OOCs με βάρος w. Αυτό συμβαίνει επειδή κάθε δύο ευθείες στην προβολική γεωμετρία τέμνονται το πολύ σε ένα σημείο. Συνεπώς, μπορεί να επιτευχθεί OOC με αυτοσυσχέτιση $\lambda_\alpha = 1$ και ετεροσυσχέτιση $\lambda_c = 1$.

Η αλγεβρική κατασκευή χρησιμοποιεί την θεωρία πεπερασμένων σωμάτων για την κατασκευή OOC. Η διαδικασία κατασκευής είναι σχετικά περίπλοκη. Μέχρι στιγμής, οι υπάρχουσες κατασκευές μπορούν να χρησιμοποιηθούν για να κατασκευαστεί κάποιος σταθερού βάρους συμμετρικός OOC με δεδομένο μήκος και βάρος κώδικα. Στις γενικότερες αλγεβρικές κατασκευές των OOCs εξακολουθούν να γίνονται έρευνες.

Οι αναδρομικές κατασκευές χρησιμοποιούν πίνακες διαφορών για να κατασκευαστούν OOC. Για παράδειγμα, ένας $(n_1 n_2, k, 1) - OOC$, C, μπορεί να κατασκευαστεί χρησιμοποιώντας έναν υπάρχων $(n_1, w, 1) - OOC$, C_1, με πληθικότητα $|C_1|$ και έναν $(n_2, w, 1) - OOC$, C_2, με πληθικότητα $|C_2|$. Αν οι πληθικότητες των C_1 και C_2 είναι βέλτιστες τότε ο C είναι επίσης βέλτιστος και η πληθικότητα του είναι $|C_2| + n_2|C_1|$. Όταν κατασκευάζεται ο C, πρέπει αρχικά να κατασκευαστεί ένας πίνακας διαφορών και στη συνέχεια να σχεδιαστεί ο C χρησιμοποιώντας τους C_1 , C_2 και τον πίνακα διαφορών. Αυτό το είδος κατασκευής είναι κατάλληλο μόνο για την κατασκευή των σταθερού βάρους συμμετρικών OOCs.

Ένας από τους λόγους για τους οποίους η πληθικότητα των σταθερού βάρους συμμετρικών OOCs είναι περιορισμένη, είναι ότι ο περιορισμός αυτοσυσχέτισης και ο περιορισμός ετεροσυσχέτιση είναι ο ίδιος. Στην πραγματικότητα, επειδή οι επιπτώσεις τους στην απόδοση του συστήματος είναι διαφορετικές, προκειμένου να αυξηθεί η ικανότητα του συστήματος, δηλαδή ο αριθμός των χρηστών, ο περιορισμός αυτοσυσχέτισης του OOC μπορεί να γίνει ελαστικότερος. Αυτό θα έχει ως αποτέλεσμα τους σταθερού βάρους ασύμμετρους OOCs που θα παρουσιαστούν στο επόμενο κεφάλαιο.

Βιβλιογραφία

[1]. M. J. Colbourn and C. J. Colbourn, Cyclic block designs with block size 3, Eur. J. Combin., Vol. 2 (1981) pp. 21–26

[2]. M. Jimbo, A recursive construction for 1-rotational Steiner 2-designs, Utilitas Math., Vol. 26 (1984) pp. 45–61.

[3]. M. Buratti, Recursive constructions for difference matrices and relative difference families, J. of Combin. Designs, Vol. 6 (1998) pp. 165–182.

[4]. J. Yin, Some combinatorial constructions for optical orthogonal codes, Discrete Math., Vol. 185 (1998) pp. 201–219.

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

3ο Κεφάλαιο
Σταθερού βάρους Ασύμμετροι OOCs

Αν η τιμή αυτοσυσχέτισης λ_α είναι μεγαλύτερη από την τιμή ετεροσυσχέτισης λ_c, τότε η πληθικότητα του OOC θα αυξηθεί σε μεγάλο βαθμό. Θα αναφερθούν, λοιπόν, OOC με $\lambda_\alpha > \lambda_c$, δηλαδή, σταθερού βάρους ασύμμετροι OOC.

Ορισμός

Ένας $(n, w, \lambda_\alpha, \lambda_c) - OOC$ καλείται σταθερού βάρους ασύμμετρος OOC (constant weight asymmetric OOC) όταν $\lambda_\alpha \neq \lambda_c, \lambda_c = 1, \lambda_\alpha > 1$.

Είναι φανερό ότι, ο σταθερού βάρους συμμετρικός οπτικός ορθογώνιος κώδικας είναι μια αξιοσημείωτη περίπτωση του σταθερού βάρους ασύμμετρου $(n, w, \lambda_\alpha, \lambda_c) - OOC$.

Πληθικότητα Σταθερού βάρους Ασύμμετρων $OOCs$

Ορισμός

Η τιμή $\Phi(n, w, \lambda_\alpha, \lambda_c)$ είναι η πληθικότητα του βέλτιστου $(n, w, \lambda_\alpha, \lambda_c) - OOC$.

Ισχύει,

$$\Phi(n, w, \lambda_\alpha, \lambda_c) \equiv \max\{|C|: C \text{ είναι ένας } (n, w, \lambda_\alpha, \lambda_c) - OOC\}.$$

Το ακόλουθο θεώρημα αναφέρεται στην πληθικότητα του άνω φράγματος για σταθερού βάρους ασύμμετρους $OOCs$.

Θεώρημα

Υποθέτοντας ότι C είναι ένας βέλτιστος $(n, w, \lambda_\alpha, \lambda) - OOC$, τότε το άνω φράγμα για σταθερού βάρους ασύμμετρους $OOCs$ θα είναι:

$$\Phi(n, w, \lambda_\alpha, \lambda) \leq \left\lceil \frac{(n-1)(n-2)\dots(n-\lambda)\lambda_\alpha}{w(w-1)(w-2)\dots(w-\lambda)} \right\rceil$$

Κατασκευές για Σταθερού βάρους Ασύμμετρους $OOCs$

Σε αυτό το κεφάλαιο θα παρουσιαστούν δύο κατασκευές για $(n, w, 2, 1) - OOCs$, οι οποίες είναι βασισμένες στους μη πλήρεις σχεδιασμούς κατά μπλοκ $(BIBD)$. Ένας $BIBD$ είναι ισοδύναμος με τον $(n, w, 1, 1) - OOC$.

1η Κατασκευή

- Αν w είναι άρτιος $w = 2m$, και αν n είναι πρώτος αριθμός τέτοιος ώστε $n = \frac{w^2 t}{2} + 1$, με t ακέραιο. Έστω α το αρχικό στοιχείο του $GF(n)$ τέτοιο ώστε $\{log_\alpha[\alpha^{kmt} - 1] : 1 \leq k \leq m\}\ (mod\ m)$.

  Τότε, τα ακόλουθα blocks:

  $$\left\{\left[\alpha^{mi}, \alpha^{m(i+t)}, \alpha^{m(i+2t)}, \dots, \alpha^{m(i+(2m-1)t)}\right] : 0 \leq 1 \leq t - 1\right\}$$

  σχηματίζουν τους σταθερού βάρους ασύμμετρους $(n, w, 2, 1) - OOCs$ με $w = 2m$ και πληθικότητα $|C| = t = \frac{2(n-1)}{w^2} \approx 2\ \Phi(n, w, 1, 1)$.

- Αν w είναι περιττός $w = 2m + 1$, και αν n είναι πρώτος αριθμός τέτοιος ώστε $n = \frac{(w^2-1)\, t}{2} + 1$, με t ακέραιο. Έστω α το αρχικό στοιχείο του $GF(n)$ τέτοιο ώστε $\left\{log_\alpha\left[\alpha^{k(m+1)t} - 1\right] : 1 \leq k \leq m\right\}\ mod\ (m + 1)$.

  Τότε, τα ακόλουθα blocks:

  $$\left\{\left[0, \alpha^{(m+1)i}, \alpha^{(m+1)(i+t)}, \alpha^{(m+1)(i+2t)}, \dots, \alpha^{(m+1)(i+(2m-1)t)}\right] : 0 \leq 1 \leq t - 1\right\}$$

  σχηματίζουν τους σταθερού βάρους ασύμμετρους $(n, w, 2, 1) - OOCs$ με $w = 2m + 1$ και πληθικότητα $|C| = t = \frac{2(n-1)}{w^2-1} \approx 2\ \Phi(n, w, 1, 1)$.

Παράδειγμα

Η κατασκευή των σταθερού βάρους ασύμμετρων $(37,5,2,1) - OOCs$.

Ο πρώτος αριθμός n ισούται με 37. Επειδή, $w = 2m + 1 = 5$ και $n = \frac{w^2 t}{2} + 1 = 37$, $m = 2\ και\ t = 3$. Το $\alpha = 2$ είναι το αρχικό στοιχείο του $GF(37)$. Τότε,

$$\{\left[0, \alpha^{3i}, \alpha^{3(i+3)}, \alpha^{3(i+6)}, \alpha^{3(i+9)}\right]\ (mod\ 37) : i = 0, 1, 2\},$$

$$2^6 = 27\ (mod\ 37), 2^9 = 31\ (mod\ 37), 2^{18} = 36\ (mod\ 37), 2^{27} = 6\ (mod\ 37)$$

Άρα, σχηματίζονται οι ακόλουθες τρεις κωδικές λέξεις:

$$\{0,1,6,31,36\}, \{0,8,11,26,29\}, \{0,10,14,23,27\}$$

2η Κατασκευή

- Η κατασκευή των $(n, w, 2, 1) - OOCs$ με $w = 4m$. Έστω, $n = \frac{w^2 t}{2} + 1$ πρώτος αριθμός, με $w = 4m$ και έστω ότι a είναι το αρχικό στοιχείο του $GF(n)$.

  Οι ακόλουθες ισότητες:

  $a^{k\,4mt+y} - 1 = a^{i_k}, για\ \ k = 0, 1, \dots, m-1$

  $a^{k\,4mt} - a^{y} = a^{j_k}\ , για\ \ k = 1, 2, \dots, m$

  $a^{k\,4mt} - 1 = a^{r_k}\ , για\ \ k = 1, 2, \dots, m$

  $a^{y}(a^{k\,4mt} - 1) = a^{s_k}\ , για\ \ k = 1, 2, \dots, m$

  για κάποιο ακέραιο y, $1 \le y \le 4mt - 1$, όπου οι ακέραιοι $i_0, i_1, \dots, i_{m-1}, j_1, \dots, j_m, r_1, \dots, r_m, s_1, \dots, s_m$ είναι όλοι διακεκριμένοι $modulo\ (4m)$.

  Τότε, τα ακόλουθα blocks:

  $$\{\left[\alpha^{4mi}, \alpha^{y+4mi}, \alpha^{4mt+4mi}, \alpha^{4mt+y+4mi}, \dots, \alpha^{4mt(2m-1)+4mi}, \alpha^{4mt(2m-1)+y+4mi}\right] : 0 \le 1 \le t-1\}$$

  σχηματίζουν κωδικές λέξεις των $(n, w, 2, 1) - OOCs$ με $w = 4m$ και η πληθικότητα του κώδικα είναι $|C| = t = \frac{2(n-1)}{w^2} \approx 2\,\Phi(n, w, 1, 1)$.

  Παράδειγμα

  Η κατασκευή των $(41, 4, 2, 1) - OOCs$.

  Το μέγεθος του κώδικα είναι $n = 41$ που είναι πρώτος αριθμός. Εφόσον, $n = \frac{w^2 t}{2} + 1 = 41$, τότε θα είναι $w = 4m = 4\ και\ t = 5$ και άρα $m = 1$. Για $y = 3\ και\ \alpha = 6$ να είναι το αρχικό στοιχείο του $GF(41)$. Επομένως,

  $$6^y - 1 = 10 = 6^8, 6^{20} - 6^y = 29 = 6^7, 6^{20} - 1 = 39 = 6^6, 6^y(6^{20} - 1) = 19 = 6^9$$

  δηλαδή, $i_0 = 8,\ j_1 = 7,\ r_1 = 6\ και\ s_1 = 9$.

  Τα $i_0,\ j_1,\ r_1,\ s_1$ είναι διακεκριμένα $modulo$ 4. Τότε,

  $$\{\left[\alpha^{4i}, \alpha^{3+4i}, \alpha^{20+4i}, \alpha^{20+3+4i}\right] (mod\ 41) : i = 0, 1, 2, 3, 4\},$$

  $$6^3 = 11\ (mod\ 41), 6^4 = 25\ (mod\ 41), 6^{20} = 40\ (mod\ 41), 6^{23} = 30\ (mod\ 41)$$

  Άρα, σχηματίζονται οι ακόλουθες τρεις κωδικές λέξεις:

$$\{1,11,30,40\},\{12,16,25,29\},\{10,13,28,31\},\{3,4,37,38\},\{7,18,23,34\}$$

Η πληθικότητα είναι $|C| = 5 > \Phi\,(41,4,1) = 3$.

Όμως, επειδή $|C| = 5 < \Phi\,(41,4,2,1) = 6$ ο κώδικας δεν είναι βέλτιστος.

- Η κατασκευή των $(n,w,2,1) - OOCs$ με $w = 4m+1$. Έστω, $n = \frac{(w^2-1)t}{2} + 1$ πρώτος αριθμός, με $w = 4m+1$ και έστω ότι a είναι το αρχικό στοιχείο του $GF(n)$.

  Οι ακόλουθες ισότητες:

  $a^{k\,(4m+2)t+y} - 1 = a^{i_k}\,, για\alpha\;\; k = 0,1,\dots,m-1$

  $a^{k\,(4m+2)t} - a^{y} = a^{j_k}\;, για\alpha\;\; k = \;1,2,\dots,m$

  $a^{k\,(4m+2)t} - 1 = a^{r_k}\,, για\alpha\;\; k = 1,2,\dots,m$

  $a^{y}(a^{k\,(4m+2)t} - 1) = a^{s_k}\,, για\alpha\;\; k = 1,2,\dots,m$

  για κάποιο ακέραιο y, $1 \le y \le (4m+2)t - 1$, όπου οι ακέραιοι $i_0, i_1, \dots, i_{m-1}$, $j_1, \dots, j_m$, $r_1, \dots, r_m$, $s_1, \dots, s_m$ είναι όλοι διακεκριμένοι $modulo(4m+2)$.

  Τότε, τα ακόλουθα blocks:

  $$\{[0, \alpha^{(4m+2)i}, \alpha^{y+(4m+2)i}, \alpha^{(4m+2)t+(4m+2)i}, \alpha^{(4m+2)t+y+(4m+2)i}, \dots,$$
  $$a^{t(4m+2)(2m-1)+(4m+2)i}, \alpha^{t(4m+2)(2m-1)+y+(4m+2)i}\,] :\; 0 \le i \le t-1\}$$

  σχηματίζουν κωδικές λέξεις των $(n,w,2,1) - OOCs$ με $w = 4m+1$ και η πληθικότητα του κώδικα είναι $|C| = t = \frac{2(n-1)}{w^2-1} \approx 2\,\Phi(n,w,1,1)$.

Βιβλιογραφία

"Optical Code Division Multiple Access Communication Networks – Theory and Application" Hongxi Yin, David J.Richardson.

4ο Κεφάλαιο
Μεταβλητού Βάρους OOCs

Ορισμός

Ένας $(n, w, \lambda_a, \lambda_c) - OOC$ καλείται μεταβλητού βάρους OOC (variable weight OOC) όταν το βάρος w δεν είναι σταθερό.

Αυτό το κεφάλαιο επικεντρώνεται στους $OOCs$ βάρους $w = 4$ και $w = 5$.

Κυκλικοί σχεδιασμοί με block μεγέθους 4

I. Εισαγωγή

Ορισμός

Ένας σχεδιασμός διαιρούμενος σε ομάδες (group divisible design) με μέγεθος block k, δείκτη λ και ομάδα τύπου g^v (εν συντομία $(k, \lambda) - GDD$ τύπου g^v) είναι μια τριάδα $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, όπου $\mathcal{V}$ είναι ένα σύνολο με vg στοιχεία , $\mathcal{G}$ είναι μία διαμέριση του $\mathcal{V}$ σε ομάδες μεγέθους g , και $\mathcal{B}$ είναι μια συλλογή από k-υποσύνολα του $\mathcal{V}$ (blocks) με την ιδιότητα ότι κάθε block τέμνει κάθε ομάδα το πολύ σε ένα σημείο και κάθε δύο σημεία που ανήκουν σε διακεκριμένες ομάδες περιέχονται, και τα δύο, σε ακριβώς λ blocks.

Στην περίπτωση όπου, $\mathcal{G}$ είναι τετριμμένη διαμέριση με μονοσύνολα, υποστηρίζεται ότι το ζεύγος $(\mathcal{V}, \mathcal{B})$ είναι ένας $2 - (v, k, \lambda)$ σχεδιασμός ή ένας $(v, k, \lambda) - BIBD$. Ένας $BIBD$ με $\lambda = 1$ είναι ένας $2^{ος}$ - σχεδιασμός Steiner .

Ορισμός

Ένας GDD ή $BIBD$ λέγεται ότι είναι κυκλικός σχεδιασμός, όταν υπάρχει $\sigma \in Sym(\mathcal{V})$ τάξης gv διατηρώντας $\mathcal{B}$.

