

Μεταπτυχιακή Εργασία
Δ.Μ.Π.Σ. “Εφαρμοσμένες Μαθηματικές Επιστήμες ”

Ο Κβαντικός και ο Twisted Κβαντικός Μετασχηματισμός Fourier Εφαρμογές στην Κβαντική Πληροφορική

Χρυσούλα Βλάχου

Επιβλέπων Καθηγητής: Εμμανουήλ Φλωράτος

Επιτροπή
Αλέξανδρος Αρβανιτάκης (ΕΜΠ)
Εμμανουήλ Φλωράτος (ΕΚΠΑ)
Παναγιώτης Ψαρράκος (ΕΜΠ)

Χειμερινό Εξάμηνο 2013-2014



Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
Τομέας Μαθηματικών
Αθήνα, 2014

Περίληψη

Τις τελευταίες δεκαετίες ο κλάδος της Κβαντικής Πληροφορικής αποτελεί πεδίο συστηματικής έρευνας, με στόχο το σχεδιασμό κβαντικών αλγορίθμων και υπολογιστών που θα επιλύουν με αποτελεσματικό τρόπο προβλήματα τα οποία είναι πρακτικώς άλυτα από τους κλασικούς υπολογιστές. Σκοπός της συγκεκριμένης εργασίας είναι να αναδείξει τον τρόπο με τον οποίο τα Μαθηματικά εφαρμόζονται στο σύγχρονο αυτό πεδίο, μέσω της μελέτης του κβαντικού μετασχηματισμού Fourier (και της twisted παραλλαγής του), ο οποίος αποτελεί τη βάση πολλών κβαντικών αλγορίθμων.

Στο πρώτο της μέρος περιγράφουμε το μαθηματικό φορμαλισμό της Κβαντομηχανικής και εισάγουμε τον κβαντικό μετασχηματισμό Fourier, ως το κβαντικό ανάλογο του κλασικού διακριτού μετασχηματισμού Fourier. Θεωρούμε τον πίνακα της αναπαράστασής του σε κατάλληλο χώρο Hilbert και βάσει αυτού αποδεικνύουμε βασικές του ιδιότητες. Ασχολούμαστε επίσης, με το πρόβλημα της διαγωνοποίησής του και παραθέτουμε μία αναλυτική μέθοδο προσδιορισμού των ιδιοτιμών και των ιδιοανυσμάτων του, την οποία εφαρμόζουμε στην περίπτωση του μετασχηματισμού Fourier διάστασης 5. Στα δύο τελευταία κεφάλαια του πρώτου μέρους αναφερόμαστε στον Twisted κβαντικό μετασχηματισμό Fourier, αναδεικνύοντας τη σχέση του με τον προηγούμενο και αναπτύσσοντας την αντίστοιχη μαθηματική διερεύνηση σχετικά με τις ιδιότητες και τη διαγωνοποίησή του.

Στο δεύτερο μέρος της εργασίας, μετά από μία γενική εισαγωγή στην Κβαντική Πληροφορική, παρουσιάζουμε τις σημαντικότερες εφαρμογές του κβαντικού αλγορίθμου που υπολογίζει τον μετασχηματισμό Fourier. Βασιζόμενοι στις μαθηματικές του ιδιότητες καταλήγουμε στην παραγοντοποιημένη μορφή του, η οποία μας επιτρέπει στη συνέχεια να σχεδιάσουμε τα κβαντικά κυκλώματα που τον υλοποιούν. Τέλος, ακολουθώντας την ίδια αποδεικτική διαδικασία, παράγουμε την αντίστοιχη παραγοντοποιημένη μορφή του Twisted κβαντικού μετασχηματισμού Fourier και σχεδιάζουμε τα κατάλληλα κβαντικά κυκλώματα.

Abstract

During the last decades, Quantum Information is a field of systematic research, as it promises the development of quantum algorithms and computers which will efficiently solve problems that, practically, cannot be solved on a classical computer. The object of this assignment is to highlight the way in which Mathematics apply to this modern area of research, throughout the study of the quantum Fourier transform (and its twisted variant), which lies on the basis of many quantum algorithms.

In the first part we describe the mathematical formalism of Quantum Mechanics and we introduce the quantum Fourier transform as the quantum analogue of the classical discrete Fourier transform. We consider its matrix representation in the respective Hilbert space and using this, we prove some basic properties. We also deal with the problem of its diagonalization and we present an analytical method for finding its eigenvalues and eigenvectors, which we implement in the case of the Fourier transform of dimension 5. In the last two chapters of the first part we study the twisted quantum Fourier transform, showing its relation to the previous one and developing the same mathematical investigation concerning its properties and diagonalization.

In the second part of this report, after a brief introduction to Quantum Information, we feature the most important applications of the quantum algorithm which computes the quantum Fourier transform. Using its mathematical properties we end up with its factorized form that enables us to design the quantum circuits. Finally, following the same method we produce the respective factorized form of the twisted quantum Fourier transform and we design the quantum circuits that implement it.

Περιεχόμενα

Εισαγωγή	7
I. Μαθηματική Μελέτη του κβαντικού μετασχηματισμού Fourier και του Twisted κβαντικού μετασχηματισμού Fourier	9
1. Ο μαθηματικός φορμαλισμός της Κβαντομηχανικής	9
1.1. Χώροι Hilbert	9
1.2. Οι χώροι Hilbert στην Κβαντομηχανική	15
2. Μορφή και ιδιότητες του μετασχηματισμού Fourier	17
3. Ιδιοανύσματα και Ιδιοτιμές του μετασχηματισμού Fourier	21
3.1. Ιδιοτιμές του μετασχηματισμού Fourier	21
3.2. Ιδιοανύσματα του μετασχηματισμού Fourier	24
3.3. Εφαρμογή για $N=5$	31
4. Μορφή και ιδιότητες του Twisted μετασχηματισμού Fourier	36
5. Ιδιοτιμές και ιδιοανύσματα του Twisted μετασχηματισμού Fourier	40
5.1. Εφαρμογή για $N = 2$	46
5.2. Σχέση μεταξύ των ιδιοανυσμάτων του μετασχηματισμού Fourier και του Twisted μετασχηματισμού Fourier	48
II. Ο κβαντικός μετασχηματισμός Fourier και ο Twisted κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική	51
6. Σύντομη εισαγωγή στην Κβαντική Πληροφορική	51
6.1. Γενικά περί Κβαντικής Πληροφορικής	51
6.2. Κβαντικά bits (qubits), κβαντικές πύλες και κβαντικά κυκλώματα	53
6.2.1. Κβαντικά bits (qubits)	53
6.2.2. Κβαντικές πύλες	55

6.2.3. Κβαντικά Κυκλώματα	59
7. Ο κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληρο- φορική	61
7.1. Εφαρμογές του κβαντικού αλγορίθμου	61
7.2. Παραγοντοποίηση του κβαντικού μετασχηματισμού Fourier	63
7.3. Κβαντικά Κυκλώματα που υλοποιούν τον κβαντικό μετασχηματι- σμό Fourier	67
8. Ο Twisted κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική	72
8.1. Παραγοντοποίηση του Twisted κβαντικού μετασχηματισμού Fourier	72
8.2. Κβαντικά Κυκλώματα που υλοποιούν τον Twisted κβαντικό με- τασχηματισμό Fourier	73

Εισαγωγή

Ένας πολύ αποτελεσματικός τρόπος για να λύσουμε ένα πρόβλημα στα Μαθηματικά,τη Φυσική ή την Επιστήμη των Υπολογιστών είναι να το μετασχηματίσουμε σε κάποιο άλλο πρόβλημα του οποίου η λύση είναι ήδη γνωστή.Υπάρχουν κάποιοι βασικοί μετασχηματισμοί που εμφανίζονται συχνά ακόμα και σε πολύ διαφορετικό πλαίσιο,οπότε η μελέτη τους αποκτά ιδιαίτερη σημασία.Μια σπουδαία ανακάλυψη της Κβαντικής Πληροφορικής είναι ότι ορισμένοι από αυτούς τους μετασχηματισμούς υπολογίζονται πολύ πιο γρήγορα σε έναν κβαντικό υπολογιστή παρά σε έναν κλασικό και με τον τρόπο αυτό διευκολύνθηκε ο σχεδιασμός γρήγορων αλγορίθμων για κβαντικούς υπολογιστές.Ένας τέτοιος μετασχηματισμός είναι ο διακριτός μετασχηματισμός Fourier ο οποίος υπολογίζεται μέσω του κλασικού αλγορίθμου του γρήγορου μετασχηματισμού Fourier(Fast Fourier Transform).Το κβαντικό του ανάλογο είναι ο κβαντικός μετασχηματισμός Fourier που βρίσκεται στη βάση πολλών κβαντικών αλγορίθμων με ιδιαίτερο ενδιαφέρον.