Ένα χρήσιμο εργαλείο για τη δημιουργία κυκλικών $GDDs$ είναι η έννοια της σχετικής οικογένειας διαφορών (relative difference family). Η έννοια αυτή εισήχθη επίσημα στο [1] και φυσικά, γενικεύει τη γνωστή έννοια του σχετικού συνόλου διαφορών (relative difference set).

Ορισμός

Ένα (vg, g, k, λ) σχετικό σύνολο διαφορών είναι ένα k-υποσύνολο του B στο $\mathbb{Z}_{gv}$ με την ιδιότητα ότι οι λίστες διαφορών $\Delta B = \{x - y \mid x, y \in B, x \neq y\}$ δεν έχουν κανένα στοιχείο στο $v\mathbb{Z}_{gv}$ ενώ, κάθε στοιχείο του $\mathbb{Z}_{gv} - v\mathbb{Z}_{gv}$ εμπεριέχεται ακριβώς λ φορές.

Γενικότερα, μία (vg, g, k, λ) σχετική οικογένεια διαφορών (εν συντομία $(vg, g, k, \lambda) - DF$) είναι μία οικογένεια $\mathcal{F}$, k-υποσυνόλων (blocks βάσης) στο $\mathbb{Z}_{gv}$ με την ιδιότητα ότι οι λίστες διαφορών $\Delta\mathcal{F} = \cup_{B\in\mathcal{F}} \Delta B$ υπάρχουν λ φορές στο $\mathbb{Z}_{gv} - v\mathbb{Z}_{gv}$.

Μια τέτοια DF παράγει έναν κυκλικό $(k, \lambda) - GDD$, τύπου g^v $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ με σημείο-σύνολο $\mathcal{V} = \mathbb{Z}_{gv}$, ομάδα-σύνολο $\mathcal{G} = \{v\mathbb{Z}_{gv} + i \mid 0 \leq i < v\}$, δηλαδή το σύνολο των συμπλόκων του $v\mathbb{Z}_{gv}$ στο $\mathbb{Z}_{gv}$, και block-πολυσύνολο $\mathcal{B} = \{B + t \mid B \in \mathcal{F}, t \in \mathbb{Z}_{gv}\}$, (το ανάπτυγμα της $\mathcal{F}$).

Η ειδική περίπτωση όπου $g = 1$ υποδηλώνει μία $(v, k, \lambda) - DF$.

Ορισμός

Μία $(gv, g, k, 1) - DF$ ονομάζεται επίσης g - κανονική κυκλική ομαδοποίηση (regular cyclic packing) $CP(1, k; gv)$.

Η ύπαρξη ενός κυκλικού $(v, k, 1) - BIBD$ είναι απολύτως ισοδύναμη με την ύπαρξη μιας $(gv, g, k, 1) - DF$ με $g = 1$ ή $g = k$.

Υπάρχει μια πολύ εκτεταμένη βιβλιογραφία, στο [2], σχετικά με κυκλικούς $BIBDs$ με ιδιαίτερη προσοχή στον κυκλικό 2^o -σχεδιασμό Steiner.

Σε γενικές γραμμές, για συγκεκριμένα k και λ, ένα πολύ δύσκολο πρόβλημα είναι να καθοριστεί το φάσμα των τιμών του v για τις οποίες υπάρχει ο κυκλικός $(v, k, \lambda) - BIBD$. Βέβαια, έχει επιλυθεί για $k = 3$ $και$ $\lambda = 1$ από τον Peltesohn στο [3], και για $k = 3$ $και$ $\lambda > 1$ από τον Colbourn στο [4],όπως και για απλούς και αδιάσπαστους κυκλικούς $(v, 3, 2) - BIBDs$ στο [5]. Πολλά άρθρα, έχουν επεξεργαστεί το ζεύγος $(k, \lambda) = (4, 1)$, όπως και κατασκευές κυκλικών $(v, 4, 1) - BIBDs$. Είναι λογικό να πιστεύεται, ότι υπάρχει ένας κυκλικός $(v, 4, 1) - BIBD$ για κάθε παραδεκτή τιμή $v \geq 37$, αλλά μια απόδειξη δεν είναι ακόμη εφικτή.

Οι σχετικές οικογένειες διαφορών με $\lambda = 1$ είναι στενά συνδεδεμένες με την έννοια του οπτικού ορθογώνιου κώδικα. Η έννοια αυτή, καθιερώθηκε και έχει πολλές σημαντικές εφαρμογές. Μια γενικότερη αναφορά γίνεται στο [4]. Συγκεκριμένα, ένας $(v, k, 1)$ οπτικός ορθογώνιος κώδικας (OOC) είναι ένα σύνολο $X, (0, 1)$ - ακολουθιών (κωδικές λέξεις) μήκους v και βάρους k που ικανοποιεί την ακόλουθη ιδιότητα (όπου όλοι οι δείκτες μειώνονται κατά $mod\ v$):

$$\sum_{i=0}^{v-1} x_i y_{i+t} = 0 \text{ ή } 1 \text{ ή } k\,, \qquad \forall (x, y, t) \in X \times X \times \mathbb{Z}_v$$

Εξακριβώνεται ότι, οποιασδήποτε κωδική λέξη $x \in X$ με υποσύνολο στο $\mathbb{Z}_v$ έχει χαρακτηριστική συνάρτηση x και ένας $(v, k, 1) - OOC$ μπορεί πιο εύκολα να αντιμετωπιστεί ως ένα σύνολο $\mathcal{F}$ k-υποσύνολων του $\mathbb{Z}_v$ (σύνολα κωδικής λέξης) με την ιδιότητα ότι $\Delta\mathcal{F}$ δεν περιλαμβάνει επαναλαμβανόμενα στοιχεία.

Ένα κοινότυπο αριθμήσιμο επιχείρημα δείχνει ότι το μέγεθος ενός $(v, k, 1) - OOC$ δεν μπορεί να υπερβεί το $\left\lfloor \frac{v-1}{k\,(k-1)} \right\rfloor$. Ένας OOC λέγεται ότι είναι βέλτιστος όταν το μέγεθός του φτάνει αυτό το όριο. Συγκεκριμένα, λέγεται ότι ένας OOC είναι τέλειος, όταν το μέγεθός του είναι ακριβώς ίσο με $\frac{v-1}{k\,(k-1)}$.

Είναι σαφές ότι μία $(gv, g, k, 1) - DF$ είναι επίσης ένας βέλτιστος $(gv, k, 1) - OCC$ όταν $g \leq k\,(k-1)$ και τέλεια όταν $g = 1$. Άρα, ένας τέλειος $(v, k, 1) - OOC$ είναι ισοδύναμος με μία $(v, k, 1) - DF$.

Η ενότητα αυτή πραγματεύεται κυκλικούς $(4, 1) - GDDs$ που προκύπτουν από $(gv, g, 4, 1) - DF$. Ασχολείται επίσης με: (a) μια σαφή κατασκευή της $(4p,\ 4, 4,\ 1) - DF$ για οποιαδήποτε πρώτο $p \equiv 1\ (mod\ 12)$ (δηλαδή, για $p \equiv 1\ (mod\ 24)$), (b) μια (μη σαφή) κατασκευή για τη $(4p,\ 4, 4,\ 1) - DF$ για οποιαδήποτε πρώτο $p \equiv 7\ (mod\ 12)$ υπό την προϋπόθεση ότι ο λόγος $\frac{(p-1)}{6}$ έχει έναν πρώτο παράγοντα όχι μεγαλύτερο από 19, (c) μια εύκολη κατασκευή της $(6p,\ 6, 4,\ 1) - DF$ για οποιαδήποτε πρώτο $p > 5$ και (d) μια σαφή κατασκευή της $(8p,\ 8,\ 4,\ 1) - DF$ για οποιαδήποτε πρώτο $p \equiv 1\ (mod\ 6)$.

Κατασκευές για $(gp, g, 4, 1) - DF$ με p πρώτο, είναι γνωστές για τις ακόλουθες περιπτώσεις:

i. $g = 1\ και\ p \equiv 1\ (mod\ 12)$
ii. $g = 2\ και\ p \equiv 1\ (mod\ 6)$
iii. $g = 3\ και\ p \equiv 1\ (mod\ 4)$
iv. $g = 4\ και\ p \equiv 1\ (mod\ 12)$
v. $g = 6\ και\ p > 5$
vi. $g = 9\ και\ 5 < p \equiv 1\ (mod\ 4)$
vii. $g = 12\ και\ 5 < p \equiv 1\ (mod\ 4)$

Οι κατασκευές δεν είναι σαφείς στις περιπτώσεις (i), (iv) εάν $p \equiv 1\ (mod\ 24)$, και στην περίπτωση (vi) εάν $p \not\equiv 13\ (mod\ 24)$.

Σημειώνεται ότι, αν $p \equiv 1\ (mod\ 6)$ είναι πρώτος, τότε υπάρχει $p \equiv 1$ ή $7 (mod\ 12)$ σύμφωνα με το εάν ο λόγος $\frac{(p-1)}{6}$ είναι ζυγός ή περιττός αντίστοιχα. Έτσι, τα (a) και (b) δίνουν μια $(4p,\ 4, 4, 1) - DF$, (και συνεπώς έναν κυκλικό $(4p, 4, 1) - BIBD$) για οποιοδήποτε πρώτο $p \equiv 1\ (mod\ 6)$ τέτοιο ώστε ο λόγος $\frac{(p-1)}{6}$ να είναι πρώτος παράγοντας και όχι μεγαλύτερος από 19.

Δίνεται επίσης, μια πολύ ισχυρή ένδειξη για την ύπαρξη του κυκλικού $(4p, 4, 1) - BIBD$ για οποιαδήποτε πρώτο $p \equiv 1\,(mod\,6)$. Έχει αποδειχθεί, ότι ένας τέτοιος $BIBD$ υπάρχει όταν ο p είναι αρκετά μεγάλος, λαμβάνοντας υπόψιν το μικρότερο πρώτο παράγοντα του $\frac{(p-1)}{6}$.

Το αποτέλεσμα του (b) επιτυγχάνεται με τη χρήση του Θεωρήματος του Weil για πολλαπλασιαστικό χαρακτήρα αθροισμάτων, που αναφέρεται στη συνέχεια.

Ο πολλαπλασιαστικός χαρακτήρας του $\mathbb{Z}_p$, όπου p πρώτος, είναι μία απεικόνιση:

$$\chi: \mathbb{Z}_p \to \{z \in C: |\, z \,| = 1 \text{ ή } 0\}$$

τέτοιος ώστε $\chi(0) = 0, \chi(1) = 1$ και με την ιδιότητα ότι $\chi(xy) = \chi(x)\,\chi(y)$ για κάθε $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Θεώρημα 1.1 (Θεώρημα του Weil)

Έστω χ ένας χαρακτήρας τάξης $m > 1$ του πεπερασμένου σώματος $\mathbb{Z}_p$.

Έστω $f \in \mathbb{Z}_p[\mathrm{x}]$ με $f \neq kg^m$ για κάθε $(k, g) \in \mathbb{Z}_p \times \mathbb{Z}_p[x]$. Τότε ισχύει:

$$\left| \sum_{x \in \mathbb{Z}_p} \chi[f(x)] \right| \leq (d-1)\sqrt{p}$$

όπου d είναι ο αριθμός των διακεκριμένων ριζών της f στο σώμα ριζών του $\mathbb{Z}_p$.

Το παραπάνω θεώρημα έχει μεγάλη σημασία για πολλές κατασκευές συνδυαστικών σχεδιασμών.

Σε όλη την ενότητα, χρησιμοποιείται σταθερός πρώτος $p \equiv 1\,(mod\,n)$ και ένα αρχικό στοιχείο $\omega \in \mathbb{Z}_p$, ως C^n θα συμβολίζεται η ομάδα $\{\omega^{in} \mid 0 \leq i \leq \frac{(p-1)}{n}\}$ n-οστης δύναμης $(mod\ p)$, ενώ ως C_j^n θα συμβολίζεται το σύμπλοκο C^n στο $\mathbb{Z}_p^*(= C^1)$, αντιπροσωπευμένο από το ω^j, δηλαδή $C_j^n = \omega^j C^n$.

Αν p είναι πρώτος $\equiv 1\,(mod\,mn)$, με τη φράση «το S είναι εγκάρσιο στο $\frac{C^n}{C^{mn}}$» εννοείται ότι, το S είναι ένα πλήρες σύστημα αντιπροσώπων για σύμπλοκα του C^{mn} στο C^n.

Κάθε φορά που κατασκευάζεται μία $(gp, g, 4, 1) - DF$ με $M.K.\Delta.(g, p) = 1$, γίνεται ταυτοποίηση του $\mathbb{Z}_{gp}$ με την ισομορφική ομάδα $\mathbb{Z}_g \times \mathbb{Z}_p$. Με τον τρόπο αυτό μία $(gp, g, 4, 1) - DF$ αντιμετωπίζεται ως ένα σύνολο $\mathcal{F}$ από 4 - υποσύνολα του $\mathbb{Z}_g \oplus \mathbb{Z}_p$ τέτοια ώστε $\Delta\mathcal{F} = (\mathbb{Z}_g \oplus \mathbb{Z}_p) - (\mathbb{Z}_g \oplus \{0\})$.

Οποιαδήποτε $(gp, g, 4, 1) - DF$ θα πραγματοποιηθεί με τη σιωπηρή χρήση μιας $(g, 4, \lambda) - DF$ ισχυρής οικογένειας διαφορών – strong difference family (SDF). Πρόκειται για μια οικογένεια $\mathcal{S}$ πολλών συμπλόκων μεγέθους 4 του $\mathbb{Z}_g$ έτσι ώστε κάθε στοιχείο του $\mathbb{Z}_g$ να εμφανίζεται ακριβώς λ φορές στη $\Delta\mathcal{S}$.

II. Ρητές Κατασκευές για $(4p, 4, 1) - BIBD$ με πρώτο $p \equiv 1\ (mod\ 12)$

Είναι δυνατόν να επεκταθεί οποιοσδήποτε κυκλικός $(p, k, 1) - BIBD$, σ' έναν κυκλικό $(kp, k, 1) - BIBD$, αν p πρώτος, σύμφωνα με το [6]. Αυτό συνεπάγει την ύπαρξη ενός $(4p, 4, 1) - BIBD$ για οποιονδήποτε πρώτο $p \equiv 1\ (mod\ 12)$ δεδομένου ότι, για κάθε έναν από αυτούς τους πρώτους αριθμούς υπάρχει ένας κυκλικός $(p, 4, 1) - BIBD$.

Στην παράγραφο αυτή, παρουσιάζεται μια ρητή κατασκευή της $(4p, 4, 4, 1) - DF$, και συνεπώς ενός κυκλικού $(4p, 4, 1) - BIBD$, για οποιονδήποτε πρώτο $p \equiv 1\ (mod\ 12)$.

<u>1η Περίπτωση:</u> $p \equiv 13\ (mod\ 24)$.

Στην περίπτωση αυτή $3 \in C^4$.

Αν $p = 13$, ένα παράδειγμα ενός κυκλικού $(4p, 4, 1) - BIBD$ είναι αυτός που παράγεται από την ακόλουθη $(52, 4, 4, 1) - DF$:

$$\{\{0, 1, 22, 47\}, \{0, 2, 9, 19\}, \{0, 3, 18, 41\}, \{0, 4, 20, 44\}\}$$

Τώρα, έστω $p = 24n + 13$ είναι πρώτος με $n > 0$ και έστω $(\alpha, b, c) \in \mathbb{Z}_p^3$ ορίζεται ως εξής:

$$(\alpha, b, c) = \begin{cases} (-2, 7, 2) & \alpha\nu\ 3 \in C^2 - C^4\ \kappa\alpha\iota\ 7 \in C^4 \\ \left(\frac{1}{2}, \frac{9}{25}, 2\right) & \alpha\nu\ 3 \in C^2 - C^4\ \kappa\alpha\iota\ 7 \notin C^4 \\ (2, -7, 2) & \alpha\nu\ 3, 7 \in C^2 - C^4 \\ (-1, -9, 1) & \alpha\nu\ 3, 5 \in C^4 \\ (-5, 25, 1) & \alpha\nu\ 3 \in C^4\ \kappa\alpha\iota\ 5 \in C^2 - C^4 \\ (-1, 5, 1) & \alpha\nu\ 3, 10 \in C^4\ \kappa\alpha\iota\ 5 \notin C^2 \\ (2, -24, 1) & \alpha\nu\ 3, \frac{5}{2} \in C^4, 5 \notin C^2\ \ \kappa\alpha\iota\ 13 \in C^2 \\ (-5, 8, 1) & \alpha\nu\ 3, \frac{5}{2} \in C^4, 5 \notin C^2\ \kappa\alpha\iota\ 13 \notin C^2 \end{cases}$$

Έστω ε είναι κυβική (τρίτη) αρχική ρίζα $(mod\ p)$, και εξετάζοντας τα ακόλουθα υποσύνολα του $\mathbb{Z}_4 \oplus \mathbb{Z}_p$:

$$B_i = \{(0,0), (0, \varepsilon^i), (1, a\varepsilon^i), (3, b\varepsilon^i)\}\ i = 0, 1, 2$$
$$B_3 = \{(0,0), (2, c), (2, c\varepsilon), (2, c\varepsilon^2)\}$$

ισχύει

$$\bigcup_{i=0}^{3} \Delta B_i = \bigcup_{\iota=0}^{3} \{i\} \times L_i\langle\varepsilon\rangle$$

όπου
$L_0 = \{\pm 1, \pm c(\varepsilon - 1)\}, L_1 = \{\alpha, \alpha - 1, -b, -b + 1\}, L_2 = \{\pm c, \pm(a - b)\}$ $\kappa\alpha\iota$ $L_3 = -L_1$.