Το βασικό αντικείμενο της συγκεκριμένης εργασίας είναι η μελέτη του μετασχηματισμού αυτού με σκοπό να αναδειχθεί ο τρόπος με τον οποίο τα Μαθηματικά εφαρμόζονται στο σύγχρονο πεδίο της Κβαντικής Πληροφορικής.Στο πρώτο της μέρος μελετάμε εκείνες τις μαθηματικές ιδιότητες του κβαντικού μετασχηματισμού Fourier και του Twisted κβαντικού μετασχηματισμού Fourier (γενίκευση του Fourier σε ανεξάρτητα συστήματα) που επιτρέπουν την εφαρμογή τους στην Κβαντική Πληροφορική,η οποία παρουσιάζεται στο δεύτερο μέρος.

Πιο συγκεκριμένα,στο πρώτο μέρος περιγράφουμε το μαθηματικό φορμαλισμό της Κβαντομηχανικής και στη συνέχεια εισάγουμε τον κβαντικό μετασχηματισμό Fourier,ως το κβαντικό ανάλογο του γνωστού διακριτού μετασχηματισμού Fourier.Θεωρούμε τον πίνακα της αναπαράστασής του σε κατάλληλο χώρο Hilbert και βάσει αυτού αποδεικνύουμε βασικές του ιδιότητες.Ασχολούμαστε επίσης,με το πρόβλημα της διαγωνοποίησής του και παραθέτουμε μία αναλυτική μέθοδο προσδιορισμού των ιδιοτιμών και των ιδιοανυσμάτων του,την οποία εφαρμόζουμε στην περίπτωση του μετασχηματισμού Fourier διάστασης 5.Στα δύο τελευταία κεφάλαια του πρώτου μέρους αναφερόμαστε στον Twisted κβαντικό μετασχηματισμό Fourier,αναδεικνύοντας τη σχέση του με τον προηγούμενο και αναπτύσσοντας την αντίστοιχη μαθηματική διερεύνηση σχετικά με τις ιδιότητες και τη διαγωνοποίησή του.

Στο δεύτερο μέρος της εργασίας,μετά από μία σύντομη γενική εισαγωγή στην Κβαντική Πληροφορική,παρουσιάζουμε τις σημαντικότερες εφαρμογές του κβαντικού αλγορίθμου που υπολογίζει τον μετασχηματισμό Fourier και βασιζόμενοι

στις μαθηματικές του ιδιότητες καταλήγουμε στην παραγοντοποιημένη μορφή του, η οποία μας επιτρέπει να σχεδιάσουμε τα χβαντικά κυκλώματα που τον υλοποιούν. Τα χβαντικά αυτά κυκλώματα συμπεριλαμβάνονται σε ξεχωριστή ενότητα του ίδιου κεφαλαίου. Τέλος, ακολουθώντας την ίδια αποδεικτική διαδικασία, παράγουμε την αντίστοιχη παραγοντοποιημένη μορφή του Twisted χβαντικού μετασχηματισμού Fourier που διευκολύνει την υλοποίησή του από χβαντικά κυκλώματα, τα οποία και έχουμε σχεδιάσει.

Μέρος I.

Μαθηματική Μελέτη του κβαντικού μετασχηματισμού Fourier και του Twisted κβαντικού μετασχηματισμού Fourier

1. Ο μαθηματικός φορμαλισμός της Κβαντομηχανικής

1.1. Χώροι Hilbert

Ορισμός 1. *Χώρος Hilbert* H καλείται ένας πραγματικός ή μιγαδικός χώρος εσωτερικού γινομένου $\langle \cdot, \cdot \rangle$, ο οποίος είναι πλήρης ως προς το εσωτερικό του γινόμενο.

Στην Κβαντομηχανική μας ενδιαφέρουν οι χώροι Hilbert επί των μιγαδικών αριθμών, οπότε λέγοντας ότι ο H είναι μιγαδικός χώρος εσωτερικού γινομένου, εννοούμε ότι είναι ένας διανυσματικός χώρος στον οποίο υπάρχει ένα εσωτερικό γινόμενο $\langle x, y \rangle$ που αντιστοιχίζει ένα μιγαδικό αριθμό σε κάθε ζεύγος στοιχείων $x, y \in H$ και ικανοποιεί τις παρακάτω ιδιότητες:

- $\langle x, y \rangle = \langle y, x \rangle^*$, όπου το $*$ συμβολίζει το μιγαδικό συζυγές.
- $\langle ax_1 + bx_2, y \rangle = a\langle x_1, y \rangle + b\langle x_2, y \rangle, \forall a, b \in \mathbb{C}$.
- $\langle x, x \rangle \geq 0$, με την ισότητα να ισχύει για $x = 0$.
- $\langle x, ay_1 + by_2 \rangle = a^*\langle x, y_1 \rangle + b^*\langle x, y_2 \rangle, \forall a, b \in \mathbb{C}$.

Οι χώροι Hilbert, όπως γνωρίζουμε, είναι απειροδιάστατοι, στην Κβαντομηχανική, όμως, χρησιμοποιούμε τον όρο χώρος Hilbert και για χώρους πεπερασμένων διαστάσεων με τις ίδιες ιδιότητες. Συνεπώς, η έννοια της ορθοκανονικής βάσης από τη Γραμμική Άλγεβρα, γενικεύεται στην περίπτωση ενός χώρου Hilbert πεπερασμένης διάστασης.

Ορισμός 2. Σε έναν χώρο Hilbert H , **ορθοκανονική βάση** είναι μια οικογένεια $\{e_k\}_{k \in B}$, $B \subset \mathbb{N}$, στοιχείων του H που ικανοποιούν τις εξής συνθήκες:

- **Ορθογωνιότητα:** $\langle e_k, e_j \rangle = 0, \forall k, j \in B \text{ με } k \neq j$.
- **Κανονικότητα:** $\langle e_k, e_k \rangle = \|e_k\|^2 = 1 \Rightarrow \|e_k\| = 1, \forall k \in B$.
- **Πληρότητα:** Η γραμμική θήκη της οικογένειας $\{e_k\}_{k \in B}$ είναι πυκνή στον H .

Ισχύει η παρακάτω πρόταση:

Πρόταση 1. Κάθε στοιχείο του H γράφεται μοναδικά σαν γραμμικός συνδυασμός των στοιχείων της ορθοκανονικής βάσης του, δηλαδή υπάρχουν μοναδικοί μη-μηδενικοί $c_1, c_2, \dots, c_k \in \mathbb{C}$ τέτοιοι ώστε κάθε $x \in H$ να γράφεται στη μορφή:

$$x = \sum_{k=1}^N c_k e_k,$$

όπου N η διάσταση του χώρου Hilbert.

Εάν ο χώρος μας είναι άπειρης διάστασης έχουμε την έννοια της βάσης Hamel που γενικεύεται σε χώρους Hilbert και τότε κάθε στοιχείο του χώρου θα γράφεται σαν το άθροισμα μιας άπειρης σειράς λόγω πληρότητας, ενώ η ορθογωνιότητα εξασφαλίζει ότι αυτή η μορφή θα είναι μοναδική.

Συνεχίζουμε παρουσιάζοντας βασικά στοιχεία για τους τελεστές σε χώρους Hilbert.

Οι συνεχείς γραμμικοί τελεστές $A : H_1 \rightarrow H_2$ από έναν χώρο Hilbert H_1 σε έναν άλλο H_2 είναι φραγμένοι, υπό την έννοια ότι απεικονίζουν φραγμένα σύνολα του H_1 σε φραγμένα σύνολα του H_2 . Ο χώρος τέτοιων φραγμένων γραμμικών τελεστών είναι εφοδιασμένος με τη νόρμα:

$$\|A\| = \sup\{\|Ax\|, \|x\| \leq 1\} \quad (1)$$

Το άθροισμα και η σύνθεση δύο φραγμένων γραμμικών τελεστών είναι επίσης φραγμένος γραμμικός τελεστής.

Για κάποιο στοιχείο $y \in H_2$ η απεικόνιση που στέλνει κάποιο $x \in H_1$ στο $\langle Ax, y \rangle$ είναι γραμμική και συνεχής και από το θεώρημα αναπαράστασης του Riesz λαμβάνουμε:

$$\langle x, A^\dagger y \rangle = \langle Ax, y \rangle,$$

για κάποιο διάνυσμα $A^\dagger y \in H_1$. Με τον τρόπο αυτό ορίζεται ο φραγμένος γραμμικός τελεστής $A^\dagger : H_2 \rightarrow H_1$, ο οποίος καλείται ερμιτιανός συζυγής του A .

Το σύνολο $B(H)$ όλων των φραγμένων γραμμικών τελεστών, μαζί με τις πράξεις της πρόσθεσης και της σύνθεσης, τη νόρμα που δίνεται από την (1) και την ενέλιξη \dagger είναι μία C^* -άλγεβρα.

Ένα στοιχείο A του $B(H)$ καλείται:

- Αυτοσυζυγές ή Ερμιτιανό, εάν $A^\dagger = A$.
- Φυσιολογικό, εάν $A^\dagger A = AA^\dagger$.
- Μοναδιαίο, εάν $A^\dagger A = AA^\dagger = I$, όπου I ο ταυτοτικός τελεστής.

Για φραγμένους τελεστές σε χώρους Hilbert πεπερασμένης διάστασης N ισχύει το **φασματικό θεώρημα**:

Θεώρημα 1. Έστω A φραγμένος τελεστής σε χώρο Hilbert H πεπερασμένης διάστασης, δηλαδή $A \in B(H)$ με $\dim H = N < +\infty$ και $\lambda_1, \lambda_2, \dots, \lambda_N$ οι διάφορες ανά δύο ιδιοτιμές του A . Έστω, επίσης $V_i, 1 \leq i \leq N$ οι αντίστοιχοι ιδιόχωροι και $B(i)$ η ορθή προβολή επί του V_i . Τότε τα επόμενα είναι ισοδύναμα:

$$(1) V_i \perp V_j, \text{ αν } i \neq j \text{ και } \sum_{i=1}^N V_i = H$$

$$(2) B(i) \perp B(j), \text{ αν } i \neq j, \sum_{i=1}^N B(i) = I \text{ και } A = \sum_{i=1}^N \lambda_i B(i)$$

$$(3) A^\dagger A = AA^\dagger$$

Κλείνοντας την ενότητα αυτή θα αναφερθούμε στο τανυστικό γινόμενο χώρων Hilbert. Για να το ορίσουμε είναι απαραίτητο να ορίσουμε πρώτα το τανυστικό γινόμενο διανυσμάτων σε γραμμικούς διανυσματικούς χώρους, γενικά. Επίσης, θα το ορίσουμε για γραμμικές απεικονίσεις και πινάκες και θα αναφέρουμε κάποιες βασικές του ιδιότητες που θα μας χρειαστούν. Εν γένει το τανυστικό γινόμενο ορίζεται και για τοπολογικούς χώρους, άλγεβρες, τετραγωνικές μορφές κ.ά., τα οποία όμως είναι εκτός του πλαισίου της συγκεκριμένης εργασίας.

Ορισμός 3. Έστω X, Y δύο διανυσματικοί χώροι και V, W δύο υπόχωροί τους, αντίστοιχα. Ορίζουμε στον V μια σχέση ισοδυναμίας R , ως εξής:

$$a \sim b \Leftrightarrow a - b \in R$$

$$[a]_{\sim} = a + R$$

Θεωρούμε, επίσης το διανυσματικό χώρο $F(V \times W)$, ο οποίος έχει σαν βάση το διανυσματικό χώρο $V \times W$, δηλαδή το καρτεσιανό γινόμενο των V, W που ορίζεται επί σώματος K . Το **τανυστικό γινόμενο δύο στοιχείων v, w** είναι η κλάση ισοδυναμίας $[v, w]_{\sim}$ του $(v, w) \in V \times W$.

Δηλαδή, ισχύει: $V \otimes W = F(V \times W)/R$.

Σημειώνουμε στον παραπάνω ορισμό, ότι η σχέση ισοδυναμίας R είναι ο διανυσματικός χώρος που παράγεται από όλα τα διανύσματα της μορφής:

- $(v_1, w) + (v_2, w) - (v_1 + v_2, w)$ με $v_1, v_2 \in V, w \in W$
- $(v, w_1) + (v, w_2) - (v, w_1 + w_2)$ με $v \in V, w_1, w_2 \in W$
- $\lambda(v, w) - (\lambda v, w)$ με $\lambda \in K, v \in V, w \in W$
- $\lambda(v, w) - (v, \lambda w)$ με $\lambda \in K, v \in V, w \in W$

Το τανυστικό γινόμενο διανυσμάτων έχει τις παρακάτω ιδιότητες:

- $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$ με $v_1, v_2 \in V, w \in W$
- $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$ με $v \in V, w_1, w_2 \in W$
- $\lambda v \otimes w = v \otimes \lambda w$ με $\lambda \in K, v \in V, w \in W$

Ορισμός 4. Έστω X, Y δύο διανυσματικοί χώροι και V, W δύο υπόχωροί τους αντίστοιχα, όπως και προηγουμένως. Έστω, επίσης δύο γραμμικές απεικονίσεις S, T με $S : V \rightarrow X$ και $T : W \rightarrow Y$. Το **τανυστικό γινόμενο των γραμμικών απεικονίσεων** είναι επίσης μια γραμμική απεικόνιση, η $S \otimes T : V \otimes W \rightarrow X \otimes Y$, η οποία ορίζεται ως εξής:

$$(S \otimes T)(v \otimes w) = S(v) \otimes T(w) \Leftrightarrow (S \otimes T)((v, w) + R) = (S(v), T(w)) + R$$

Εάν οι S, T είναι 1-1, επί ή συνεχείς το τανυστικό τους γινόμενο $S \otimes T$ θα είναι επίσης 1-1, επί ή συνεχής απεικόνιση, αντίστοιχα.

Το τανυστικό γινόμενο πινάκων, το οποίο στη βιβλιογραφία απαντάται και ως γινόμενο Kronecker, είναι μία πράξη μεταξύ δύο πινάκων αυθαίρετου μεγέθους που έχει ως αποτέλεσμα έναν πίνακα που γράφεται σε μορφή επιμέρους blocks. Αποτελεί γενίκευση του εξωτερικού γινομένου διανυσμάτων σε πίνακες.

Ορισμός 5. Έστω A πίνακας $m \times n$ και B πίνακας $p \times q$. Το **τανυστικό γινόμενο των πινάκων** $A \otimes B$ ορίζεται ως ο πίνακας με διάσταση $mp \times nq$:

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}$$

Στην περίπτωση που οι πίνακες A και B είναι πίνακες αναπαράστασης γραμμικών απεικονίσεων, όπως οι S, T παραπάνω, τότε ο $A \otimes B$ θα είναι ο πίνακας που αναπαριστά το τανυστικό γινόμενο των δύο απεικονίσεων $S \otimes T$.

Αν A, B, C πίνακες και λ βαθμωτό, ισχύουν οι παρακάτω ιδιότητες:

- $A \otimes (B + C) = A \otimes B + A \otimes C$
- $(A + B) \otimes C = A \otimes C + B \otimes C$
- $(\lambda A) \otimes B = \lambda(A \otimes B)$
- $A \otimes B \neq B \otimes A$, εν γένει.
- $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- $(A \otimes B)(C \otimes D) = AC \otimes BD$
- $\text{Tr}(A \otimes B) = \text{Tr}A \cdot \text{Tr}B$

Στη Συναρτησιακή Ανάλυση το τανυστικό γινόμενο χώρων Hilbert αποτελεί μία επέκταση του τανυστικού γινομένου διανυσματικών χώρων, τέτοια ώστε εάν πολλαπλασιάσουμε τανυστικά δύο χώρους Hilbert, το αποτέλεσμα να είναι επίσης ένας χώρος Hilbert.