Χρησιμοποιώντας στοιχειώδη θεωρία αριθμών μπορεί να αποδειχθεί σε οποιαδήποτε περίπτωση ότι, κάθε L_i είναι εγκάρσιο στο $\mathbb{Z}_p^*/C^4$, εάν S είναι εγκάρσιο στο $C^4/\langle\varepsilon\rangle$, και τότε θα ισχύει $L_i\langle\varepsilon\rangle S = \mathbb{Z}_p^*$ για κάθε i. Επομένως,

$$\mathcal{F} = \{B_i \cdot (1, s) | 0 \le i \le 3; s \in S\}$$

είναι $(4p, 4, 4, 1) - DF$.

<u>2η Περίπτωση</u>: $p \equiv (mod\ 24)$ $\kappa\alpha\iota$ $3 \in C^4$

Έστω x ένας αριθμός που δεν είναι τέλειο τετράγωνο, τέτοιος ώστε ο $x^2 - 1$ να μην είναι επίσης τέλειο τετράγωνο. Ένα τέτοιο x μπορεί να βρεθεί με τον ακόλουθο τρόπο. Έστω y και $y + 1$ δύο συνεχόμενοι αριθμοί, που δεν είναι τέλεια τετράγωνα στο $\mathbb{Z}_p$.

Έστω z ο μικρότερος ακέραιος του $\{y + 2, y + 3, \dots, p - 1\}$, τέτοιος ώστε z να είναι ένα τέλειο τετράγωνο $(mod\ p)$. Είναι προφανές ότι, $x = z - 1$ πληροί τις απαιτούμενες συνθήκες.

Τώρα, έστω ε είναι μία κυβική αρχική ρίζα $(mod\ p)$, και εξετάζοντας τα ακόλουθα υποσύνολα του $\mathbb{Z}_4 \oplus \mathbb{Z}_p$:

$$B_i = \{(0, x\varepsilon^i), (0, -x\varepsilon^i), (1,0), (2, \varepsilon^i)\} \quad i = 0, 1, 2$$
$$B_3 = \{(0,1), (0, \varepsilon), (0, \varepsilon^2), (1,0)\}$$

ισχύει

$$\bigcup_{i=0}^{3} \Delta B_i = \bigcup_{\iota=0}^{3} \{i\} \times L_i\langle-\varepsilon\rangle$$

όπου
$L_0 = \{\varepsilon - 1, 2x\}$, $L_1 = L_3 = \{1, x\}$ $\kappa\alpha\iota$ $L_2 = \{x - 1, x + 1\}$.

Η υπόθεση ότι $3 \in C^4$ σημαίνει ότι $\varepsilon - 1$ είναι τέλειο τετράγωνο $(mod\ p)$, λαμβάνοντας υπόψιν την ταυτότητα $(\varepsilon - 1)^2 = -3\varepsilon$. Τότε, εφόσον, το 2 είναι επίσης τέλειο τετράγωνο, κάθε L_i θα περιέχει έναν αριθμό τέλειο τετράγωνο και έναν μη τέλειο τετράγωνο. Έτσι, εάν S είναι εγκάρσιο στο $C^2/\langle-\varepsilon\rangle$, τότε θα ισχύει ότι $L_i\langle-\varepsilon\rangle S = \mathbb{Z}_p^*$ για κάθε i. Επομένως,

$$\mathcal{F} = \{B_i \cdot (1, s) | 0 \le i \le 3; s \in S\}$$

είναι $(4p, 4, 4, 1) - DF$.

3η Περίπτωση: $p \equiv 1\ (mod\ 24)$ *και* $3 \notin C^4$

Για την επίλυση αυτής της περίπτωσης, αρκεί να συνδυαστεί η κατασκευή του Bose [6α] για κυκλικούς $(p, 4, 1) - BIBD$ με το «μείγμα» κατασκευών που δίνεται στο [6β].

Συμβολίζονται: με φ μια αρχική 4η ρίζα της μονάδας, με ε μια αρχική κυβική ρίζα της μονάδα, με S ένα εγκάρσιο σύνολο στο $C^2/\langle -\varepsilon \rangle$, και με T ένα εγκάρσιο σύνολο στο $\mathbb{Z}_p^*/\langle \varphi \rangle$.

Ισχύει ότι

$$\mathcal{F} = \{\{(0,0),(0,s),(0,\varepsilon s),(0,\varepsilon^2 s)\}|s \in S\} \cup \{\{(0,t),(1,\varphi t),(2,-t),(3,-\varphi t)\}\big|t \in T\}$$

είναι $(4p, 4, 4, 1) - DF$.

III. Κυκλικοί $(4p, 4, 1) - BIBD$ με p πρώτο $\equiv 7\ (mod\ 12)$

Σε αυτήν την παράγραφο αναφέρεται το εξής πρόβλημα.

Ερώτηση:

Για ποιους πρώτους $p \equiv 7\ (mod\ 12)$ υπάρχει ένας κυκλικός $(4p, 4,1) - BIBD$;

Είναι γνωστό ότι ένας τέτοιος $BIBD$ σχεδιασμός δεν υπάρχει για $p = 7$. Ένας πολύ απλός τρόπος για να δειχθεί αυτός ο ισχυρισμός είναι ο ακόλουθος. Εάν υπάρχει ο κυκλικός $(28, 4, 1) - BIBD$, αυτός θα παράγεται από την $(28, 4, 4, 1) - DF$. Η μείωση $(mod\ 4)$ δύο blocks μιας τέτοιας DF θα δώσει $(4,4,6) - SDF$. Είναι σχεδόν άμεσο ότι μια τέτοια SDF δεν υπάρχει.

Παρόλα αυτά, είναι λογική η εικασία ότι ένας κυκλικός $(4p, 4, 1) - BIBD$ υπάρχει για κάθε πρώτο $p \equiv 7\ (mod\ 12)$ μεγαλύτερο από 7.

Αν και δεν είναι εφικτό να αποδειχθεί η εικασία αυτή , θα δοθεί μια πολύ ισχυρή ένδειξη για την ορθότητά της.

Ειδικότερα, θα αποδειχθεί η ύπαρξη ενός κυκλικού $(4p, 4, 1) - BIBD$ για οποιονδήποτε πρώτο $p \equiv 7\ (mod\ 12)$ τέτοιο ώστε ο λόγος $\frac{(p-1)}{6}$ να έχει ένα πρώτο παράγοντα όχι μεγαλύτερο από 19. Η απόδειξη βασίζεται στην ακόλουθη εφαρμογή του Θεωρήματος του Weil.

Θεώρημα 3.1

Έστω p πρώτος $\equiv 1\ (mod\ q)$ με $p > (2q^3 - 3q^2 + 1)^2 + 3q^2$. Τότε, για οποιαδήποτε δοσμένη τριάδα $(j_1, j_2, j_3) \in \{0, 1, \dots, q-1\}^3$ και οποιαδήποτε δοσμένη τριάδα (c_1, c_2, c_3) του $\mathbb{Z}_p$, θα υπάρχει ένα στοιχείο $x \in \mathbb{Z}_p$ τέτοιο ώστε $x + c_i \in C_{j_i}^q$ για κάθε i.

Απόδειξη:

Για $i = 1, 2, 3$ ορίζεται ένα στοιχείο $a_i \in C^q_{-j_i}$ και ένα σύνολο $b_i = a_i c_i$. Με αυτόν τον τρόπο, το άθροισμα $x + c_i \in C^q_{j_i}$ είναι ισοδύναμο με το $a_i x + b_i \in C^q$.

Έτσι, αποδεικνύεται ότι το σύνολο

$$A = \{x \in \mathbb{Z}_p \mid a_i x + b_i \in C^q \ \gamma\iota\alpha \ i = 1, 2, 3\}$$

δεν είναι κενό.

Για $i = 1, 2, 3$ έστω $f_i \in \mathbb{Z}_p[x]$ που ορίζεται ως $f_i = a_i x + b_i$.

Έστω χ ένας πολλαπλασιαστικός χαρακτήρας τάξης q του $\mathbb{Z}_p$, και έστω το άθροισμα

$$S = \sum_{x \in \mathbb{Z}_p} \prod_{i=1}^{3} \left[1 + \chi(f_i(x)) + \chi\left({f_i}^2(x)\right) + \cdots + \chi\left({f_i}^{q-1}(x)\right)\right]$$

Για $i = 1, 2, 3$ ισχύει:

$$1 + \chi(f_i(x)) + \chi\left({f_i}^2(x)\right) + \cdots + \chi\left({f_i}^{q-1}(x)\right) = \begin{cases} q & \alpha\nu \ f_i(x) \in C^q \\ 0 & \alpha\nu \ f_i(x) \in \mathbb{Z}_p^* - C^q \\ 1 & \alpha\nu \ x = -\dfrac{b_i}{a_i} \end{cases}$$

Αυτό εύκολα σημαίνει ότι $q^3|A| \le S \le q^3|A| + 3q^2$.

Από την άλλη πλευρά ισχύει ότι

$$S = \sum_{(e_1,e_2,e_3)} \sum_{x \in \mathbb{Z}_p} \chi[f_1^{e_1} \ f_2^{e_2} \ f_3^{e_3}(x)]$$

όπου (e_1, e_2, e_3) λαμβάνει τιμές στο $\{0, 1, \dots, q-1\}^3$.

Σημειώνεται ότι, αν $(e_1, e_2, e_3) \neq (0,0,0)$ τότε $f_1^{e_1} \ f_2^{e_2} \ f_3^{e_3} = kg^q$ για κανένα ζευγάρι δεν θα ισχύει ότι $(k, g) \in \mathbb{Z}_p \times \mathbb{Z}_p[\mathrm{x}]$.

Χρησιμοποιώντας το Θεώρημα 1.1, θα ισχύει:

$$\left|\sum_{x \in \mathbb{Z}_p} \chi[f_1^{e_1} \ f_2^{e_2} \ f_3^{e_3}(x)]\right| \ \begin{cases} \le 2\sqrt{p} & \alpha\nu \ e_i \neq 0 \ \forall \ i \\ \le \sqrt{p} & \alpha\nu \ e_i = 0 \ \gamma\iota\alpha \ \alpha\kappa\rho\iota\beta\acute{\omega}\varsigma \ \acute{\varepsilon}\nu\alpha \ i \\ = 0 & \alpha\nu \ e_i \neq 0 \ \gamma\iota\alpha \ \alpha\kappa\rho\iota\beta\acute{\omega}\varsigma \ \acute{\varepsilon}\nu\alpha \ i \\ = p & \alpha\nu \ e_i = 0 \ \forall \ i \end{cases}$$

Προκύπτει, λοιπόν, $|S| \ge p - (2q^3 - 3q^2 + 1)\sqrt{p}$.

Όμως, $S \le q^3|A| + 3q^2$, συνεπώς, $|A| > 0$ για $p - \left(2q^3 - 3q^2 + 1\right)\sqrt{p} - 3q^2 > 0$ και άρα $p > (2q^3 - 3q^2 + 1)^2 + 3q^2$.

Που σημαίνει ότι, ο ισχυρισμός ισχύει.

▪

Θεώρημα 3.2

Υπάρχει ο κυκλικός $(4p, 4, 1) - BIBD$ για $p \equiv 19\ (mod\ 36)$.

Απόδειξη:

Έστω p πρώτος $\equiv 19\ (mod\ 36)$ και έστω ε κυβική αρχική ρίζα $(mod\ p)$. Έστω ένα ζεύγος $(x, y) \in \mathbb{Z}_p^2$ που πληροί τις ακόλουθες προϋποθέσεις:

(1) $y \in C^6, y - 1 \notin C^3$

(2) $x - 1 \in C_1^3, x - y \in C_2^3, x(y - 1) \in C^3$

Μια εύκολη υπολογιστική έρευνα δείχνει ότι για $p < 811$, ένα τέτοιο ζεύγος (x, y) μπορεί να συμπεριλήφθη στον ακόλουθο πίνακα:

p	19	127	163	199	271	307	379	487	523	631	739
x	3	18	10	7	12	31	12	21	5	16	19
y	7	4	21	5	8	6	5	18	11	5	4

Για $p > 811 (= (2 \cdot 3^3 - 3 \cdot 3^2 + 1)^2 + 3 \cdot 3^2)$ η ύπαρξη ενός ζεύγους (x, y) που ικανοποιεί τις (1) και (2) μπορεί να αποδειχθεί ως εξής:

Με το Θεώρημα 3.1 μπορεί να βρεθεί ένα στοιχείο $z \in \mathbb{Z}_p$ τέτοιο ώστε z να είναι αριθμός 3ης δύναμης, ενώ οι $z - 1$ και $z + 1$ να μην είναι αριθμοί 3ης δύναμης.

Έστω $y = z$ ή $y = -z$ επειδή z είναι ή δεν είναι 6η δύναμη, αντίστοιχα, και εφόσον, το -1 είναι αριθμός 3ης δύναμης, αλλά όχι 6ης δύναμης, φαίνεται εύκολα ότι το y πληροί τις προϋποθέσεις (1).

Παρατηρείται επίσης ότι, στην περίπτωση όπου το -3 δεν είναι 6η δύναμη $(mod\ p)$, θα υπάρχει ένα στοιχείο y που πληροί την (1) δηλαδή το $y = \varepsilon$.

Αν το y είναι σταθερό, από το Θεώρημα 3.1, μπορεί να βρεθεί ένα στοιχείο x που να ικανοποιεί τις υπόλοιπες προϋποθέσεις του (2).

Τώρα, εξετάζοντας τα ακόλουθα υποσύνολα του $\mathbb{Z}_4 \oplus \mathbb{Z}_p$:

$$B_i = \{(0,0), (1, \varepsilon^i), (2, x\varepsilon^i), (3, y\varepsilon^i)\} \quad i = 0, 1, 2$$
$$B_3 = \{(0, x - 1), (0, x\varepsilon - \varepsilon), (0, x\varepsilon^2 - \varepsilon^2), (1,0)\}$$
$$B_4 = \{(0, y - x), (0, \varepsilon y - \varepsilon x), (0, \varepsilon^2 y - \varepsilon^2 x), (1,0)\}$$
$$B_5 = \{(0,1), (0, \varepsilon), (0, \varepsilon^2), (2,0)\}$$

ισχύει

$$\bigcup_{i=0}^{5} \Delta B_i = \bigcup_{\iota=0}^{3} \{i\} \times L_i\langle\varepsilon\rangle$$

όπου
$L_0 = \{\pm 1, \pm(x-1), \pm(y-x)\}(\varepsilon - 1), L_1 = \{1, -y, \pm(x-1), \pm(y-x)\},$

$L_2 = \{\pm 1, \pm x, \pm(y-1)\}$ $\kappa\alpha\iota$ $L_3 = -L_1.$

Λαμβάνοντας υπόψιν τις συνθήκες (1) και (2), κάθε L_i είναι εγκάρσιο στο $\mathbb{Z}_p^*/C^6$. Έτσι, εάν S είναι εγκάρσιο στο $C^6/\langle\varepsilon\rangle$, τότε θα ισχύει $L_i\langle\varepsilon\rangle S = \mathbb{Z}_p^*$ για κάθε i. Επομένως, εύκολα αποδεικνύεται ότι

$$\mathcal{F} = \{B_i \cdot (1, s) \mid 0 \le i \le 5; s \in S\}$$

είναι $(4p, 4, 4, 1) - DF$.

▪

Τώρα, έχουν μελετηθεί πρώτοι $p \equiv 1\,(mod\,6)$ έτσι ώστε ο μικρότερος πρώτος παράγοντας του λόγου $\frac{(p-1)}{6}$ να είναι μεγαλύτερος από 3.

Κατασκευή Α

Έστω p $\pi\rho\acute{\omega}\tau o\varsigma \equiv 1\,(mod\,6)$ και έστω $q = 2n + 1$ είναι πρώτος παράγοντας του $\frac{(p-1)}{6}$ μεγαλύτερος από 3.

Έστω

$$L = \{\alpha_i, b_i \mid 1 \le i \le n-1\} \cup \{c, d, e, f\} \cup \{g_i \mid 1 \le i \le n-2\}$$

είναι μια λίστα με στοιχεία στο $\mathbb{Z}_p$, έτσι ώστε κάθε μία από τις ακόλουθες q - λίστες

$L_0 = \{g_i\,, g_i\,(\varepsilon - 1) | 1 \le i \le n-2\} \cup \{c(\varepsilon-1), d(\varepsilon-1), e(\varepsilon-1), c-d, f(\varepsilon-1)\}$
$L_1 = \{\alpha_i, b_i \mid 1 \le i \le n-1\} \cup \{c, d, e\}$
$L_2 = \{\alpha_i + b_i\,, \alpha_i - b_i \mid 1 \le i \le n-1\} \cup \{c-e, d-e, f\}$

να είναι εγκάρσιες στο $\mathbb{Z}_p^*/C^q$.