Έστω, λοιπόν H_1, H_2 δύο χώροι Hilbert. Κατασκευάζουμε τον $H_1 \otimes H_2$, σύμφωνα με τα όσα γνωρίζουμε μέχρι στιγμής για το τανυστικό γινόμενο διανυσματικών χώρων. Σε αυτόν το χώρο θα πρέπει να ορίσουμε και ένα εσωτερικό γινόμενο, το οποίο να προκύπτει φυσιολογικά από τα εσωτερικά γινόμενα των H_1, H_2 .

Ορισμός 6. Έστω H_1, H_2 δύο χώροι Hilbert με εσωτερικά γινόμενα $\langle \cdot, \cdot \rangle_1$ και $\langle \cdot, \cdot \rangle_2$, αντίστοιχα. Ορίζουμε το εσωτερικό γινόμενο του χώρου $H_1 \otimes H_2$ ως εξής:

$$\langle \phi_1 \otimes \phi_2, \psi_1 \otimes \psi_2 \rangle = \langle \phi_1, \psi_1 \rangle_1 \langle \phi_2, \psi_2 \rangle_2, \forall \phi_1, \psi_1 \in H_1, \forall \phi_2, \psi_2 \in H_2$$

Το ότι οι διγραμμικές μορφές του $H_1 \times H_2$ ταυτίζονται με τα γραμμικά συναρτησιακά του $H_1 \otimes H_2$ (δηλαδή, απεικονίζονται σε αυτά μέσω της ταυτοτικής συνάρτησης), μας εξασφαλίζει ότι το παραπάνω εσωτερικό γινόμενο ορίζεται φυσιολογικά.

Ο διανυσματικός χώρος $H_1 \otimes H_2$ με το εσωτερικό του γινόμενο και την αντίστοιχη γραμμική επέκταση, είναι πλέον χώρος εσωτερικού γινομένου.

Ορισμός 7. Η πλήρωση ως προς το εσωτερικό γινόμενο του Ορισμού 6 του χώρου εσωτερικού γινομένου $H_1 \otimes H_2$ είναι ένας χώρος Hilbert, ο οποίος καλείται **τανυστικό γινόμενο των χώρων Hilbert H_1 και H_2** .

Η διάσταση του $H_1 \otimes H_2$ είναι το γινόμενο (ως πληθικοί αριθμοί) των διαστάσεων των H_1, H_2 .

Μία πολύ σημαντική ιδιότητα του τανυστικού γινομένου χώρων Hilbert δίνεται από την παρακάτω πρόταση:

Πρόταση 2. Έστω H_1, H_2 δύο χώροι Hilbert και $H_1 \otimes H_2$, το τανυστικό τους γινόμενο. Εάν η $\{\phi_k\}$ είναι ορθοκανονική βάση του H_1 και η $\{\psi_l\}$ ορθοκανονική βάση του H_2 τότε η $\{\phi_k \otimes \psi_l\}$ είναι ορθοκανονική βάση του $H_1 \otimes H_2$.

1.2. Οι χώροι Hilbert στην Κβαντομηχανική

Σύμφωνα με το μαθηματικό φορμαλισμό της Κβαντομηχανικής, η κατάσταση ενός κβαντομηχανικού συστήματος αναπαρίστανται από ένα διάνυσμα σε έναν κατάλληλο μιγαδικό διαχωρίσιμο χώρο Hilbert, ο οποίος καλείται χώρος των καταστάσεων. Η ακριβής φύση αυτού του χώρου Hilbert εξαρτάται από το εκάστοτε φυσικό σύστημα. Για παράδειγμα, οι καταστάσεις θέσης και ορμής ενός μη σχετικιστικού σωματίου με μηδενικό spin βρίσκονται εντός του χώρου όλων των τετραγωνικά ολοκληρώσιμων συναρτήσεων, ενώ οι καταστάσεις του spin ενός πρωτονίου βρίσκονται εντός του διδιάστου μιγαδικού χώρου Hilbert των σπινόρων. Όπως αναφέραμε νωρίτερα, κάθε διάνυσμα σε έναν χώρο Hilbert μπορεί να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων της βάσης του, τα οποία αναπαριστούν τις πιθανές καταστάσεις στις οποίες μπορεί να βρεθεί το σύστημά μας. Συνεπώς, η κατάσταση ενός κβαντομηχανικού συστήματος είναι μία υπέρθεση των πιθανών καταστάσεων στις οποίες μπορεί να βρεθεί το σύστημα, με τους συντελεστές c_k (βλ. Πρόταση 1) να αντιπροσωπεύουν το πλάτος πιθανότητας, όταν μετρήσουμε, να βρούμε το σύστημα στην κατάσταση e_k . Το πλάτος πιθανότητας είναι, εν γένει, ένας μιγαδικός αριθμός, ο οποίος όταν υψωθεί στο τετράγωνο μας δίνει την πιθανότητα το σύστημα να βρίσκεται στην αντίστοιχη κατάσταση. Για τον πλήρη προσδιορισμό του χρειαζόμαστε τόσο το μέτρο του (απόλυτο μέγεθος της πιθανότητας), όσο και την αντίστοιχη φάση. Το γεγονός αυτό μας φανερώνει ότι η δομή των κβαντομηχανικών συστημάτων είναι κατά πολύ βαθύτερη από αυτή των κλασικών. Εκτός από την πιθανότητα της κάθε κατάστασης, έχουμε επιπροσθέτως και μία φάση που σχετίζεται με την πιθανότητα αυτή και οδηγεί σε κυματικού τύπου αλληλοσυσχέτιση (λόγω του κυματοσωματιδιακού дуϊσμού), καθώς το σύστημα εξελίσσεται. Για το λόγο αυτό, η εξίσωση Schroedinger που περιγράφει τη δυναμική ενός κβαντομηχανικού συστήματος επιδέχεται λύσεις κυματικού τύπου, δηλαδή η κατάσταση του συστήματος είναι μία κυματοσυνάρτηση. Κάθε μέγεθος το οποίο μπορούμε να μετρήσουμε το αντιπροσωπεύει ένας αυτοσυζυγής γραμμικός τελεστής που δρά στο χώρο Hilbert. Κάθε ιδιοκατάσταση (δηλαδή πιθανή κατάσταση) του μεγέθους που μετράμε αντιστοιχεί σε ένα ιδιοδιάνυσμα του τελεστή αυτού, με τη σχετική ιδιοτιμή να αντιστοιχεί στην τιμή του μεγέθους για αυτήν την ιδιοκατάσταση. Αυτό εξηγεί και την επιλογή αυτοσυζυγών τελεστών, των οποίων όλες οι ιδιοτιμές είναι πραγματικές. Προσδιορίζοντας τη φασματική ανάλυση του τελεστή, λαμβάνουμε την κατανομή των πιθανοτήτων για κάποιο μέγεθος σε δεδομένη κατάσταση. Η δράση του τελεστή που αντιπροσωπεύει την ολική ενέργεια του συστήματος (καλείται Χαμιλτονιανή) είναι αυτή

που προκαλεί την εξέλιξη του συστήματος στο χρόνο,όπως αυτή περιγράφεται από την εξίσωση Schroedinger.

Ένα ιδιαίτερο χαρακτηριστικό των κβαντικών συστημάτων που χρειάζεται να αναφέρουμε είναι η λεγόμενη “κατάρρευση” της κυματοσυνάρτησης.Οποτεδήποτε παρατηρούμε,δηλαδή μετράμε κάποια από τις συνιστώσες της,το σύστημα αμέσως μεταπίπτει σε αυτήν την κατάσταση και παύουν να υπάρχουν οι υπόλοιπες συνιστώσες.Κατά τη διάρκεια μιας ιδανικής μέτρησης το πλάτος πιθανότητας το σύστημα από μία αρχική κατάσταση να καταρρεύσει σε μία συγκεκριμένη ιδιοκατάσταση δίνεται από το εσωτερικό γινόμενο της αρχικής και τελικής κατάστασης και τα πιθανά αποτελέσματα της μέτρησης είναι οι ιδιοτιμές του αντίστοιχου τελεστή.Θεωρώντας τα αρχικά πλάτη πιθανότητας και τα πλάτη πιθανότητας μετάβασης μεταξύ διαφορετικών καταστάσεων προκύπτει η εξέλιξη του συστήματος. Τέλος,εάν έχουμε δύο (ή και περισσότερα) ανεξάρτητα συστήματα,έστω H_1 και H_2 οι αντίστοιχοι χώροι Hilbert,οι καταστάσεις του συνολικού συστήματος που περιλαμβάνει και τα δύο θα βρίσκονται εντός του $H_1 \otimes H_2$,για τον οποίο ισχύουν οι ιδιότητες που παρουσιάσαμε στην προηγούμενη ενότητα.

2. Μορφή και ιδιότητες του μετασχηματισμού Fourier

Στην ενότητα αυτή θα παρουσιάσουμε τη μορφή του κβαντικού μετασχηματισμού Fourier και θα αποδείξουμε κάποιες βασικές μαθηματικές του ιδιότητες, οι οποίες θα μας χρειαστούν στη συνέχεια.

Η δράση του στα διανύσματα βάσης $|j\rangle$ (σύμφωνα με το συμβολισμό Dirac της Κβαντομηχανικής) του αντίστοιχου χώρου Hilbert διάστασης N , δίνεται από την παρακάτω σχέση:

$$F|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle \quad (2)$$

όπου $\omega = e^{\frac{2\pi i}{N}}$, η N -οστή ρίζα της μονάδας.

Σε αυτό το σημείο υπενθυμίζουμε το διακριτό μετασχηματισμό Fourier:

$$X_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_k \omega^{jk},$$

ο οποίος μετασχηματίζει μια ακολουθία N μιγαδικών αριθμών x_0, x_1, \dots, x_{N-1} σε μία N -περιοδική ακολουθία μιγαδικών αριθμών $X_0, X_1, \dots, X_{N-1}, \dots$ με $\omega = e^{\frac{2\pi i}{N}}$, τη N -οστή ρίζα της μονάδας.

Άμεσα παρατηρούμε ότι ο κβαντικός μετασχηματισμός Fourier είναι το κβαντικό ανάλογο του διακριτού μετασχηματισμού Fourier, με τον παράγοντα $\frac{1}{\sqrt{N}}$ να εισάγεται για λόγους νορμαλισμού.

Θεωρώντας τον πίνακα F που αναπαριστά τον κβαντικό μετασχηματισμό Fourier με

$$[F]_{jk} = \frac{1}{\sqrt{N}} \omega^{jk},$$

όπου $j, k = 0, 1, \dots, N-1$, θα αποδείξουμε ότι αυτός είναι συμμετρικός, μοναδιαίος και ότι για κάθε N ισχύει $F^4 = I$, όπου I ο ταυτοτικός πίνακας.

- Ο F είναι συμμετρικός

Ορισμός 8. Ο *ανάστροφος* ενός πίνακα A ορίζεται ως εξής:

$$[A^T]_{ij} = [A]_{ji}$$

Ορισμός 9. Ένας πίνακας A καλείται **συμμετρικός** εάν ισούται με τον ανάστροφό του, δηλαδή:

$$A = A^T \Leftrightarrow [A]_{ij} = [A]_{ji}, \forall i, j$$

Για τον F λαμβάνουμε άμεσα:

$$[F]_{jk} = \frac{1}{\sqrt{N}} \omega^{jk} = \frac{1}{\sqrt{N}} \omega^{kj} = [F]_{kj}, \forall j, k$$

- Ο F είναι μοναδιαίος

Ορισμός 10. Ο **ερμιτιανός συζυγής** ή (συζυγής ανάστροφος ή ερμιτιανός ανάστροφος) ενός πίνακα A ορίζεται ως εξής:

$$[A^\dagger]_{ij} = ([A]_{ji})^*,$$

όπου το $*$ συμβολίζει το μιγαδικό συζυγές.

Δηλαδή ο ερμιτιανός συζυγής του A προκύπτει από τον A παίρνοντας τον ανάστροφό του και στη συνέχεια το μιγαδικό συζυγές του κάθε στοιχείου του.

Ορισμός 11. Ένας πίνακας A καλείται **μοναδιαίος** εάν ισχύει:

$$A^\dagger A = A A^\dagger = I$$

όπου I ο ταυτοτικός πίνακας. Ισοδύναμα:

$$[A^\dagger]_{jk} [A]_{jk} = [A]_{jk} [A^\dagger]_{jk} = 1, \forall j = k$$

και

$$[A^\dagger]_{jk} [A]_{jk} = [A]_{jk} [A^\dagger]_{jk} = 0, \forall j \neq k$$

Για τον F έχουμε:

$$[F^\dagger]_{jk} [F]_{jk} = \sum_{l=0}^{N-1} [F^\dagger]_{jl} [F]_{lk} = \sum_{l=0}^{N-1} ([F]_{lj})^* [F]_{lk} = \frac{1}{N} \sum_{l=0}^{N-1} (\omega^*)^{lj} \omega^{lk}$$

Όμως $\omega^* = \frac{1}{\omega}$, οπότε η παραπάνω σχέση γίνεται:

$$[F^\dagger]_{jk}[F]_{jk} = \frac{1}{N} \sum_{l=0}^{N-1} \left(\frac{1}{\omega}\right)^{lj} \omega^{lk} = \frac{1}{N} \sum_{l=0}^{N-1} (\omega^{k-j})^l$$

Διακρίνουμε περιπτώσεις για τα k, j :

– $k = j$

$$[F^\dagger]_{jk}[F]_{jk} = \frac{1}{N} \sum_{l=0}^{N-1} (\omega^{k-j})^l = \frac{1}{N} \sum_{l=0}^{N-1} 1^l = \frac{1}{N} \cdot N = 1$$

– $k \neq j$

Το $\frac{1}{N} \sum_{l=0}^{N-1} (\omega^{k-j})^l$ είναι γεωμετρική σειρά, οπότε:

$$[F^\dagger]_{jk}[F]_{jk} = \frac{1}{N} \cdot \frac{\omega^{N(k-j)} - 1}{\omega^{k-j} - 1} = 0$$

Συνοψίζοντας τα παραπάνω: $F^\dagger F = I$.

Όμοια, αποδεικνύεται και ότι $FF^\dagger = I$.

Συνεπώς

$$F^\dagger F = FF^\dagger = I,$$

δηλαδή ο F είναι μοναδιαίος πίνακας.

• $F^4 = I$

Υπολογίζουμε πρώτα τον F^2 :

$$[F^2]_{jk} = \sum_{l=0}^{N-1} [F]_{jl}[F]_{lk} = \frac{1}{N} \sum_{l=0}^{N-1} \omega^{jl} \omega^{lk} = \frac{1}{N} \sum_{l=0}^{N-1} \omega^{(j+k)l}$$

Διακρίνουμε περιπτώσεις για τα k, j :

– $j + k = 0 \pmod{N}$

$$[F^2]_{jk} = \frac{1}{N} \sum_{l=0}^{N-1} \omega^{(j+k)l} = \frac{1}{N} \sum_{l=0}^{N-1} 1^l = \frac{1}{N} \cdot N = 1$$

– $j + k \neq 0 \pmod{N}$

Το $\frac{1}{N} \sum_{l=0}^{N-1} (\omega^{j+k})^l$ είναι γεωμετρική σειρά, οπότε:

$$[F^2]_{jk} = \frac{1}{N} \cdot \frac{\omega^{N(j+k)} - 1}{\omega^{j+k} - 1} = 0$$

Συνοπτικά:

$$[F^2]_{jk} = \delta_{j,-k}$$

Για τον F^4 θα έχουμε τώρα:

$$[F^4]_{jk} = \sum_{l=0}^{N-1} [F^2]_{jl} [F^2]_{lk}$$

– Εάν $j + l = 0 \pmod{N}$ και $k + l = 0 \pmod{N} \Leftrightarrow j = k$

$$[F^4]_{jk} = \frac{1}{N^2} \cdot N \cdot N = 1$$

– Ενώ,εάν $j + l \neq 0 \pmod{N}$ ή $k + l \neq 0 \pmod{N} \Leftrightarrow j \neq k$

$$[F^4]_{jk} = 0$$

Συνοψίζοντας,λαμβάνουμε το ζητούμενο: $F^4 = I$.