Έστω $\mathcal{F}_0$ η οικογένεια που αποτελείται από τα ακόλουθα 4 - υποσύνολα του $\mathbb{Z}_4 \oplus \mathbb{Z}_p$:

$\{(0,0), (1, \alpha_i\varepsilon^j), (2, \alpha_i\varepsilon^j + b_i\varepsilon^j), (3, b_i\varepsilon^j)\}, i = 1, \dots, n-1; j = 0, 1, 2$
$\{(0,0), (1, c), (1, c\varepsilon), (1, c\varepsilon^2)\}$
$\{(0,0), (1, d), (1, d\varepsilon), (1, d\varepsilon^2)\}$
$\{(0, e), (1, e\varepsilon), (1, e\varepsilon^2), (1,0)\}$
$\{(0, c\varepsilon^j), (0, d\varepsilon^j), (1,0), (2, e\varepsilon^j)\}, j = 0, 1, 2$
$\{(0,0), (0, g_i\,), (0, g_i\,\varepsilon), (0, g_i\,\varepsilon^2)\}, i = 1, \dots, n-2$
$\{(0, f), (0, f\varepsilon), (0, f\varepsilon^2), (2,0)\}$

ισχύει

$$\Delta\mathcal{F}_0 = \bigcup_{i=0}^{3} \{i\} \times L_i\langle -\varepsilon\rangle$$

όπου
$\langle -\varepsilon \rangle = \{\pm 1, \pm\varepsilon, \pm\varepsilon^2\}$ είναι η ομάδα της 6ης ρίζας της μονάδας και $L_3 = L_1$.

Έστω S εγκάρσιο στο $C^6/\langle -\varepsilon \rangle$, και έστω ότι κάθε L_i είναι εγκάρσιο στο $\mathbb{Z}_p^*/C^q$, τότε θα ισχύει $L_i\langle -\varepsilon \rangle S = \mathbb{Z}_p^*$ για κάθε i, έτσι ώστε

$$\mathcal{F} = \{B \cdot (1, s) \,|B \in \mathcal{F}_0 \,; s \in S\}$$

είναι $(4p, 4, 4, 1) - DF$.

▪

Παράδειγμα

Έστω $p = 43$ και $q = 7$. Να ελεγχθεί αν η Κατασκευή Α μπορεί να υλοποιηθεί χρησιμοποιώντας την ακόλουθη λίστα L:

$$L = (a_1, a_2, b_1, b_2, c, d, e, f, g_1) = (4, 5, 20, 16, 1, 2, 3, 5, 9)$$

Χρησιμοποιώντας τον ισόμορφο δακτύλιο

$$\psi : (\alpha, \beta) \in \mathbb{Z}_4 \oplus \mathbb{Z}_{43} \rightarrow 44b - 43\alpha \in \mathbb{Z}_{172} ,$$

μπορεί κανείς να δει ότι η αντιπροσωπευτική $(172, 4, 4, 1) - DF$ έχει τα ακόλουθα blocks βάσης:

{0, 133, 110, 63}	{0, 153, 58, 163}	{0, 101, 90, 75}	{0, 5, 150, 59}
{0, 73, 126, 139}	{0, 137, 154, 103}	{0, 1, 49, 165}	{0, 45, 141, 29}
{132, 104, 108, 129}	{44, 88, 129, 46}	{92, 12, 129, 18}	{36, 72, 129, 22}
	{0, 52, 140, 152}	{48, 116, 8, 86}	

Για $p = 463$ και $q = 7$ μια "καλή" λίστα για την εφαρμογή της Κατασκευής Α είναι:

$$L = (a_1, a_2, b_1, b_2, c, d, e, f, g_1) = (8, 24, 17, 27, 1, 2, 3, 8, 9) .$$

Κατασκευή Β

Έστω p πρώτος $\equiv 1 \,(mod\, 6)$ και έστω $q = 2n + 1$ είναι πρώτος παράγοντας του $\frac{(p-1)}{6}$ μεγαλύτερος από 3.

Έστω

$$L = \{\alpha_i, b_i \,|i = 1, 2, \dots \,, n - 2\} \cup \{c, d, e, f, g\}$$

είναι μία q - λίστα με στοιχεία στο $\mathbb{Z}_p$ τέτοια ώστε, κάθε μία από τις ακόλουθες q - λίστες να είναι εγκάρσιες στο $\mathbb{Z}_p^*/C^q$:

$$L_0 = \{\alpha_i(\varepsilon - 1) | i = 1, 2, \dots, n - 2\} \cup (2b_i \,|i = 1, \dots, n - 2\}$$
$$\cup \{c - d, c(\varepsilon - 1), d(\varepsilon - 1), e(\varepsilon - 1), (\varepsilon - 1)\}$$

$L_1 = L$
$L_2 = \{\alpha_i - b_i, \alpha_i + b_i | i = 1, \dots, n-2\} \cup \{c-e, d-e, f+g, f-g, 1\}$

Για μία οικογένεια $\mathcal{F}_0$ που αποτελείται από τα ακόλουθα 4 - υποσύνολα του $\mathbb{Z}_4 \oplus \mathbb{Z}_p$:

$\{(0,\alpha_i), (0,\alpha_i\varepsilon), (0,\alpha_i\varepsilon^2), (1,0)\}\ i = 1, \dots, n-2$
$\{(0, b_i\varepsilon^j), (0, -b_i\varepsilon^j), (1,0), (2, \alpha_i\varepsilon^j)\}\ i = 1, \dots, n-2;\quad j = 0,1,2$
$\{(0,0), (1,c), (1,c\varepsilon), (1,c\varepsilon^2)\}$
$\{(0,0), (1,d), (1,d\varepsilon), (1,d\varepsilon^2)\}$
$\{(0,e), (0,e\varepsilon), (0,e\varepsilon^2), (1,0)\}$
$\{(0, c\varepsilon^j), (0, d\varepsilon^j), (1,0), (2, e\varepsilon^j)\},\ j = 0,1,2$
$\{(0,0), (1, f\varepsilon^j), (2, f\varepsilon^j + g\varepsilon^j), (3, g\varepsilon^j)\}, j = 0,1,2$
$\{(0,1), (0,\varepsilon), (0,\varepsilon^2), (2,0)\}$

ισχύει

$$\Delta\mathcal{F}_0 = \bigcup_{\iota=0}^{3} \{i\} \times L_i\langle -\varepsilon \rangle$$

όπου $\langle -\varepsilon \rangle = \{\pm 1, \pm\varepsilon, \pm\varepsilon^2\}$ είναι η ομάδα $6^{\eta\varsigma}$ ρίζας της μονάδας και $L_3 = L_1$.

Αν S εγκάρσιο στο $C^q/\langle -\varepsilon \rangle$, τότε θα ισχύει ότι

$$\mathcal{F} = \{B \cdot (1,s)\ | B \in \mathcal{F}_0\ ; s \in S\}$$

είναι $(4p, 4, 4, 1) - DF$.

▪

Για σταθερό πρώτο q που διαιρεί το $\frac{(p-1)}{6}$, θα παρουσιαστεί ένας απλός τρόπος για να εφαρμοστούν οι παραπάνω κατασκευές.

<u>1η Περίπτωση</u>: $\varepsilon - 1 \notin C^q$ ή/και $q = 5$

Στην περίπτωση αυτή, η Κατασκευή Α μπορεί να πραγματοποιηθεί αμέσως μόλις βρεθεί ένα στοιχείο $x \in \mathbb{Z}_p$ τέτοιο ώστε

(3) $\left\{x-1, \frac{x}{\varepsilon-1}, (x+1)(\varepsilon-1)\right\} \subset C^q$

Στην πραγματικότητα, εάν ισχύει η (3), τότε η Κατασκευή Α λειτουργεί χρησιμοποιώντας ως L την ακόλουθη λίστα που ορίζεται ως εξής:

$(\alpha_i, b_i) = \left(x^{2i-2}, x^{2i-1}\right), i = 1, 2, \dots, n-1$

$(c,d,e,f) = (x^{-3}, x^{-1}, x^{-2}, x^{-4}), g_i = x^{2i-1}, i = 1, 2, \dots, n-2$

2η Περίπτωση: $\varepsilon - 1 \in C^q \ \ και \ \ 2 \notin C^q$

Στην περίπτωση αυτή, η Κατασκευή Α δεν μπορεί να πραγματοποιηθεί εάν $q > 5$ δεδομένου ότι η λίστα L_0 θα περιέχει ζεύγη των στοιχείων $(g_i \, και \, g_i \, (\varepsilon - 1),$ $i = 1, 2, \ldots, n-2)$ που αντιπροσωπεύουν το ίδιο σύμπλοκο του C^q.

Από την άλλη πλευρά, η Κατασκευή Β μπορεί να υλοποιηθεί με το που βρεθεί ένα ζευγάρι $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ το οποίο θα πληροί τις ακόλουθες προϋποθέσεις:

$$(4) \ \left\{2x^2, \frac{(x-1)^2}{2}, x+1\right\} \subset C^q \, , \left\{2y^2, \frac{(y-1)^2}{2}, \frac{y+1}{2}\right\} \subset C^q$$

Στην πραγματικότητα, εάν ισχύει η (4), τότε η Κατασκευή Β λειτουργεί χρησιμοποιώντας ως L την ακόλουθη λίστα που ορίζεται ως εξής:

$(\alpha_i, b_i) = \left(x^{2i}, x^{2i+1}\right), i = 1, 2, \ldots, n-2$

$(c, d, e, f, g) = (x^{-3}, x^{-2}, x^{-1}, 1, y)$

3η Περίπτωση: $\varepsilon - 1 \in C^q \ \ και \ \ 2 \in C^q$

Επίσης, εδώ, η Κατασκευή Α δεν λειτουργεί ποτέ για $q > 5$. Από την άλλη πλευρά, η Κατασκευή Β μπορεί να πραγματοποιηθεί μόλις βρεθεί ένα ζευγάρι $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ που πληροί τις ακόλουθες προϋποθέσεις:

$$(5) \ x \notin C^q, \left\{\frac{x^4}{x-1}, \frac{x^3}{x+1}, \frac{x}{y}, \frac{x^2}{y-1}, \frac{x}{y+1}\right\} \subset C^q$$

Στην πραγματικότητα, εάν ισχύει η (5), τότε η Κατασκευή Β λειτουργεί χρησιμοποιώντας ως L τη λίστα που ορίζεται στη 2η περίπτωση.

Τώρα σημειώνεται ότι οι συνθήκες (3), (4) και (5) του Θεωρήματος 3.1 πληρούνται για $p > (2q^3 - 3q^2 + 1)^2 + 3q^2$.

Θεώρημα 3.3

Αν $p = 6n + 1$ είναι πρώτος και $p > (2q^3 - 3q^2 + 1)^2 + 3q^2$, όπου q είναι ο μικρότερος πρώτος παράγοντας του n,τότε θα υπάρχει ένας κυκλικός $(4p, 4, 1) - BIBD$.

Θεώρημα 3.4

Αν $p = 6n + 1$ είναι πρώτος > 7 και ο μικρότερος πρώτος παράγοντας του n δεν είναι μεγαλύτερος από 19, τότε θα υπάρχει ένας κυκλικός $(4p, 4, 1) - BIBD$.

Απόδειξη:

Έστω q ο μικρότερος πρώτος παράγοντας του n. Αν $q = 2$ ή 3 $\tau\acute{o}\tau\varepsilon$ $p \equiv 1\ (mod\ 12)$ ή $p \equiv 19\ (mod\ 36)$. Σε αυτές τις περιπτώσεις η ύπαρξη ενός κυκλικού $(4p, 4, 1) - BIBD$ έχει ήδη παγιωθεί (από την ενότητα 2 και το Θεώρημα 3.2).

Για $5 \leq q \leq 19$ έχει ελεγχθεί, με τη βοήθεια υπολογιστή, ότι οι Κατασκευές Α ή Β μπορούν να πραγματοποιηθούν με επιτυχία για $p > (2q^3 - 3q^2 + 1)^2 + 3q^2$. Η εγκυρότητα του ισχυρισμού προκύπτει από το Θεώρημα 3.3.

IV. Κυκλικοί $(4, 1) - GDD$ Τύπου 6^p

Η ύπαρξη ενός κυκλικού $(4, 1) - GDD$ τύπου 6^p με p πρώτο, έχει λυθεί από τους Brouwer, Schrjiver και Hanani στο [7] για $p \equiv 3\ (mod\ 4)$, και για $p \equiv 1\ (mod\ 4)$,$p \neq 5$ από τους Chen, η Ge και Zhu στο [8].

Θεώρημα 4.1

Υπάρχει ένας κυκλικός $(4, 1) - GDD$ τύπου 6^p , για κάθε περιττό πρώτο $p = 5$.

Απόδειξη:

Έστω p είναι περιττός πρώτος. Διακρίνονται δύο περιπτώσεις ανάλογα με το αν p είναι ή δεν είναι πρώτος Fermat , δηλαδή της μορφής $2^n + 1$.

1η Περίπτωση: p δεν είναι πρώτος Fermat

Έστω e η μεγαλύτερη δύναμη του 2 που διαιρεί το $p - 1$ και ω η αρχική ρίζα $(mod\ p)$. Εξετάζοντας το ακόλουθο υποσύνολο του $\mathbb{Z}_6 \oplus \mathbb{Z}_p$:

$$B = \left\{(0,\ 0),\ (0,\ 2),\ (1,\ 1), \left(4, \frac{2}{\omega^e + 1}\right)\right\}$$

θα ισχύει:

$$\Delta B = \bigcup_{\iota=0}^{5} \{i\} \times L_i$$

όπου $L_0 = \{\pm 2\}$, $L_1 = \{\pm 1\}$, $L_2 = \{\frac{-2}{\omega^e + 1}, \frac{2\omega^e}{\omega^e + 1}\}$, $L_3 = \{\pm \frac{\omega^e - 1}{\omega^e + 1}\}$.

Θέτοντας $S = \left\{\omega^{ei+j} \,\middle|\, 0 \leq i < \frac{p-1}{e};\ 0 \leq j < \frac{e}{2}\right\}$ τότε, $L_i S = \mathbb{Z}_p^*$ για κάθε i,

και

$$\mathcal{F} = \{B \cdot (1, s)\ |s \in S\}$$

είναι μία $(6p,\ 6, 4,\ 1) - DF$.

2η Περίπτωση: p είναι πρώτος Fermat

Αν $p = 5$, μία υπολογιστική έρευνα δείχνει ότι δεν υπάρχει $(6p,\ 6, 4,\ 1) - DF$.
Αν $p > 5$ και ε 4η αρχική ρίζα $(mod\ p)$ τότε, για τα ακόλουθα υποσύνολα του $\mathbb{Z}_6 \oplus \mathbb{Z}_p$:

$$B_1 = \{(0,\ 0),\ (0,\ 1),\ (1, -2),\ (1,\ 3)\}$$
$$B_2 = \{(0,\ 0),\ (0, \varepsilon),\ (2, -2\varepsilon),\ (2,\ 3\varepsilon)\}$$
$$B_3 = \{(0,\ 0),\ (1,\ 2\varepsilon),\ (3,\ 2\varepsilon + 2),\ (4,\ 2)\}$$
$$B_4 = \{(0,\ 0),\ (1,\ 3\varepsilon),\ (3,\ 3\varepsilon + 3),\ (4,\ 3)\}$$

θα ισχύει:

$$\bigcup_{i=0}^{4} \Delta B_i = \bigcup_{\iota=0}^{5} \{i\} \times L_i\langle\varepsilon\rangle$$

όπου $L_0 = \{1,\ 5\}$, $L_1 = L_2 = L_4 = L_5 = \{2,\ 3\}$, $L_3 = \{2\ (\varepsilon + 1), 3\ (\varepsilon + 1)\}$.

Σημειώνεται ότι, το 2 είναι τέλειο τετράγωνο $(mod\ p)$, δεδομένου ότι $p \equiv 1\ (mod\ 8)$. Επίσης, χρησιμοποιώντας το νόμο της τετραγωνικής αντιστροφής, φαίνεται εύκολα ότι και οι 3 και 5 είναι μη τέλεια τετράγωνα $(mod\ p)$. Επομένως, κάθε L_i έχει έναν αριθμό τέλειο τετράγωνο και έναν μη τέλειο τετράγωνο $(mod\ p)$. Έτσι, εάν S είναι εγκάρσιο στο $\mathbb{Z}_p^*/C^2$, θα ισχύει ότι

$$\mathcal{F} = \{B_i \cdot (1, s) | 1 \le i \le 4;\ s \in S\}$$

είναι ένα $(6p,\ 6, 4,\ 1) - DF$.

V. Κυκλικοί $(4,\ 1) - GDD$ Τύπου 8^p

Σε αυτή την παράγραφο παρουσιάζεται μια ρητή κατασκευή.

Θεώρημα 5.1.

Υπάρχει ο κυκλικός $(4,\ 1) - GDD$ τύπου 8^p για οποιοδήποτε πρώτο $p \equiv 1\ (mod\ 6)$.

Έστω p πρώτος $\equiv 1\ (mod\ 6)$ και έστω ε μία κυβική πρωταρχική ρίζα της μονάδας $(mod\ p)$.