3. Ιδιοανύσματα και Ιδιοτιμές του μετασχηματισμού Fourier

Ο μετασχηματισμός Fourier, όπως είδαμε και προηγουμένως αναπαρίσταται από το μοναδιαίο πίνακα:

$$F_{jk} = \frac{1}{\sqrt{N}} \exp\left(\frac{2\pi i}{N} j \cdot k\right)$$

Το πρόβλημα της διαγωνοποίησής του ανακύπτει σε πολλές περιπτώσεις και έχει μελετηθεί εκτενώς. Οι ιδιοτιμές του προσδιορίστηκαν από τον Schur [6] με σκοπό να υπολογιστεί το ίχνος του πίνακα. Στη συνέχεια θα παρουσιάσουμε μία σχετικά απλή διαδικασία [5, II] με την οποία μέσω του ίχνους μπορούμε να τις ανακτήσουμε. Ο προσδιορισμός των ιδιοανυσμάτων αποτελεί ένα πιο πολύπλοκο πρόβλημα, κυρίως λόγω του μεγάλου εκφυλισμού που εμφανίζεται. Ακολουθώντας την τυπική μαθηματική μέθοδο της ενότητας (3.2) [5, III], κατά την οποία χρησιμοποιούμε τις προβολές του F στους ιδιόχωρους του, όπως αυτοί προκύπτουν από τις αντίστοιχες ιδιοτιμές, καταφέρνουμε να προσδιορίσουμε τα ιδιοανύσματά του, τα οποία όμως δεν είναι ορθογώνια μεταξύ τους. Στο πλαίσιο αυτό, δεν υπάρχει συγκεκριμένη αναλυτική φόρμουλα που να μας δίνει απευθείας ορθογώνια ιδιοανύσματα του F για κάθε N , έχουν όμως προταθεί αρκετές μέθοδοι σε διαφορετικά πλαίσια [8], [5, IV], [7] από τις οποίες προκύπτει το ζητούμενο.

3.1. Ιδιοτιμές του μετασχηματισμού Fourier

Έχουμε ήδη δει ότι:

$$F_{jk}^2 = \frac{1}{N} \sum_{l=0}^{N-1} \exp\left(\frac{2\pi i}{N} l(j+k)\right) \quad (3)$$

Στην περίπτωση που $j+k = 0 \pmod{N}$ έχουμε:

$$F_{jk}^2 = 1,$$

ενώ $F_{jk}^2 = 0$ σε κάθε άλλη περίπτωση. Χρησιμοποιώντας το σύμβολο του Kronecker $\delta_{j,-k}$ μπορούμε να γράψουμε

$$F_{jk}^2 = \delta_{j,-k} = I'_{jk} \quad (4)$$

Για τις υπόλοιπες δυνάμεις του F έχουμε:

$$F^3 = FF^2 = FI' = F^{-1}$$

Έχουμε,όμως δείξει ότι ο F είναι μοναδιαίος πίνακας,δηλαδή $F^{-1} = F^\dagger$,οπότε:

$$F^3 = F^\dagger = (F^T)^*$$

Επιπλέον,επειδή ο F είναι και συμμετρικός,δηλαδή $F^T = F$,θα έχουμε τελικά ότι

$$F^3 = F^*$$

Στην προηγούμενη ενότητα δείξαμε ότι

$$F^4 = I,$$

μία σχέση πολύ χρήσιμη,καθώς μας πληροφορεί ότι οι ιδιοτιμές του F είναι οι $1, -1, i, -i$. Για τις ανώτερες δυνάμεις του F θα ισχύει:

$$F^{4+j} = F^j.$$

Στη συνέχεια,θα υπολογίσουμε το ίχνος των πινάκων αυτών,με σκοπό να προσδιορίσουμε τις πολλαπλότητες των ιδιοτιμών.

Εν γένει,ισχύει:

$$\text{tr}F = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(\frac{2\pi i}{N} j^2\right)$$

και εφαρμόζοντας τον τύπο του Gauss λαμβάνουμε:

$$\text{tr}F = \frac{1}{2}(1+i)[1+(-i)^N]$$

Διακρίνουμε τις εξής περιπτώσεις:

- $N = 0 \pmod{4}$
 $\text{tr}F = (1+i)$
- $N = 1 \pmod{4}$
 $\text{tr}F = \frac{1}{2}(1+i)(1-i)$
- $N = 2 \pmod{4}$
 $\text{tr}F = 0$

- $N = 3 \pmod{4}$
 $\text{tr}F = i$

Επιπλέον, αφού $F^{4j+1} = F$ θα έχουμε ότι $\text{tr}F^{4j+1} = \text{tr}F$.

Γράφοντας αναλυτικά τον πίνακα για τον F^2 σε διαφορετικές διαστάσεις, παρατηρούμε ότι το ίχνος του θα είναι 1, εάν το N είναι περιττός, ενώ αν το N είναι άρτιος το ίχνος θα είναι 2.

Επίσης, επειδή $F^{4j+2} = F^2$ μπορούμε να γράψουμε:

$$\text{tr}F^{4j+2} = \text{tr}F^2 = \frac{1}{2}(3 + (-1)^N), j = 0, 1, 2, \dots$$

Δεδομένου ότι $F^{4j+3} = F^3 = F^*$, $j = 0, 1, 2, \dots$ θα έχουμε:

$$\text{tr}F^{4j+3} = \text{tr}F^3 = \text{tr}F^* = (\text{tr}F)^*.$$

Διακρίνουμε κι εδώ τις περιπτώσεις:

- $N = 0 \pmod{4}$
 $\text{tr}F^3 = (1 - i)$
- $N = 1 \pmod{4}$
 $\text{tr}F^3 = \frac{1}{2}(1 - i)(1 + i)$
- $N = 2 \pmod{4}$
 $\text{tr}F^3 = 0$
- $N = 3 \pmod{4}$
 $\text{tr}F^3 = -i$

Τέλος, για το ίχνος του F^4 , έχουμε:

$$\text{tr}F^4 = \text{tr}I = N$$

και αφού $F^{4j+4} = F^{4j} = F^4 = I$, $j = 0, 1, 2, \dots$ προκύπτει ότι $\text{tr}F^{4j+4} = N$.

Τα παραπάνω αποτελέσματα συνοψίζονται στην εξής σχέση:

$$\text{tr} F^s = 1 + \sum_{k=2}^N (-i)^{ks},$$

με το s να παίρνει τις τιμές $4j, 4j+1, 4j+2$ και $4j+3, j=0, 1, 2, \dots$

Η τελευταία εξίσωση ισχύει για κάθε ακέραιο s , είναι όμως αρκετό για τον προσδιορισμό των πολλαπλοτήτων των ιδιοτιμών να την εφαρμόσουμε μέχρι το N και με τη βοήθεια της σχέσης

$$\text{tr} F^s = \sum_{i=1}^N \lambda_i^s,$$

να καταλήξουμε στο ότι οι πολλαπλότητες των ιδιοτιμών $1, -1, i, -i$ θα είναι αντίστοιχα $[\frac{N+4}{4}], [\frac{N+2}{4}], [\frac{N+1}{4}], [\frac{N-1}{4}]$, όπου $[x]$ είναι ο μεγαλύτερος ακέραιος, μικρότερος ή ίσος του x .