Εξετάζοντας τα ακόλουθα υποσύνολα του $\mathbb{Z}_8 \oplus \mathbb{Z}_p$:

$$B_i = \{(0,\ 0),\ (1,\ 2\varepsilon^i)\ (3, -\varepsilon^{i+1}),\ (5, -\varepsilon^i)\}\ i = 0,\ 1,\ 2$$
$$B_3 = \{(0,\ 2),\ (0,\ 2\varepsilon),\ (0,\ 2\varepsilon^2),\ (1,\ 0)\}$$

και λαμβάνοντας υπόψιν τη βασική ταυτότητα $\varepsilon^2 + \varepsilon + 1 = 0$,

θα ισχύει:

$$\bigcup_{i=0}^{3} \Delta B_i = \bigcup_{\iota=0}^{7} \{i\} \times x_i\langle -\varepsilon\rangle$$

όπου $x_0 = 2(\varepsilon - 1)$, $x_1 = x_7 = 2$, $x_2 = x_6 = \varepsilon - 1$, $x_3 = x_5 = 1$ *και* $x_4 = 3$.

Συνεπώς, εάν S είναι εγκάρσιο στο $\mathbb{Z}_p^*/\langle -\varepsilon \rangle$

θα ισχύει

$$\mathcal{F} = \{B_i \cdot (1, s) | 0 \leq i \leq 3;\ s \in S\}$$

είναι ένα $(8p,\ 8,\ 4,\ 1) - DF$.

VI. Αναδρομικές κατασκευές, Θεωρία σχεδιασμών και Βέλτιστοι $OOCs$

Υπενθύμιση του ακόλουθου θεωρήματος.

Θεώρημα 6.1

Αν υπάρχει μία $(gv_i, g, k, 1) - DF$ *για* $i = 1,2$ και k δεν είναι μεγαλύτερος από τον μικρότερο πρώτο παράγοντα v_2, δηλαδή $M.K.\Delta.(k!,\ v_2) = 1$, τότε θα υπάρχει και μια $(gv_1v_2, g, k, 1) - DF$.

Οι περιπτώσεις για $g = k$ *και* $g = k - 1$ δίνονται στα [1] και [2], αντίστοιχα. Για αυθαίρετο g, γίνεται αναφορά στο [3] και [4].

Η εφαρμογή του Θεώρημα 6.1 και ο συνδυασμός όλων των αποτελεσμάτων που επιτεύχθηκαν στις προηγούμενες παραγράφους, οδηγούν στα ακόλουθα θεώρημα:

Θεώρημα 6.2

Υπάρχει ο κυκλικός $(4,\ 1) - GDD$ τύπου 4^v ή ισοδύναμα, ένας κυκλικός $(4v, 4,\ 1) - BIBD$, για όλα τα v της μορφής $v = 4\,p_1\,p_2 \ldots p_n$, όπου p_i είναι πρώτος $\equiv 1\ (mod\ 6)$ τέτοιος ώστε ο λόγος $\frac{(p_i - 1)}{6}$ να έχει έναν πρώτο παράγοντα που δεν υπερβαίνει το 19.

Θεώρημα 6.3

Υπάρχει ένας κυκλικός $(4,\ 1) - GDD$ τύπου 6^v για όλα τα v τέτοιος ώστε $M.K.\Delta.(t, 30) = 1$.

Θεώρημα 6.4

Υπάρχει ένας κυκλικός $(4,\ 1) - GDD$ τύπου 8^v για όλα τα v έτσι ώστε κάθε p_i να είναι πρώτος $\equiv 1\ (mod\ 6)$.

Τέλος, δεδομένου ότι $(v,\ g,\ k,\ 1) - DF$ με $g \leq k(k - 1)$ είναι επίσης βέλτιστος $(v, 4,1) - OOC$, τα παραπάνω θεωρήματα μπορούν να μεταφράσουν ως εξής.

Θεώρημα 6.5

Υπάρχει ο βέλτιστος $(v, 4, 1) - OOC$ για όλα τα v των εξής τύπων:

$v = 4\,p_1\,p_2 \ldots p_n$ όπου κάθε p_i είναι ένα πρώτος $\equiv 1\ (mod\ 6)$ τέτοιος ώστε $\frac{(p_i - 1)}{6}$ έχει έναν πρώτο παράγοντα που δεν υπερβαίνει το 19.

$v = 6t$ με $\text{M.K.Δ.}(t, 30) = 1$.

$v = 8\,p_1\,p_2 \ldots p_n$ όπου κάθε p_i είναι ένα πρώτος $\equiv 1\ (mod\ 6)$.

Βιβλιογραφία

[1]. M. Buratti, Recursive constructions for difference matrices and relative difference families, J. of Combin. Designs, Vol. 6 (1998) pp. 165–182.

[2]. M. J. Colbourn and R. A. Mathon, On cyclic Steiner 2-designs, Ann. Discrete Math.

[3]. R. Peltesohn, Eine Losung der beiden Heffterschen Differenzenprobleme, Compos. Math., Vol. 6 (1938) pp. 251–257.

[4]. M. J. Colbourn and C. J. Colbourn, Cyclic block designs with block size 3, Eur. J. Combin., Vol. 2 (1981) pp. 21–26.

[5]. R. Rees and N. Shalaby, Simple and indecomposable twofold cyclic triple systems from Skolem sequences, J. Combin. Designs, Vol. 8 (2000) pp. 402–4

[6α]. R. C. Bose, On the construction of balanced incomplete block designs, Ann. Eugenics, Vol. 9 (1939) pp. 353–399.

[6β]. M. Buratti, From a (G, k, 1) to a ($C_k \oplus$G, k, 1) difference family, Designs, Codes and Cryptography, Vol. 11 (1997) pp. 5–9.

[7]. A. E. Brouwer, A. Schrijver and H. Hanani, Group divisible design with block-size four, Discrete Math., Vol. 20 (1977) pp. 1–19.

[8]. K. Chen, G. Ge and L. Zhu, Starters and related codes, J. Statist. Plann. Inference, Vol. 86 (2000) pp. 595–604.

[9]. M. Jimbo, A recursive construction for 1-rotational Steiner 2-designs, Utilitas Math., Vol. 26 (1984) pp. 45–61.

[10]. J. Yin, Some combinatorial constructions for optical orthogonal codes, Discrete Math., Vol. 185 (1998) pp. 201–219.

Βέλτιστοι Οπτικοί Ορθογώνιοι Κώδικες με βάρος $w = 5$

I. Εισαγωγή

Ο $(v, k, 1) - OOC$ είναι βέλτιστος, αν δεν υπάρχει $(v, k, 1) - OOC$ με περισσότερες κωδικές λέξεις. Έστω C ένας $(v, k, 1) - OOC$. Αν ληφθεί υπόψιν, κάθε ακολουθία του C και όλες οι κυκλικές μετατοπίσεις του ως κωδικές λέξεις, τότε θα προκύψει ένας σταθερού βάρους δυαδικός κώδικας διόρθωσης σφαλμάτων μήκους v και βάρους k, που θα περιέχει $|C|v$ κωδικές λέξεις. Έτσι, από το γνωστό φράγμα Johnson, θα ισχύει $|c| \leq \frac{\mathrm{v}-1}{\mathrm{k}\,(\mathrm{k}-1)}$. Όταν ο $(v, k, 1) - OOC$ περιέχει $\left\lfloor \frac{\mathrm{v}-1}{\mathrm{k}\,(\mathrm{k}-1)} \right\rfloor$ κωδικές λέξεις, τότε είναι βέλτιστος. Έχει αποδειχθεί στα [1] , [2] ότι ο βέλτιστος $(v, 3, 1) - OOC$ υπάρχει αν και μόνο εάν $v \neq 6t + 2$ με $t \equiv 2$ ή 3 $(mod\ 4)$. Για $\kappa \geq 4$, το υπάρχον πρόβλημα για το βέλτιστο$(v, k, 1) - OOC$ απέχει πολύ από το να ρυθμιστεί, παρά τις πολλές προσπάθειες που δαπανώνται για τις μεθόδους κατασκευής και την υπόθεση ύπαρξης του.

Βέλτιστοι $(v, k, 1) - OOC$s είναι στενά συνδεδεμένοι με συνδυαστικούς σχεδιασμούς.

Στο [3], η $(G, N, k, 1)$ οικογένεια διαφορών (εν συντομία DF) ορίζεται να είναι μια οικογένεια $\mathcal{D} = \{D_i : i \in I\}$ ορισμένων k - υποσύνολων (blocks βάση) της ομάδας G τέτοια ώστε η λίστα των διαφορών $\{d - d' : d, d' \in D_i, i \in I\}$ να περιλαμβάνει κάθε στοιχείο της $G - N$ ακριβώς μια φορά και κάθε στοιχείο του N καμία φορά, όπου N είναι μια υποομάδα της G. Μια τέτοια οικογένεια λέγεται ότι είναι πάνω στη G και σχετική με την N. Αν G είναι μια κυκλική ομάδα τάξης v , και N είναι μια υποομάδα τάξης n, η σχετική οικογένεια διαφορών συμβολίζεται απλά ως $(v, n, k, 1) - DF$.

Μια $(v, n, k, 1) - DF$ ονομάζεται επίσης (n - regular cyclic packing) τακτική κυκλική ομαδοποίηση $CP\ (k, 1\ ; v)$ ή ομοιόμορφος κυκλικά μεταθέσιμος κώδικας $(n\frac{v}{n}, 2k - 2, k)$.

Από μια $(v, n, k, 1) - DF$, μπορεί να κατασκευαστεί μία (0, 1) - ακολουθία μήκους v από κάθε block βάσης. Είναι εύκολο να δειχθεί ότι η παραγωγή (0, 1) - ακολουθιών συγκροτεί έναν $(v, k, 1) - OOC$. Η σύνδεση αυτή προσφέρει έναν τρόπο ώστε να επιτευχθούν $OOCs$ από σχετικές οικογένειες διαφορών. Μια $(v, n, k, 1) - DF$ περιέχει $\frac{v-n}{k\,(k-1)}$ blocks και ο αντίστοιχος $(v, k, 1) - OOC$ είναι βέλτιστος, αν $\frac{v-n}{k\,(k-1)} = \left\lfloor \frac{v-1}{k\,(k-1)} \right\rfloor$.

Πολλές εργασίες έχουν γίνει για $(np, n, 4,1) - DF$ όπου p είναι πρώτος. Για $n \geq 12$, έχει αποδειχθεί ότι υπάρχουν τέτοιες DFs, στο [4] γίνονται αναφορές. Όλες αυτές οδηγούν σε βέλτιστους $(np, 4, 1) - OOCs$. Πρόβλημα έχει εμφανιστεί για $k = 5$. Ο Hanani στο [5] κατασκεύασε την $(5p, 5, 5, 1) - DF$ για οποιονδήποτε πρώτο $p \equiv 1\ (mod\ 4)$ και $p \neq 5$. Η $(p, 1, 5, 1) - DF$ φαίνεται να υπάρχει για κάθε πρώτο $p \equiv 1\ (mod\ 20)$, στα [6], [7]. Οι Tang και Yin στο [4] έδειξαν την ύπαρξη της $(15p, 15, 5, 1) - DF$ για οποιονδήποτε πρώτο $p \equiv 1\ (mod\ 4)$ και $p > 5$. Στο [8], αναφέρεται μια κατασκευή $(4p, 4, 5, 1) - DF$ για πρώτο $p \equiv 31\ (mod\ 60)$.

Σε αυτήν την ενότητα, θα διερευνηθεί η ύπαρξη $(4p, 4, 5, 1) - DF$ για οποιαδήποτε πρώτο $p \equiv 1\ (mod\ 10)$, και $(4up, 4u, 5,1) - DF$ για κάθε πρώτο $p \equiv 11\ (mod\ 20)$ και $u = 2, 3$. Αυτές οι DFs οδηγούν σε βέλτιστους $(np, 5, 1) - OOCs$.

Για να απεδείχθη η ύπαρξη τέτοιων $(4up, 4u, 5, 1) - DFs$, πρέπει πρώτα να παρουσιαστεί στην παράγραφο 2, ότι η ύπαρξή των DFs είναι εγγυημένη με την ύπαρξη ορισμένων στοιχείων στο πεπερασμένο σώμα $GF(p)$. Αυτό, δίνει τη δυνατότητα να χρησιμοποιηθεί το θεώρημα του Weil, όπου ο αθροιστικός χαρακτήρας εκτιμάται στο $GF(p)$ ώστε να επιλυθεί. Στην παράγραφο 3 παρουσιάζεται η ύπαρξη μεγάλων p, και στην παράγραφο 4, παρουσιάζονται οι DFs και οι κώδικες που είναι κατασκευασμένοι για μικρές τιμές p. Τα βασικά αποτελέσματα θα ακολουθήσουν.

Θεώρημα 1.1

Για οποιαδήποτε πρώτο $p \equiv 1\ (mod\ 10)$, υπάρχουν μία $(4p, 4, 5, 1) - DF$ με μοναδική εξαίρεση το βέλτιστο $(4p, 5, 1) - OOC\ για\ p = 11$.

Θεώρημα 1.2

Για οποιαδήποτε πρώτο $p \equiv 11\ (mod\ 20)$ και για κάθε $u = 2, 3$, υπάρχουν μία $(4up, 4u, 5, 1) - DF$, καθώς και ένας βέλτιστος $(4up, 5, 1) - OOC$.

II. DFs και ορισμένα στοιχεία στο $GF(p)$

Στην παράγραφο αυτή θα δειχθεί ότι υπάρχει μια $(4up, 4u, 5, 1) - DF$ εάν υπάρχουν, κάποια στοιχεία στο $GF(p)$ που ικανοποιούν ορισμένες ιδιότητες.

Σταθερός πρώτος $p \equiv 1\ (mod\ n)$ και ένα αρχικό στοιχείο $w \in GF(p)$, με C_0^n θα συμβολίζεται η πολλαπλασιαστική υποομάδα $\left\{w^{in} : 0 \le i < \frac{p-1}{n}\right\}$ της n-οστης δύναμης $modulo\ p$, ενώ $με\ C_j^n$ θα συμβολίζεται το σύμπλοκο του C_0^n στο $GF(p)^*(= C_0^1)$ εκπροσωπούμενο από το w^j, δηλαδή $C_j^n = w^j C_0^n$. Έστω G η προσθετική ομάδα του δακτυλίου $GF(p) \times \mathbb{Z}_{4u}$. Για $u = 1, 2, 3$ η G είναι μια κυκλική ομάδα αν $p \ge 5$. Σε αυτά που ακολουθούν, το (i, j) ανήκει στο $GF(p) \times \mathbb{Z}_{4u}$ και απλά συμβολίζεται i_j.

Για $p \equiv 1\ (mod\ 10)$, δεδομένου ότι κάθε μπλοκ βάσης δημιουργεί 20 διαφορές, η $(4p, 4, 5, 1) - DF$ περιέχει $\frac{4p-4}{20} = \frac{p-1}{5}$ blocks βάσης. Τα απαιτούμενα $\frac{p-1}{5}$ blocks βάσης θα δημιουργούνται από 2 αρχικά blocks βάσης, σύμφωνα με όλους τους αντιπροσώπους του $C_0^5/\{1, -1\}$.

Στόχος είναι να βρεθούν τέτοια αρχικά blocks βάσης;

Λήμμα 2.1

Έστω $p \equiv 1 \ (mod\ 10)$ είναι πρώτος.

Αν υπάρχει ένα ζευγάρι (x, y) που πληροί τις παρακάτω ιδιότητες:

(1) $1,\ x-1,\ x-2,\ \frac{x-3}{2}$ $και$ $x+2y$ είναι ένα αντιπροσωπευτικό σύστημα συμπλόκου τάξεων $\{C_0^5, C_1^5, C_2^5, C_3^5, C_4^5\}$,

(2) $1,\ x,\ x-2,\ 2x-3$ $και$ $x+2y$ είναι ένα αντιπροσωπευτικό σύστημα συμπλόκου τάξεων $\{C_0^5, C_1^5, C_2^5, C_3^5, C_4^5\}$,

(3) $\frac{x-1}{2},\ y,\ x+y,\ y-\frac{x-3}{2}$ $και$ $y+3\frac{x-1}{2}$ είναι ένα αντιπροσωπευτικό σύστημα συμπλόκου τάξεων $\{C_0^5, C_1^5, C_2^5, C_3^5, C_4^5\}$,

Τότε, θα υπάρχει η $(4p, 4, 5, 1) - DF$.

Απόδειξη:

Ισχύει ότι $-1 \in C_0^5$. Συνεπώς, $\{1, -1\}$ είναι μια υποομάδα του C_0^5. Σύμφωνα με την υπόθεση, υπάρχει ένα ζευγάρι (x, y) που ικανοποιεί τις ιδιότητες (1) - (3). Η επιθυμητή $(4p, 4, 5, 1) - DF$ μπορεί να κατασκευαστεί λαμβάνοντας υπόψιν τα ακόλουθα $\frac{p-1}{5}$ blocks βάσης που βασίζονται στην προσθετική ομάδα $GF(p) \times \mathbb{Z}_4$,

$$\left\{0_0, 1_0, (x-1)_0, \left(\frac{x}{2}\right)_1, \left(\frac{1}{2}\right)_3\right\} \cdot r_1,$$
$$\left\{0_0, \left(\frac{x-3}{2}\right)_0, y_2, (-x-y)_2, \left(-\frac{x}{2}\right)_1\right\} \cdot r_1,$$

όπου r λαμβάνει τιμές από όλους τους εκπροσώπους του $C_0^5/\{1, -1\}$.