3.2. Ιδιοανύσματα του μετασχηματισμού Fourier

Για τον F έχουμε δείξει ότι $F^\dagger F = F F^\dagger$ (για την ακρίβεια έχουμε δείξει ότι ο F είναι μοναδιαίος, που είναι ισχυρότερο) και στην προηγούμενη ενότητα βρήκαμε τις ιδιοτιμές του $i, -1, -i, 1$, οπότε εφαρμόζοντας το φασματικό θεώρημα μπορούμε να τον γράψουμε στη μορφή:

$$F = \sum_{j=1}^4 i^j B(j) = iB(1) - B(2) - iB(3) + B(4) \quad (5)$$

με τους $B(j)$ να ικανοποιούν τις ιδιότητες (2) του φασματικού θεωρήματος. Πρώτος μας σκοπός είναι να προσδιορίσουμε τους πίνακες $B(j)$ και να αναδείξουμε κάποιες βασικές τους ιδιότητες, ώστε στη συνέχεια μέσω αυτών να βρούμε και τα ιδιοανύσματα του F . Γνωρίζουμε ότι ισχύει:

$$F_{jk} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} jk} = \frac{1}{\sqrt{N}} \left(\cos\left(\frac{2\pi}{N} jk\right) + i \sin\left(\frac{2\pi}{N} jk\right) \right)$$

Θέτοντας

$$C_{jk} = \frac{1}{\sqrt{N}} \cos\left(\frac{2\pi}{N} jk\right)$$

και

$$S_{jk} = \frac{1}{\sqrt{N}} \sin\left(\frac{2\pi}{N} jk\right)$$

ο F παίρνει τη μορφή:

$$F = C + iS \quad (6)$$

Στη συνέχεια εκφράζουμε και τις υπόλοιπες δυνάμεις του F με τη βοήθεια των C και S .

Για τον F^2 από την (6) έχουμε:

$$F^2 = (C + iS)^2 = [C^2 - S^2 + i(CS + SC)]$$

Όμως $F^2 = I'$, όπως δείξαμε στην προηγούμενη ενότητα, με τον I' να είναι πραγματικός πίνακας, συνεπώς $CS + SC = 0$, οπότε τελικά:

$$F^2 = I' = C^2 - S^2 \quad (7)$$

Έχουμε δείξει ότι ο F^3 ισούται με το συζυγή του F , άρα

$$F^3 = C - iS = F^* \quad (8)$$

Τέλος,

$$F^4 = I \quad (9)$$

Αντίστροφα, τώρα, από τις (6) και (8), εκφράζουμε τους C και S μέσω των F και F^* :

$$C = \frac{F + F^*}{2} \quad (10)$$

$$S = \frac{F - F^*}{2i} \quad (11)$$

Κάνοντας χρήση των παραπάνω σχέσεων και λαμβάνοντας υπόψη ότι ο F είναι μοναδιαίος, δηλαδή $F^\dagger F = FF^\dagger = I \Rightarrow F^* F = FF^* = I$, μπορούμε να δείξουμε ότι $C^3 = C$ και $S^3 = S$.

$$\bullet \quad C^3 = C$$

$$\begin{aligned} C^3 &= \left(\frac{F + F^*}{2} \right)^3 \\ &= \frac{F^3 + 3F^2F^* + 3F(F^*)^2 + (F^*)^3}{8} \\ &= \frac{F^* + 3F + 3F^* + F}{8} \\ &= \frac{F + F^*}{2} \\ &= C \end{aligned}$$

- $S^3 = S$

$$\begin{aligned}
S^3 &= \left(\frac{F - F^*}{2i}\right)^3 \\
&= \frac{F^3 - 3F^2F^* + 3F(F^*)^2 - (F^*)^3}{-8i} \\
&= \frac{F^* - 3F + 3F^* - F}{-8i} \\
&= \frac{F - F^*}{2i} \\
&= S
\end{aligned}$$

Επανερχόμαστε τώρα στην (5) και λαμβάνοντας υπόψη ότι εξ' ορισμού για τους $B(j)$ ισχύει:

$$B(j)B(k) = B(j)\delta_{jk} \quad (12)$$

εκφράζουμε τους F^2, F^3 και F^4 μέσω των $B(1), B(2), B(3)$ και $B(4)$.

$$F^2 = -B(1) + B(2) - B(3) + B(4) \quad (13)$$

$$F^3 = -iB(1) - B(2) + iB(3) + B(4) \quad (14)$$

$$F^4 = B(1) + B(2) + B(3) + B(4) = I \quad (15)$$

Οι (5), (13), (14) και (15) αποτελούν ένα γραμμικό σύστημα 4×4 , από την επίλυση του οποίου θα προκύψουν οι $B(1), B(2), B(3)$ και $B(4)$ που αναζητούμε. Έχουμε:

$$\begin{pmatrix} I \\ F \\ F^2 \\ F^3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ i & -1 & -i & 1 \\ -1 & 1 & -1 & 1 \\ -i & -1 & i & 1 \end{pmatrix} \begin{pmatrix} B(1) \\ B(2) \\ B(3) \\ B(4) \end{pmatrix}$$

Για να βρούμε τους $B(1), B(2), B(3)$ και $B(4)$, αρκεί να βρούμε τον αντίστροφο του παραπάνω 4×4 πίνακα, έστω A . Εξετάζουμε πρώτα εάν ο A , είναι μοναδιαίος, δηλαδή εάν $AA^\dagger = I$.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ i & -1 & -i & 1 \\ -1 & 1 & -1 & 1 \\ -i & -1 & i & 1 \end{pmatrix} \begin{pmatrix} 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} = 4I$$

Εφόσον ο A είναι μοναδιαίος θα έχουμε $A^{-1} = A^\dagger$ και το σύστημα των εξισώσεών μας γίνεται:

$$\frac{1}{4} \begin{pmatrix} 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} I \\ F \\ F^2 \\ F^3 \end{pmatrix} = \begin{pmatrix} B(1) \\ B(2) \\ B(3) \\ B(4) \end{pmatrix}$$

Άρα τελικά λαμβάνουμε:

$$\begin{aligned} B(1) &= \frac{I - iF - F^2 + iF^3}{4} \\ &= \frac{I - i(C + iS) - I' + i(C - iS)}{4} \\ &= \frac{1}{2}S + \frac{1}{4}(I - I') \end{aligned}$$

$$\begin{aligned} B(2) &= \frac{I - F + F^2 - F^3}{4} \\ &= \frac{I - (C + iS) + I' - (C - iS)}{4} \\ &= -\frac{1}{2}C + \frac{1}{4}(I + I') \end{aligned}$$

$$\begin{aligned} B(3) &= \frac{I + iF - F^2 - iF^3}{4} \\ &= \frac{I + i(C + iS) - I' - i(C - iS)}{4} \\ &= -\frac{1}{2}S + \frac{1}{4}(I - I') \end{aligned}$$

$$\begin{aligned} B(4) &= \frac{I + F + F^2 + F^3}{4} \\ &= \frac{I + (C + iS) + I' + (C - iS)}{4} \\ &= \frac{1}{2}C + \frac{1}{4}(I + I') \end{aligned}$$

Ισοδύναμα, το (j, k) στοιχείο των πινάκων αυτών θα δίνεται από τις:

$$\begin{aligned} [B(1)]_{jk} &= \frac{1}{2\sqrt{N}} \sin\left(\frac{2\pi}{N}jk\right) + \frac{1}{4}(\delta_{j,k} - \delta_{j,-k}) \\ [B(2)]_{jk} &= -\frac{1}{2\sqrt{N}} \cos\left(\frac{2\pi}{N}jk\right) + \frac{1}{4}(\delta_{j,k} + \delta_{j,-k}) \\ [B(3)]_{jk} &= -\frac{1}{2\sqrt{N}} \sin\left(\frac{2\pi}{N}jk\right) + \frac{1}{4}(\delta_{j,k} - \delta_{j,-k}) \\ [B(4)]_{jk} &= \frac{1}{2\sqrt{N}} \cos\left(\frac{2\pi}{N}jk\right) + \frac{1}{4}(\delta_{j,k} + \delta_{j,-k}) \end{aligned}$$