Εύκολα ελέγχεται ότι η λίστα των διαφορών, προκύπτει από αυτά τα blocks βάσης, τα οποία καλύπτουν κάθε στοιχείο του $(GF(p) \times \mathbb{Z}_4) \backslash (\{0\} \times \mathbb{Z}_4)$ ακριβώς μια φορά, ενώ κάθε στοιχείο της προσθετικής υποομάδας $\{0\} \times \mathbb{Z}_4$ δεν καλύπτεται καθόλου. Τότε η απόδειξη, έχει ολοκληρωθεί.

▪

Για $p \equiv 11 \ (mod\ 20)$ και $u = 2, 3,$ η $(4up, 4u, 5, 1) - DF$ περιέχει $\frac{4up-4u}{20} = 2ut$ blocks βάσης, όπου $t = \frac{p-1}{10}$. Σαφώς, t είναι περιττός και $-1 \in C_5^{10}$. Υποτίθεται ότι τα $2ut$ blocks βάσης δημιουργούνται από $2u$ αρχικά blocks βάσης, σύμφωνα με την πολλαπλασιαστική υποομάδα $C_0^{10} \times \{1\}$. Στόχος, είναι η εύρεση αρχικής βάσης με blocks, όπως επίσης και η εύρεση αρχικής βάσης με blocks για $p \equiv 11 \ (mod\ 20)$ και $u = 1$, η οποία είναι διαφορετική από αυτή στο Λήμμα 2.1.

Σημείωση

Υποτίθεται ότι x είναι ένα στοιχείο στο $GF(p)$ τέτοιο ώστε

$$x \in C_i^{10}, i \in \{1,3,7,9\}$$

Αν $x-1, x+1, x^2+x+1 \in GF(p)^*$, τότε υπάρχουν μοναδικά $0 \le j,s,h \le 9$ τέτοια ώστε

$$x-1 \in C_{ji}^{10},\ x+1 \in C_{si}^{10},\ x^2+x+1 \in C_{hi}^{10}\ .$$

Αυτή η ιδιότητα συμβολίζεται, εν σύντομα ως $T(x) = (j,s,h)$.

Λήμμα 2.2

Αν $T(x) = (2,2,4)$, τότε υπάρχει $(4up, 4u, 5,1) - DF$ για οποιοδήποτε $u = 1,2,3$.

Απόδειξη:

Για $u = 1$, έχουν ληφθεί τα εξής δύο αρχικά blocks βάσης:

$$\{0_0, 1_0, x_0^1, x_1^2, x_3^3\}, \{0_0, x_0^4, x_1^5, x_2^6, x_2^7\}$$

Υπολογίζοντας τις διαφορές αυτών, για ένα σταθερό j στο $\mathbb{Z}_{4u}$, συμβολίζεται

$$D_j = \{d : d_j \text{ είναι μια διαφορά από τα αρχικά blocks βάσης}\}.$$

Τότε,

$$D_0 = \pm\{1, x, x-1, x^4, x^7 - x^6\}$$
$$D_1 = \{x^2, x^2-1, x^2-x, x^3, 1-x^3, x-x^3, x^5, x^5-x^4, x^6-x^5, x^7-x^5\}$$
$$D_2 = \pm\{x^3-x^2, x^6, x^6-x^4, x^7, x^7-x^4\}$$
$$D_3 = -D_1.$$

Είναι εύκολο να ελεγχθεί ότι κάθε D_j είναι ένα σύνολο διακεκριμένων αντιπροσωπευτικών συμπλόκων - set of distinct representatives of cosets - (εν συντομία SDRC). Πράγματι, τα δύο blocks αποτελούν τα αρχικά blocks βάσης.

Για $u = 2$, υπάρχουν τέσσερα αρχικά blocks βάσης, τα εξής:

$$\{0_1, x_2^2, 1_0, x_0^1, x_0^3\}, \{0_4, x_6^6, x_0^7, x_0^8, x_1^9\}$$

$$\{0_0, x_0^3, x_3^5, x_4^6, x_5^4\}, \{0_1, x_3^7, x_4^8, x_6^6, x_0^9\}$$

Είναι εύκολο να ελεγχθεί ότι κάθε D_j για $0 \le j \le 4$ είναι ένα SDRC. Συνεπώς, τα τέσσερα blocks αποτελούν πράγματι τα αρχικά blocks βάσης.

Για $u = 3$, υπάρχουν έξι αρχικά blocks βάσης, τα εξής:

$$\{0_0, x_0, x_0^3, 1_1, x_1^2\}, \quad \{0_0, x_0^7, x_3^8, x_5^6, x_8^9\}, \quad \{0_0, x_1^6, x_2^3, x_5^4, x_8^5\}$$

$$\{0_0, x_1^5, x_3^4, x_6^3, x_8^2\}, \quad \{0_0, x_1^8, x_3^7, x_6^6, x_{10}^5\}, \quad \{0_0, x_2^2, x_4, 1_6, x_8^3\}$$

Είναι εύκολο να ελεγχθεί ότι κάθε D_j για $0 \le j \le 6$ είναι ένα SDRC. Συνεπώς, τα έξι blocks αποτελούν πράγματι τα αρχικά blocks βάσης. Αυτό ολοκληρώνει την απόδειξη.

Λήμμα 2.3

Αν $T(x) = (2, 7, 4)$, τότε υπάρχει $(4up, 4u, 5, 1) - DF$ για οποιαδήποτε $u = 1, 2, 3$.

Απόδειξη:

Για $u = 1, 2, 3$, παρατίθεται η λίστα που αντιστοιχεί στα αρχικά blocks βάσης ως εξής:

$u = 1,$ $\{0_0, x_0^1, x_0^2, x_1^4, x_2^3\}$ $\{0_0, 1_0, x_1^2, x_1^3, x_2\}$
$u = 2,$ $\{0_0, x_0^3, x_0^5, x_1^4, x_2^2\}$ $\{0_3, x_4^8, x_0^7, x_0^9, x_1^6\}$
$\{0_4, 1_5, x_0^2, x_0^3, x_2\}$ $\{0_6, x_0^4, x_1, x_3^3, x_4^2\}$
$u = 3,$ $\{0_0, x_0^2, x_0^3, 1_1, x_2\}$ $\{0_0, x_0^5, x_1^6, x_3^3, x_6^4\}$ $\{0_0, x_0, 1_4, x_5^2, x_8^3\}$
$\{0_0, x_1^5, x_3^6, x_6^7, x_8^8\}$ $\{0_0, x_1^3, x_4^2, x_8^4, x_{10}\}$ $\{0_0, x_1^8, x_5^7, x_7^6, x_{10}^5\}$

▪

Λήμμα 2.4

Αν $T(x) = (7, 2, 4)$, τότε υπάρχει $(4up, 4u, 5,1) - DF$ για οποιαδήποτε $u = 1, 2, 3$.

Απόδειξη:

Για $u = 1, 2, 3$, παρατίθεται η λίστα που αντιστοιχεί στα αρχικά blocks βάσης ως εξής:

$u = 1,$ $\{0_0, 1_0, x_0^3, x_1^2, x_2\}$ $\{0_1, x_1^4, x_2^7, x_0^5, x_0^6\}$
$u = 2,$ $\{0_2, x_0^2, x_0^3, x_0^4, x_1^5\}$ $\{0_0, x_0^2, x_2, x_4^4, x_5^3\}$
$\{0_4, x_5^4, x_0^2, x_0^5, x_3^3\}$ $\{0_5, x_0^2, x_1^3, 1_2, x_3\}$
$u = 3,$ $\{0_0, 1_0, x_0, x_1^2, x_1^3\}$ $\{0_0, x_0^3, x_5^2, x_8^4, x_{10}^5\}$ $\{0_0, x_1^4, x_3^6, x_7^5, x_9^7\}$
$\{0_4, x_6^2, x_9, x_0^3, 1_1\}$ $\{0_8, x_{10}^5, x_0^4, x_1^7, x_4^6\}$ $\{0_7, x_{10}^7, x_0^6, x_1^5, x_5^4\}$

▪

Λήμμα 2.5

Αν $T(x) = (7, 7, 4)$, τότε υπάρχει $(4up, 4u, 5,1) - DF$ για οποιοδήποτε $u = 1, 2, 3$.

Απόδειξη:

Για $u = 1, 2, 3$, παρατίθεται η λίστα που αντιστοιχεί στα αρχικά blocks βάσης ως εξής:

$u = 1,$ $\{0_0, x_0, x_0^3, x_1^2, 1_2\}$ $\{0_1, x_1^4, x_2^7, x_0^5, x_0^6\}$
$u = 2,$ $\{0_0, x_0^4, x_0^6, x_1^5, x_2^3\}$ $\{0_1, x_3^2, x_0, 1_4, x_0^3\}$
$\{0_4, x_5^4, x_0^3, x_0^5, x_2^2\}$ $\{0_1, x_3^6, x_4^7, x_6^4, x_0^5\}$
$u = 3,$ $\{0_0, x_0^5, x_0^6, x_1^7, x_1^8\}$ $\{0_0, x_0^8, x_3^7, x_4^5, x_6^6\}$ $\{0_0, x_1^2, x_3^4, x_6^3, x_8^5\}$
$\{0_0, x_1^5, x_4^6, x_6^4, x_8^3\}$ $\{0_0, x_1^1, x_5^4, x_8^2, x_{10}^3\}$ $\{0_0, 1_2, x_4^3, x_6^2, x_9\}$

▪

Τα Λήμματα 2.2 έως 2.5 μπορούν να συνδυαστούν για να προκύψει το ακόλουθο.

Λήμμα 2.6

Έστω ότι υπάρχει ένα στοιχείο x στο $GF(p)$ τέτοιο ώστε $x \in C_i^{10}$, $x - 1 \in C_{2i}^{10} \cup C_{7i}^{10}$, $x + 1 \in C_{2i}^{10} \cup C_{7i}^{10}$ $και$ $x^2 + x + 1 \in C_{4i}^{10}$, όπου $i \in \{1, 3, 7, 9\}$.

Τότε υπάρχει $(4up, 4u, 5,1) - DF$ για κάθε $u = 1, 2, 3$.

Αυτό το λήμμα πραγματεύεται ομοιόμορφα και τις τρεις περιπτώσεις για $u = 1, 2, 3$. Στα Λήμματα 2.1 και 2.6 γίνεται χρήση του Θεωρήματος του Weil, όπου ο αθροιστικός χαρακτήρας εκτιμάται στο $GF(p)$, ο οποίος θα συζητηθεί στην επόμενη παράγραφο.

III. Η χρήση του Θεωρήματος του Weil

Ο πολλαπλασιαστικός χαρακτήρας του $GF(p)$, όπου p πρώτος, είναι η απεικόνιση $\chi: GF(p) \to \{z \in C: |z| = 1 \text{ ή } 0\}$ τέτοια ώστε $\chi(0) = 0$, $\chi(1) = 1$, με την ιδιότητα $\chi(xy) = \chi(x)\chi(y)$ για οποιαδήποτε $(x, y) \in GF(p) \times GF(p)$.

Ακολουθεί το θεώρημα του Weil:

Θεώρημα 3.1 [9]

Έστω ψ ένας πολλαπλασιαστικός χαρακτήρας του $GF(p)$ τάξης $m > 1$ και έστω $GF(p)[x]$ αποτελεί το μοναδικό πολυώνυμο θετικού βαθμού που δεν είναι m-οστης δύναμης. Έστω d ο αριθμός των διακεκριμένων ριζών της f στο σώμα ριζών του $GF(p)$, τότε για κάθε ένα $a \in GF(p)$, θα ισχύει

$$\left| \sum_{c \in GF(p)} \psi[\alpha f(c)] \right| \leq (d-1)\sqrt{p}$$

Σχέση (1)

Σαν εφαρμογή του Θεωρήματος 3.1, μπορεί να δοθεί το ακόλουθο θεώρημα, γεγονός που επιβεβαιώνεται από τον Buratti στο [10].

Θεώρημα 3.2

Έστω p είναι πρώτος $\equiv 1 \, (mod\ q)$ με

$$p - \left[\sum_{i=0}^{s-2} \binom{S}{i} (s-i-1)(q-1)^{s-i} \right] \sqrt{p} - sq^{s-1} > 0$$

Τότε, για κάθε δοσμένη s – αδα $(j_1, j_2, \dots, j_s) \in \{0,\ 1, \dots,\ q-1\}^s$ και κάθε δοσμένη s - αδα $(c_1, c_2, \dots, c_s)$ του $GF(p)$, υποδηλώνεται ότι θα υπάρχει ένα στοιχείο $x \in GF(p)$ τέτοιο ώστε $x + c_i \in C_{j_i}^q$ για κάθε i.

Απόδειξη:

Για $i = 1, 2, \dots, s$ ορίζεται ένα στοιχείο $a_i \in C_{-j_i}^q$ και ένα σύνολο $b_i = a_i c_i$. Με τον τρόπο αυτό, το άθροισμα $x + c_i \in C_{j_i}^q$ είναι ισοδύναμο με το άθροισμα $a_i x + b_i \in C^q$. Έτσι, έχει αποδειχθεί ότι το σύνολο

$$A = \{x \in GF(p) \mid a_i x + b_i \in C^q \ \gamma\iota\alpha\ i = 1, 2, \dots, s\}$$

δεν είναι κενό.

Για $i = 1, 2, \dots, s$ ορίζεται $f_i \in GF(p)[x]$ ως $f_i = a_i x + b_i$.

Έστω χ είναι πολλαπλασιαστικός χαρακτήρας τάξης q του $GF(p)$ και το άθροισμα

$$S = \sum_{x \in GF(p)} \prod_{i=1}^{s} [1 + \chi(f_i(x)) + \chi\left({f_i}^2(x)\right) + \cdots + \chi\left({f_i}^{q-1}(x)\right)]$$

Για $i = 1, 2, \dots, s$ θα είναι:

$$1 + \chi(f_i(x)) + \chi\left({f_i}^2(x)\right) + \cdots + \chi\left({f_i}^{q-1}(x)\right) = \begin{cases} q & \alpha\nu\ f_i(x) \in C^q \\ 0 & \alpha\nu\ f_i(x) \in GF(p)^* - C^q \\ 1 & \alpha\nu\ x = -b_i/a_i \end{cases}$$

Αυτό εύκολα σημαίνει ότι $q^s|A| \le S \le q^s|A| + sq^{s-1}$.

Από την άλλη πλευρά, πρέπει επίσης

$$S = \sum_{(e_1, e_2, \dots, e_s)} \sum_{x \in GF(p)} \chi[f_1^{e_1}\ f_2^{e_2} \dots f_s^{e_s}(x)]$$

όπου $(e_1, e_2, \dots, e_s)$ λαμβάνει τιμές από το $\{0, 1, \dots, q-1\}^s$.

Σημειώνεται ότι αν $(e_1, e_2, \dots, e_s) \neq (0,0, \dots, 0)$ τότε $f_1^{e_1}\ f_2^{e_2} \dots f_s^{e_s} = kg^q$, με κανένα ζευγάρι $(k, g) \in GF(p) \times GF(p)[x]$.

Άρα, χρησιμοποιώντας το Θεώρημα 3.1, θα ισχύει:

$$\left| \sum_{x \in GF(p)} \chi[f_1^{e_1}\ f_2^{e_2} \dots f_s^{e_s}(x)] \right| \begin{cases} \le (s-1)\sqrt{p} & \alpha\nu\ e_i \neq 0\ \forall\ i \\ \le (s-t-1)\sqrt{p} & \alpha\nu\ e_i = 0\ \gamma\iota\alpha\ \alpha\kappa\rho\iota\beta\acute{\omega}\varsigma\ t\ \ i \\ = 0 & \alpha\nu\ e_i \neq 0\ \gamma\iota\alpha\ \alpha\kappa\rho\iota\beta\acute{\omega}\varsigma\ \acute{\varepsilon}\nu\alpha\ i \\ = p & \alpha\nu\ e_i = 0\ \ \forall\ i \end{cases}$$

Έτσι

$$S \ge p - \left[\sum_{i=0}^{s-2} \binom{S}{i} (s-i-1)(q-1)^{s-i}\right]\sqrt{p}$$

Συγκρίνοντας με $S \le q^s|A| + sq^{s-1}$ προκύπτει $|A| > 0$ για

$$p - \left[\sum_{i=0}^{s-2} \binom{S}{i} (s-i-1)(q-1)^{s-i}\right]\sqrt{p} - sq^{s-1} > 0$$

Τότε, ο ισχυρισμός ισχύει.

▪

Εφαρμόζοντας το Θεώρημα 3.2 για $s = 5$ θα ισχύει το ακόλουθο πόρισμα.

Πόρισμα 3.1

Έστω p είναι πρώτος $\equiv 1\ (mod\ q)$ με

$$p - [4(q-1)^5 + 15(q-1)^4 + 20(q-1)^3 + 10(q-1)^2]\sqrt{p} - 5q^4 > 0.$$

Τότε, για κάθε δοσμένη s – αδα $(j_1, j_2, \dots, j_s) \in \{0,\ 1, \dots,\ q\ -1\}^s$ και κάθε δοσμένη s - αδα $(c_1, c_2, \dots, c_s)$ του $GF(p)$, υποδηλώνεται ότι θα υπάρχει ένα στοιχείο $x \in GF(p)$ τέτοιο ώστε $x + c_i \in C_{j_i}^q$ για κάθε i.

Λήμμα 3.1

Έστω p πρώτος $\equiv 1\ (mod\ 10)$ και $p > 8.7916 \times 10^7$, τότε θα υπάρχει ένα ζευγάρι (x, y) που πληροί τις προϋποθέσεις (1) - (3) του Λήμματος 2.1.

Απόδειξη:

Έστω i_0 είναι ακέραιος αριθμός τέτοιος ώστε $2 \in C_{i_0}^5$ και $0 \le i_0 \le 4$. Έστω ένα ζευγάρι (x, y) που πληροί τις ακόλουθες δύο προϋποθέσεις:

(a) $x,\ x-1 \in C_1^5,\ x-2 \in C_2^5,\ \frac{x-3}{2},\ 2x-3 \in C_3^5$

(b) $y + \frac{x}{2} \in C_{4-i_0}^5,\ y,\ y+x,\ y - \frac{x-3}{2}$ και $y + 3\frac{x-1}{2}$ ανήκουν σε διακεκριμένες τάξεις $\{C_{2-i_0}^5, C_{3-i_0}^5, C_{4-i_0}^5, C_{3-i_0}^5\}$, όπου όλοι οι δείκτες λαμβάνονται $modulo$ 5.

Είναι εύκολο να δειχθεί ότι ένα τέτοιο ζευγάρι (x, y) πληροί επίσης τις προϋποθέσεις (1) - (3) του Λήμματος 2.1.

Εφόσον, τα $0, -1, -2, -\frac{3}{2}, -3$ είναι διακεκριμένα στοιχεία στο $GF(p)$ (αν $p \ge 11$), σύμφωνα με το Πόρισμα 3.1 για $q = 5$, ένα στοιχείο x που ικανοποιεί την πρώτη προϋπόθεση (a) θα υπάρχει πάντα στο $GF(p)$ για οποιονδήποτε πρώτο $p \equiv 1\ (mod\ 10)$ και $p \ge 8.7916 \times 10^7$. Προφανώς, $x \ne 0, 1, 2, \frac{3}{2}, 3$. Μόλις το στοιχείο $x \in GF(p)$ προσδιοριστεί, μπορεί να εφαρμοστεί και πάλι το Πόρισμα 3.1 για να επιτευχθεί το απαιτούμενο στοιχείο y που ικανοποιεί τον όρο (b) για κάθε πρώτο $p \equiv 1\ (mod\ 10)$ και $p \ge 8.7916 \times 10^7$. Αυτό ολοκληρώνει την απόδειξη.

▪

Λήμμα 3.2

Έστω p πρώτος $\equiv 1\ (mod\ 10)$ και $p > 8.7916 \times 10^7$. Τότε, θα υπάρχει μια $(4p, 4, 5, 1) - DF$.

Απόδειξη:

Το συμπέρασμα προκύπτει από τα Λήμματα 2.1 και 3.1.

▪

Έστω, ότι υπάρχουν κάποια στοιχεία που ικανοποιούν το Λήμμα 2.6 Χρησιμοποιώντας το Θεώρημα 3.1 θα προκύψει το εξής λήμμα:

Λήμμα 3.3

Υποθέτοντας ότι p είναι πρώτος, $p \equiv 11\ (mod\ 20)$ και $p > 1.6 \times 10^7$. Τότε, θα υπάρχει $(4up, 4u, 5, 1) - DF$ για κάθε $u = 1, 2, 3$.

Απόδειξη:

Στόχος για την απόδειξη είναι στο $GF(p)$, $p \equiv 11\ (mod\ 20)$, να βρεθεί ένα στοιχείο x που να ικανοποιεί τις συνθήκες του Λήμματος 2.6.

$g_1(x) = x^3(x-1)$

$g_2(x) = x^3(x+1)$

$g_3(x) = x^6(x^2+x+1)$

Αντίστοιχα, οι συνθήκες μπορούν να διατυπωθούν ως εξής:

(i) $x \in C_i^{10}$, $i \in \{1, 3, 7, 9\}$

(ii) $για$ $k = 1, 2,$ $\quad g_k(x) \in C_0^{10} \cup C_5^{10}$

(iii) $g_3(x) \in C_0^{10}$

Έστω χ δεν είναι κύριος πολλαπλασιαστικός χαρακτήρας τάξης 10. Δηλαδή, $\chi(x) = \theta^t$, εάν $x \in C_t^{10}$ όπου $\theta = e^{\frac{2\pi i}{10}}$ είναι η 10^{η} ρίζα της μονάδας. Έστω

$$A = \chi(x)$$

$$B_k = \chi\big(g_k(x)\big), k = 1, 2, 3$$

Αυτές οι συναρτήσεις έχουν τις παρακάτω τιμές:

$$(1+A)(1-A^5) = \begin{cases} 2\big(1+\theta^i\big), & \alpha\nu\ x \in C_i^{10}, i \in \{1, 3, 7, 9\} \\ 1, & \alpha\nu\ x = 0 \\ 0, & \alpha\nu\ x \notin \{0\} \cup C_1^{10} \cup C_3^{10} \cup C_7^{10} \cup C_9^{10} \end{cases}$$

Για $k = 1, 2$

$$1 + B_k^2 + B_k^4 + B_k^6 + B_k^8 = \begin{cases} 5, & \alpha\nu\ g_k(x) \in C_0^{10} \cup C_5^{10} \\ 1, & \alpha\nu\ g_k(x) = 0 \\ 0, & \alpha\nu\ g_k(x) \notin \{0\} \cup C_0^{10} \cup C_5^{10} \end{cases}$$

και

$$1 + B_3 + B_3^2 + \cdots + B_3^9 = \begin{cases} 10, & \alpha\nu\ g_3(x) \in C_0^{10} \\ 1, & \alpha\nu\ g_3(x) = 0 \\ 0, & \alpha\nu\ g_3(x) \notin \{0\} \cup C_0^{10} \end{cases}$$

Από αυτά, έστω

$$S(x) = (1 + A - A^5 - A^6)(1 + B_1^2 + \cdots + B_1^8)(1 + B_2^2 + \cdots + B_2^8)(1 + B_3 + \cdots + B_3^9)$$

και

$$S = \sum_{x \in GF(p)} S(x)$$

Σχέση (2)

Έστω $X \subset GF(p)$ τέτοια ώστε $S(x) \neq 0$ όταν $x \in X$, και συμβολίζοντας $X_1 = \{x \in X : xg_1(x)g_2(x)g_3(x) = 0\}$ *και* $X_2 = X \backslash X_1$, τότε, το x θα πληροί τις προϋποθέσεις (i), (ii), και (iii) εάν $x \in X_2$, και το άθροισμα $|S|$ είναι:

$$|S| \leq \sum_{x \in X_1} |S(x)| + \sum_{x \in X_2} |S(x)|$$

Το πρώτο άθροισμα συμβολίζεται S_1. Εάν το $x = 0$, τότε $g_1(x) = g_2(x) = g_3(x) = 0$ και η συμβολή του S_1 είναι 1. Αν $x \neq 0$ και $g_k(x) = 0, k = 1, 2$ $\tau\acute{o}\tau\varepsilon$ $x = 1$ ή -1. Από $(1 + A)(1 - A^5)$ στην περίπτωση αυτή, η συμβολή του S_1 είναι 0. Αν $x \neq 0, 1, -1$ και $g_3(x) = 0$, η συμβολή του S_1 είναι το πολύ $2 \times 4 \times 5 \times 5 = 200$. Έτσι, η συμβολή του S_1 είναι το πολύ 201. Αν μπορεί να δειχθεί ότι $|S| > 201$ σε κάποια $GF(p)$, τότε το δεύτερο άθροισμα είναι διάφορο του μηδενός και πρέπει να υπάρχει τουλάχιστον ένα x που πληροί τις προϋποθέσεις (i), (ii), και (iii), δημιουργώντας μια $(4up, 4u, 5, 1) - DF$ για $u = 1, 2, 3$.

Η επέκταση του εσωτερικού γινομένου στη σχέση (2) δίνει:

$$S \geq \sum_{x \in GF(p)} 1 - \sum_{u \in \{1,5,6\}} \left| \sum_{x \in GF(p)} A^u \right| - \sum_{u \in \{0,1,5,6\}} \sum_{0 \leq r_1, r_2 \leq 4} \sum_{\substack{0 \leq r_3 \leq 9 \\ r_1 + r_2 + r_3 > 0}} \left| \sum_{x \in GF(p)} A^u B_1^{2r_1} B_2^{2r_2} B_3^{r_3} \right|$$

Για την εκτίμηση των εσωτερικών αθροισμάτων, μπορεί να χρησιμοποιηθεί το θεώρημα του Weil σε πολλαπλασιαστικούς χαρακτήρες αθροισμάτων.

Υποθέτοντας ότι

$$A^u B_1^{2r_1} B_2^{2r_2} B_3^{r_3} = \chi\big(G(x)\big), r_1 + r_2 + r_3 > 0$$

τότε,

$$G(x) = x^{u+6r_1+6r_2+6r_3}(x-1)^{2r_1}(x+1)^{2r_2}(x^2+x+1)^{r_3}.$$

Αν υπάρχει πολυώνυμο $P(x)$ τέτοιο ώστε $G(x) = [P(x)]^{10}$, τότε

$$x^{u+6r_1+6r_2+6r_3}(x-1)^{2r_1}(x+1)^{2r_2}(x^2+x+1)^{r_3} = P(x)^{10}$$

Εφόσον, $x, x-1, x+1,$ και $x^2+x+1,$ είναι κατά ζεύγη πρώτοι προς αλλήλους, τότε, $r_1 + r_2 + r_3 = 0.$ Από το Θεώρημα 3.1,

$$\left| \sum_{x \in GF(p)} A^u B_1^{2r_1} B_2^{2r_2} B_3^{r_3} \right| \leq 4\sqrt{p}$$

αφού

$$\sum_{x \in GF(p)} A^u = 0$$

τότε

$$|S| \geq p - \sum_{u \in \{0,1,5,6\}} \sum_{0 \leq r_1, r_2 \leq 4} \sum_{\substack{0 \leq r_3 \leq 9 \\ r_1+r_2+r_3 > 0}} (4\sqrt{p})$$

και κατ' επέκταση

$$|S| > 201$$

αν

$$p - 3984\sqrt{p} > 201.$$

Αυτό μπορεί να επιτευχθεί αν $p > 1.6 \times 10^7$. Τότε, το συμπέρασμα προκύπτει.

▪

IV. Κύρια αποτελέσματα

Αποδεικνύεται πρώτα το ακόλουθο.

Λήμμα 4.1

Υποθέτοντας ότι p είναι πρώτος, $p \equiv 1 \,(mod\, 10)$, $11 \leq p \leq 8.7916 \times 10^7$ και $p \notin \{11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 241, 311, 661\}$.

Τότε θα υπάρχει $(4up, 4u, 5, 1) - DF$.

Απόδειξη:

Για κάθε δοσμένο πρώτο p, υπάρχουν στοιχεία x και y στο $GF(p)$ που ικανοποιούν το Λήμμα 2.1. Για $20001 \leq p \leq 8.7916 \times 10^7$ τα στοιχεία x και y στο $GF(p)$ πληρούν το Λήμμα 3.1. Για εξοικονόμηση χώρου παρατίθενται, στον πίνακα Ι οι παράμετροι: πρώτοι p έως το 991, αρχικό στοιχείο w, τα στοιχεία x, y. Σημειώνεται, ότι τα x και y του πίνακα Ι ανταποκρίνονται στο Λήμμα 2.1 και ενδέχεται να μην ικανοποιούν το Λήμμα 3.1.

Πίνακας Ι - Παράμετροι για $11 < p \leq 991$

p	w	x	y	p	w	x	y
11	2	-	-	31	3	-	-
41	6	-	-	61	2	-	-
71	7	-	-	101	2	-	-
131	2	-	-	151	6	-	-
181	2	-	-	191	19	-	-
211	2	20	44	241	7	-	-
251	6	15	31	271	6	82	47
281	3	22	14	311	17	-	-
331	3	54	20	401	3	122	11
421	2	73	373	431	7	250	17
461	2	53	56	491	2	72	165
521	3	4	38	541	2	111	121
571	3	13	45	601	7	48	55
631	3	11	266	641	3	56	180
661	2	-	-	691	3	38	40
701	2	147	178	751	3	39	322
761	6	31	71	811	3	20	37
821	2	8	23	881	3	57	126
911	17	109	18	941	2	102	363
971	6	42	9	991	6	11	95

Λήμμα 4.2

Για $p = 31, 71, 131, 151, 191, 311$, υπάρχει $(4p, 4, 5, 1) - DF$. Δεν υφίσταται $(44, 4, 5, 1) - DF$, όμως υπάρχει βέλτιστος $(44, 5, 1) - OCC$.

Απόδειξη:

Με εξαντλητική έρευνα μέσω του υπολογιστή, δεν υφίσταται η $(44, 4, 5, 1) - DF$, αλλά υπάρχει ο βέλτιστος $(44, 5, 1) - OCC$, τα blocks του οποίου παρατίθενται στη συνέχεια. Για κάθε άλλο πρώτο p, τα blocks βάσης δημιουργούνται από τα ακόλουθα δύο αρχικά block βάσης, σύμφωνα με την πολλαπλασιαστική υποομάδα $C_0^{10} \times \{1\}$.

$p = 11$ $\{0_0, 1_1, 3_3, 6_0, 7_0\}$ $\{0_0, 6_2, 3_2, 2_0, 2_3\}$
$p = 31$ $\{0_0, 1_0, 3_0, 2_1, 10_3\}$ $\{0_0, 7_0, 15_1, 4_2, 12_2\}$
$p = 71$ $\{0_0, 7_0, 49_0, 1_1, 59_2\}$ $\{0_1, 2_0, 58_0, 51_1, 59_2\}$
$p = 131$ $\{0_0, 1_0 3_0, 2_1, 13_3\}$ $\{0_0, 6_0, 15_1, 25_2, 56_2\}$
$p = 151$ $\{0_0, 1_0, 6_0, 3_1, 15_3\}$ $\{0_0, 11_0, 46_1, 71_2, 113_2\}$
$p = 191$ $\{0_0, 1_0, 3_0, 2_1, 10_3\}$ $\{0_0, 4_0, 8_1, 27_2, 153_2\}$
$p = 311$ $\{0_0, 1_0, 101_0, 153_1, 84_2\}$ $\{0_2, 249_0, 79_0, 155_1, 269_1\}$.

▪

Λήμμα 4.3

Για $p = 41, 61, 101, 181, 241, 661$, υπάρχει $(4p, 4, 5, 1) - DF$.

Απόδειξη:

Για $p = 41$, παρατίθενται τα 8 blocks. Για $p = 241$, τα 48 blocks βάσης έχουν ως εξής, όπου $0 \leq i \leq 14$ και $0 \leq j \leq 2$. Για κάθε άλλο πρώτο p, η βάση των blocks παράγεται από τα ακόλουθα τέσσερα αρχικά blocks βάσης, σύμφωνα με την πολλαπλασιαστική υποομάδα $C_0^{20} \times \{1\}$.

$p = 41$ $\{0_0, 15_3, 32_0, 7_0, 26_3\}$ $\{0_0, 20_0, 5_2, 14_0, 39_1\}$
$\{0_0, 21_1, 14_3, 36_1, 13_0\}$ $\{0_0, 1_1, 8_0, 38_3, 18_1\}$
$\{0_0, 2_2, 6_2, 11_3, 5_0\}$ $\{0_0, 3_3, 13_1, 32_1, 21_3\}$
$\{0_0, 12_0, 29_3, 16_1, 39_3\}$ $\{0_0, 14_2, 10_3, 39_0, 38_0\}$
$p = 61$ $\{0_0, 1_0, 3_0, 7_0, 2_1\}$ $\{0_0, 8_0, 5_1, 11_2, 36_2\}$
$\{0_0, 11_0, 34_1, 24_2, 22_3\}$ $\{0_0, 12_0, 20_1, 8_2, 37_3\}$
$p = 101$ $\{0_0, 1_0, 3_0, 16_0, 4_1\}$ $\{0_0, 4_0, 9_1, 1_2, 26_2\}$
$\{0_0, 10_0, 8_1, 33_2, 74_3\}$ $\{0_0, 26_0, 22_1, 73_2, 63_3\}$
$p = 181$ $\{0_0, 1_0, 3_0, 7_0, 2_1\}$ $\{0_0, 8_0, 4_1, 2_2, 22_2\}$
$\{0_0, 13_0, 3_1, 20_2, 46_3\}$ $\{0_0, 24_0, 36_1, 13_2, 90_3\}$
$p = 241$ $\{0_0, 1_0, 2_1, 5_2, 23_2\} \cdot 24_1^i$ $\{0_0, 35_0, 39_1, 188_2, 78_3\} \cdot 24_1^i$
$\{0_0, 2_0, 19_0, 8_1, 24_3\} \cdot 24_1^i$ $\{0_0, 86_0, 90_0, 97_0, 204_0\} \cdot 24_1^i$
$p = 661$ $\{0_0, 1_0, 5_0, 19_0, 3_1\}$ $\{0_0, 7_0, 4_1, 9_2, 17_2\}$
$\{0_0, 16_0, 28_1, 42_2, 105_3\}$ $\{0_0, 28_0, 194_1, 519_2, 75_3\}$

▪

Συνδυάζοντας, λοιπόν , τα Λήμματα 4.1 έως 4.3 και το Λήμμα 3.2, αποδεικνύεται το Θεώρημα 1.1.

Λήμμα 4.4

Υποθέτοντας ότι p είναι πρώτος $p \equiv 1\ (mod\ 20)$, $431 \le p \le 1.6 \times 10^7$ και $p \neq 491, 751, 1451, 1831$.

Τότε, θα υπάρχει $(4up, 4u, 5,1) - DF$ για κάθε $u = 2, 3$.

Απόδειξη:

Για κάθε δοσμένο πρώτο p, θα υπάρχει ένα στοιχείο x στο $GF(p)$ που θα ικανοποιεί το Λήμμα 2.6. Παρατίθενται στον πίνακα ΙΙ οι ακόλουθοι παράμετροι: πρώτος p, αρχικό στοιχείο w, τον δείκτη i για $x \in C_i$, και τα j, s, h για $T(j, s, h)$ στο Λήμμα 2.6. . Για εξοικονόμηση χώρου παραθέτονται μόνο μικροί πρώτοι έως το 2011.

Πίνακας ΙΙ - Παράμετροι για $431 < p \le 2011$

p	w	x	i	(j, s, h)
431	7	136	1	(2, 7, 4)
491	2	-		
571	3	88	3	(7, 7, 4)
631	3	140	1	(2, 7, 4)
691	3	70	3	(2, 2, 4)
751	3	-		
811	3	466	9	(2, 2, 4)
911	17	727	9	(2, 7, 4)
971	6	30	3	(7, 7, 4)
991	6	177	7	(7, 7, 4)
1031	14	910	9	(2, 7, 4)
1051	7	333	1	(2, 4, 4)
1091	2	882	7	(2, 7, 4)
1151	17	377	7	(2, 2, 4)
1171	2	416	1	(7, 7, 4)
1231	3	1169	3	(7, 2, 4)
1291	2	1166	1	(2, 2, 4)
1451	2	-		
1471	6	1094	7	(7, 2, 4)
1511	11	229	1	(2, 7, 4)
1531	2	1525	3	(7, 7, 4)
1571	2	595	3	(2, 2, 4)
1811	6	24	1	(2, 2, 4)
1831	3	-		
1871	14	311	7	(2, 2, 4)
1931	2	1798	3	(7, 7, 4)
1951	3	369	1	(2, 2, 4)
2011	3	1814	7	(7, 7, 4)

Λήμμα 4.5

Αν $T(x) = (7, 3, 7)$, τότε θα υπάρχει $(4up, 4u, 5,1) - DF$ για οποιοδήποτε $u = 2, 3$.

Απόδειξη:

Για $u = 2, 3$ παρατίθεται η λίστα που αντιστοιχεί στα αρχικά blocks βάσης όπως στο Λήμμα 2.2.

$u = 2$ $\{0_2, x_0, x_0^2, x_0^4, x_1^3\}$, $\{0_0, x_0^4, x_1^6, x_3^7, x_5^5\}$
$\{0_3, x_4^7, x_5^5, x_0^6, x_0^8\}$, $\{0_0, x_1^2, x_2, 1_4, x_6^3\}$
$u = 3$ $\{0_0, x_0^5, x_1^3, x_2^4, x_5^2\}$, $\{0_0, x_0^2, x_1^4, x_3, x_5^3\}$, $\{0_0, x_0^4, x_1^5, x_5^6, x_7^3\}$
$\{0_0, x_0^3, x_2^5, x_3^4, x_8^2\}$, $\{0_0, x_0, x_3^2, x_4^3, 1_6\}$, $\{0_0, x_1^7, x_3^6, x_5^5, x_9^4\}$

▪

Λήμμα 4.6

Για $p = 251, 311, 491, 751, 1451, 1831,$ υπάρχει $(4up, 4u, 5,1) - DF$, για οποιαδήποτε $u = 2, 3$.

Απόδειξη:

Για κάθε πρώτο p, εφαρμόζεται το Λήμμα 4.5 με $(j, s, h) = (7, 3, 7)$ και τις ακόλουθες παραμέτρους

$p = 251$ $w = 6$ $x = 43$ $i = 7$
$p = 311$ $w = 17$ $x = 153$ $i = 9$
$p = 491$ $w = 2$ $x = 90$ $i = 7$
$p = 751$ $w = 3$ $x = 136$ $i = 7$
$p = 1451$ $w = 2$ $x = 265$ $i = 9$
$p = 1831$ $w = 3$ $x = 864$ $i = 3$

▪

Υπάρχουν ωστόσο και μερικοί πρώτοι που δεν έχουν εξεταστεί, οι οποίοι είναι οι $11, 31, 71, 131, 151, 191, 211, 271, 331$.

Δύο από τους οποίους μπορούν να εξεταστούν ομοιόμορφα.

Λήμμα 4.7

Για $p = 71,$ υπάρχει $(4up, 4u, 5, 1) - DF$ για κάθε $u = 2, 3$.

Απόδειξη:

Για τις παραμέτρους $w = 7, x = 7, i = 1$ $και$ $(j, s, h) = (2, 8, 2)$ και τα αρχικά blocks βάσης, θα είναι:

$u = 2,$ $\{0_0, x_0^5, x_0^6, x_1^7, x_6^4\}$ $\{0_0, x_0^3, x_1^2, x_4^5, x_5^4\}$
$\{0_0, x_0^4, x_2, x_3^2, x_6^3\}$ $\{0_0, 1_1, x_2^3, x_3, x_6^2\}$
$u = 3,$ $\{0_0, x_0^2, x_0^3, x_2, x_3^4\}$ $\{0_0, x_0^5, x_1^3, x_5^2, x_7^4\}$ $\{0_3, x_8^7, x_0^4, x_0^5, x_2^6\}$
$\{0_0, x_1^6, x_2^9, x_4^8, x_8^7\}$ $\{0_0, x_1^4, x_3^3, x_5^5, x_6^6\}$ $\{0_0, x_1^2, x_4, x_7^3, 1_8\}$

▪

Λήμμα 4.8

Για $p = 271$, υπάρχει $(4up, 4u, 5, 1) - DF$ για κάθε $u = 2, 3$.

Απόδειξη:

Για τις παραμέτρους $w = 6, x = 52, i = 3$ $και$ $(j, s, h) = (7, 2, 9)$ και τα αρχικά blocks βάσης, θα είναι:

$u = 2,$ $\{0_0, x_0^6, x_0^8, x_1^5, x_2^7\}$ $\{0_1, x_3^2, x_5^4, x_0^3, x_0^5\}$
$\{0_3, x_4, 1_2, x_0^2, x_0^3\}$ $\{0_0, x_2^3, x_4^2, x_6^5, x_0^4\}$
$u = 3,$ $\{0_0, x_0^2, x_0^5, x_1^3, x_2^4\}$ $\{0_0, x_0^4, x_1^5, x_3^3, x_7^6\}$ $\{0_3, x_0, x_3^2, 1_4, x_8^3\}$
$\{0_0, x_1^6, x_3^7, x_6^8, x_8^9\}$ $\{0_0, x_1^8, x_4^7, x_6^6, x_7^9\}$ $\{0_0, x_2^2, x_4^3, x_6^4, x_9^5\}$

▪

Λήμμα 4.9

Για $p = 11, 31, 131, 151, 191, 211, 331$, υπάρχει η $(8p, 8, 5, 1) - DF$.

Απόδειξη:

Για κάθε δοσμένο πρώτο p, τα blocks βάσης δημιουργούνται από τα ακόλουθα δύο αρχικά blocks βάσης, σύμφωνα με την πολλαπλασιαστική υποομάδα $C_0^{10} \times \{1\}$.

$p = 11$ $\{0_0, 2_0, 6_0, 1_2, 4_7\}$ $\{0_0, 3_0, 5_3, 2_5, 6_7\}$
$\{0_4, 4_5, 5_6, 7_0, 8_0\}$ $\{0_0, 7_3, 2_4, 5_5, 1_7\}$
$p = 31$ $\{0_0, 1_0, 3_0, 2_1, 4_6\}$ $\{0_0, 4_0, 7_1, 1_4, 15_5\}$
$\{0_0, 8_0, 15_2, 11_3, 17_6\}$ $\{0_0, 16_1, 2_2, 14_3, 6_6\}$
$p = 131$ $\{0_0, 1_0, 3_0, 2_1, 5_6\}$ $\{0_0, 6_0, 3_1, 1_4, 7_5\}$
$\{0_0, 9_0, 1_2, 12_3, 115_6\}$ $\{0_0, 13_1, 110_2, 44_3, 84_6\}$
$p = 151$ $\{0_0, 1_0, 6_0, 3_1, 4_6\}$ $\{0_0, 11_0, 7_1, 1_4, 10_5\}$
$\{0_0, 15_0, 5_2, 89_6, 26_3\}$ $\{0_0, 11_1, 65_2, 40_3, 100_6\}$
$p = 191$ $\{0_0, 1_0, 3_0, 2_1, 4_6\}$ $\{0_0, 4_0, 7_1, 1_4, 28_5\}$
$\{0_0, 8_0, 1_2, 9_3, 29_6\}$ $\{0_0, 21_1, 110_2, 184_3, 86_6\}$
$p = 211$ $\{0_0, 1_0, 3_0, 2_1, 4_6\}$ $\{0_0, 4_0, 7_1, 1_4, 5_5\}$
$\{0_0, 6_0, 4_2, 10_3, 55_6\}$ $\{0_0, 9_1, 123_2, 44_3, 192_6\}$
$p = 331$ $\{0_0, 1_0, 4_0, 2_1, 5_6\}$ $\{0_0, 8_0, 4_1, 6_4, 22_5\}$
$\{0_0, 16_0, 1_2, 33_3, 18_6\}$ $\{0_0, 20_1, 110_2, 80_3, 290_6\}$

▪

Λήμμα 4.10

Για $p = 11, 31, 131, 151, 191, 211, 331$, υπάρχει η $(12p, 12, 5, 1) - DF$.

Απόδειξη:

Για κάθε δοσμένο πρώτο p, είναι τα blocks βάσης δημιουργούνται από τα ακόλουθα δύο αρχικά blocks βάσης, σύμφωνα με την πολλαπλασιαστική υποομάδα $C_0^{10} \times \{1\}$.

$p = 11$ $\{0_0, 1_0, 3_0, 7_3, 5_{10}\}$ $\{0_0, 5_0, 3_3, 8_4, 4_{11}\}$
$\{0_0, 7_0, 8_3, 5_5, 3_{11}\}$ $\{0_0, 3_2, 2_3, 6_9, 1_{10}\}$
$\{0_6, 5_8, 1_0, 4_1, 2_2\}$ $\{0_4, 2_6, 6_8, 5_{11}, 7_0\}$
$p = 31$ $\{0_0, 1_0, 3_0, 2_2, 4_3\}$ $\{0_0, 4_0, 1_1, 2_5, 9_7\}$
$\{0_0, 8_0, 11_2, 6_3, 13_8\}$ $\{0_0, 11_1, 28_2, 19_4, 2_8\}$

	$\{0_0, 14_1, 22_3, 3_5, 7_6\}$	$\{0_0, 21_1, 23_4, 3_7, 16_8\}$
$p = 131$	$\{0_0, 1_0, 3_0, 2_2, 5_3\}$	$\{0_0, 6_0, 1_1, 2_5, 8_7\}$
	$\{0_0, 9_0, 3_2, 1_3, 4_8\}$	$\{0_0, 6_1, 5_2, 2_4, 15_8\}$
	$\{0_0, 10_1, 110_3, 9_5, 70_6\}$	$\{0_0, 12_1, 97_4, 52_7, 40_8\}$
$p = 151$	$\{0_0, 1_0, 6_0, 3_2, 4_3\}$	$\{0_0, 11_0, 3_1, 1_5, 6_7\}$
	$\{0_0, 15_0, 7_2, 22_3, 3_8\}$	$\{0_0, 5_1, 22_2, 39_4, 40_8\}$
	$\{0_0, 7_1, 60_3, 114_5, 70_6\}$	$\{0_0, 11_1, 117_4, 65_7, 102_8\}$
$p = 191$	$\{0_0, 1_0, 3_0, 2_2, 4_3\}$	$\{0_0, 4_0, 1_1, 2_5, 9_7\}$
	$\{0_0, 8_0, 4_2, 2_3, 5_8\}$	$\{0_0, 3_1, 16_2, 24_4, 34_8\}$
	$\{0_0, 4_1, 61_3, 49_5, 171_6\}$	$\{0_0, 21_1, 61_4, 44_7, 117_8\}$
$p = 211$	$\{0_0, 1_0, 3_0, 2_2, 4_3\}$	$\{0_0, 4_0, 1_1, 2_5, 5_7\}$
	$\{0_0, 6_0, 4_2, 2_3, 3_8\}$	$\{0_0, 3_1, 7_2, 2_4, 13_8\}$
	$\{0_0, 6_1, 19_3, 56_5, 119_6\}$	$\{0_0, 7_1, 105_4, 150_7, 146_8\}$
$p = 331$	$\{0_0, 1_0, 4_0, 2_2, 5_3\}$	$\{0_0, 8_0, 1_1, 2_5, 10_7\}$
	$\{0_0, 16_0, 4_2, 8_3, 7_8\}$	$\{0_0, 8_1, 19_2, 2_4, 36_8\}$
	$\{0_0, 13_1, 7_3, 41_5, 254_6\}$	$\{0_0, 16_1, 54_4, 17_7, 50_8\}$

▪

Συνδυάζοντας το Λήμμα 3.3 και τα Λήμματα 4.4 έως 4.10 αποδεικνύεται το Θεώρημα 1.2.

Παρατήρηση

Για $p \equiv 11\ (mod\ 20)$ και $u = 1$, υπάρχουν επίσης αρχικά blocks βάσης με τα ίδια x, i $και$ (j, s, h) όπως στα Λήμματα 4.4 έως 4.8.

V. Συμπέρασμα

Εφόσον, ορίστηκε η ύπαρξη $(4p, 4, 5, 1) - DF$, θα μπορούσε κανείς να ελπίζει ότι η ύπαρξη $(4up, 4u, 5, 1) - DF$ για $u = 2, 3$ μπορεί να καθοριστεί ομοίως. Εφόσον, οι $(4up, 4u, 5, 1) - DFs$ πραγματοποιούνται ομοιόμορφα για $p \equiv 1\ (mod\ 20)$ και $u = 1, 2, 3$, τότε θα μπορούσε να υπάρχει ελπίδα υλοποίησης και με $u = 4$. Σε αυτή την περίπτωση, οκτώ αρχικά blocks βάσης είναι απαραίτητα για κάθε p.

Για $4u \leq 20$, $u = 5$ μπορεί επίσης να εξεταστεί. Ωστόσο, η ύπαρξη $(4p, 4, 5, 1) - DF$ προϋποθέτει την ύπαρξη της $(20p, 20, 5, 1) - DF$ από Buratti [6, Πόρισμα 5.10]. Το ακόλουθο θεώρημα μπορεί να επικρατήσει περισσότερο από το Θεώρημα 1.1, όταν η $(20 \times 11, 20, 5, 1) - DF$ κατασκευαστεί στο $\mathbb{Z}_{220}$, με τα 10 blocks βάσης που αναφέρονται παρακάτω.

0	40	118	181	210	0	25	101	107	215	0	18	111	149	158
0	95	122	123	179	0	19	26	91	178	0	16	24	36	59
0	53	67	70	104	0	54	86	171	216	0	13	15	96	160
0	21	52	126	172										

Θεώρημα 5.1

Για κάθε $p \equiv 1\ (mod\ 10)$, υπάρχουν $(20p, 20, 5, 1) - DF$ και βέλτιστος $(20p, 5, 1) - OCC$.

Τέλος, πρέπει να αναφερθεί ότι η $(4p, 4, 5, 1) - DF$ είναι απολύτως ισοδύναμη με τον $(4p + 1, 5, 1) - BIBD$.

Βιβλιογραφία

[1] E. F. Brickell and V. K. Wei, Optical orthogonal codes and cyclic block designs, Congr Numer 58 (1987), 175–192.

[2] F. P. K. Chung, J. A. Salehi, and V. K. Wei, Optical orthogonal codes: Design, analysis, and applications, IEEE Trans Inform Theory 35 (1989), 595–604.

[3] M. Buratti, Recursive constructions for difference matrices and relative difference families, J Combin Designs 6 (1998), 165–182.

[4] Y. Tang and J. Yin, Combinatorial constructions for a class of optimal optical orthogonal codes, Sci China Ser A 45 (2002), 1268–1275.

[5] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math 11 (1975), 255–369.

[6] M. Buratti, Constructions of (q,k,1) difference families with q a prime power and k= 4, 5, Discrete Math 138 (1995), 169–175.

[7] K. Chen and L. Zhu, Existence of (q,k,1) difference families with q a prime power and k= 4, 5, J Combin Designs 7 (1999), 21–30.

[8] M. Buratti, Some constructions for 1-rotational BIBD's with block-size 5, Australas J Combin 17 (1998), 199–227

[9] R. Lidl and H. Niederreiter, Finite fields, Cambridge, UK: Cambridge University Press, 1997.

[10] M. Buratti, unpublished communication.