Είναι εύκολο να δειχθεί με τη βοήθεια των (5) και (12), ότι ισχύει:

$$FB(j) = i^j B(j) \quad (16)$$

Η σχέση αυτή είναι εξαιρετικά σημαντική, καθώς μας δείχνει ότι οι μη-μηδενικές στήλες του $B(j)$ είναι ιδιοανύσματα του F που αντιστοιχούν στην ιδιοτιμή i^j . Οι ιδιοτιμές των $B(j)$ για κάθε j θα είναι 1 ή 0, λόγω του ότι οι $B(j)$ είναι προβολικοί πίνακες. Συνεπώς, το ίχνος κάθε $B(j)$ θα ισούται με την πολλαπλότητα της ιδιοτιμής 1 αυτού, δηλαδή:

$$\text{Tr}B(j) = m(1, B(j)), j = 1, 2, 3, 4$$

Συγκεκριμένα, αθροίζοντας τα στοιχεία της διαγωνίου των πινάκων αυτών λαμβάνουμε:

$$\begin{aligned} \text{Tr}B(1) &= m(1, B(1)) = \sum_{j=0}^{N-1} \left(\frac{1}{2\sqrt{N}} \sin\left(\frac{2\pi}{N}j^2\right) + \frac{1}{4}(\delta_{j,j} - \delta_{j,-j}) \right) \\ \text{Tr}B(2) &= m(1, B(2)) = \sum_{j=0}^{N-1} \left(-\frac{1}{2\sqrt{N}} \cos\left(\frac{2\pi}{N}j^2\right) + \frac{1}{4}(\delta_{j,j} + \delta_{j,-j}) \right) \\ \text{Tr}B(3) &= m(1, B(3)) = \sum_{j=0}^{N-1} \left(-\frac{1}{2\sqrt{N}} \sin\left(\frac{2\pi}{N}j^2\right) + \frac{1}{4}(\delta_{j,j} - \delta_{j,-j}) \right) \\ \text{Tr}B(4) &= m(1, B(4)) = \sum_{j=0}^{N-1} \left(\frac{1}{2\sqrt{N}} \cos\left(\frac{2\pi}{N}j^2\right) + \frac{1}{4}(\delta_{j,j} + \delta_{j,-j}) \right) \end{aligned}$$

Όμως,όπως έχουμε δει νωρίτερα:

$$\text{tr}F = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(\frac{2\pi i}{N} j^2\right) = \frac{1}{2}(1+i)[1+(-i)^N]$$

Συνεπώς:

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \cos\left(\frac{2\pi}{N} j^2\right) = \text{Re}(\text{Tr}F)$$

και

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sin\left(\frac{2\pi}{N} j^2\right) = \text{Im}(\text{Tr}F)$$

Διακρίνοντας περιπτώσεις για το N , δηλαδή εάν $N = 0 \pmod{4}$, $N = 1 \pmod{4}$, κλπ. και λαμβάνοντας επιπλέον υπόψη ότι

$$\sum_{j=0}^{N-1} \delta_{j,j} = N$$

και

$$\sum_{j=0}^{N-1} \delta_{j,-j} = \frac{1}{2}(3+(-1)^N)$$

μπορούμε από τις τελευταίες σχέσεις να υπολογίσουμε ακριβώς τις πολλαπλότητες της ιδιοτιμής 1 των πινάκων $B(1)$, $B(2)$, $B(3)$ και $B(4)$.

Όσον αφορά στις ιδιοτιμές των C και S , έχουμε ότι αυτές θα είναι ± 1 ή 0, εφόσον ισχύει ότι $C^3 = C$ και $S^3 = S$.

Τέλος, προς επαλήθευση των παραπάνω, μπορούμε θεωρώντας την ανάλυση του F στους $B(j)$ και τις εκφράσεις αυτών ως προς C και S , να προσδιορίσουμε τις πολλαπλότητες των ιδιοτιμών τους ως εξής:

$$m(1, C) = m(1, B(4)) = m(1, F) = \left\lfloor \frac{N+4}{4} \right\rfloor$$

$$m(-1, C) = m(1, B(2)) = m(-1, F) = \left\lfloor \frac{N+2}{4} \right\rfloor$$

$$m(1, S) = m(1, B(1)) = m(i, F) = \left\lfloor \frac{N+1}{4} \right\rfloor$$

$$m(-1, S) = m(1, B(3)) = m(-i, F) = \left\lfloor \frac{N-1}{4} \right\rfloor$$

Γνωρίζουμε ότι ο αριθμός των γραμμικώς ανεξάρτητων διανυσμάτων-στηλών ενός πίνακα είναι ο αριθμός των μη μηδενικών ιδιοτιμών του. Άρα, από τις παραπάνω σχέσεις ο $B(j)$, $j = 1, 2, 3, 4$ θα έχει $m(1, B(j))$ γραμμικώς ανεξάρτητα διανύσματα-στήλες.

Για τον F θα έχουμε ότι τα ιδιοανύσματά του που αντιστοιχούν στην ιδιοτιμή i^j , θα είναι τα $m(1, B(j))$ γραμμικώς ανεξάρτητα διανύσματα-στήλες του $B(j)$. Πρέπει, όμως, επιπλέον τα διανύσματα αυτά να είναι και ορθογώνια μεταξύ τους. Για την ορθογωνιοποίησή τους εφαρμόζουμε τη γνωστή μέθοδο Gram-Schmidt.

• **Ορθογωνιοποίηση των στηλών ενός πίνακα B με τη μέθοδο Gram-Schmidt**

Έχουμε ήδη δει ότι εάν για έναν πραγματικό συμμετρικό πίνακα B ισχύει: $B^2 = B$, δηλαδή ο B είναι προβολικός, τότε οι ιδιοτιμές του είναι 0 ή 1 και είναι μη αρνητικά ορισμένος. Επίσης, ότι τα στοιχεία της διαγωνίου του είναι μεταξύ 0 και 1, δηλαδή $0 \leq B_{jj} \leq 1$ και το ίχνος του (που είναι ένας ακέραιος αριθμός) μας δίνει τον αριθμό των γραμμικώς ανεξάρτητων στηλών (ή γραμμών) του. Ισχύει ακόμα ότι εάν $B_{jj} = 0$ ή 1 τότε $B_{jk} = 0$ για $j \neq k$. Επιπλέον, εάν $B_{11} \neq 0$, τότε προσθέτοντας στην k -οστή στήλη ($k = 2, 3, \dots, N$) ένα σταθερό πολλαπλάσιο (που εξαρτάται από το k) της πρώτης στήλης τότε μπορούμε να αντικαταστήσουμε το $(1, k)$ στοιχείο της με το 0. Έχουμε, λοιπόν, ότι:

$$B \rightarrow \begin{bmatrix} B_{11} & 0 \\ B_{j1} & B' \end{bmatrix}$$

όπου για $j, k = 2, 3, \dots, N$ έχουμε

$$B'_{jk} = B_{jk} - \frac{B_{1j}B_{1k}}{B_{11}}$$

Ο B' είναι επίσης ένας πραγματικός συμμετρικός πίνακας για τον οποίο ισχύει $B'^2 = B'$, δηλαδή είναι και προβολικός. Το ίχνος του είναι $\text{Tr} B' = \text{Tr} B - 1$ και κάθε του στήλη είναι ορθογώνια με την πρώτη στήλη του B , δηλαδή $\sum_{j=2}^N B_{j1}B'_{jk} = 0$, $k = 2, 3, \dots, N$.

Άρα, ο B' έτσι όπως έχει κατασκευαστεί, έχει τις ίδιες ιδιότητες με τον

B . Συνεπώς μπορούμε να επαναλάβουμε την ίδια διαδικασία για κάθε μη μηδενικό στοιχείο της διαγωνίου του B' . Σε κάθε επανάληψη διαχωρίζουμε μία ακόμα μη μηδενική στήλη, η οποία θα είναι ορθογώνια με όλες τις προηγούμενες και μειώνουμε το ίχνος του πίνακα κατά μία μονάδα. Στο τέλος της διαδικασίας αυτής θα μείνει μόνο ένας μηδενικός πίνακας.

Συνοψίζοντας, το σύνολο των ιδιοανυσμάτων του F που αντιστοιχούν στην ιδιοτιμή i^j είναι το σύνολο των $m(1, B(j))$ γραμμικώς ανεξάρτητων στηλών του $B(j)$ οι οποίες ορθογωνοποιούνται με την παραπάνω αναδρομική διαδικασία.

3.3. Εφαρμογή για $N=5$

Ο πίνακας του μετασχηματισμού Fourier με διάσταση 5 έχει ως εξής:

$$F = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{bmatrix}$$

όπου $\omega = e^{\frac{2\pi i}{5}} \approx 0,31 + 0,95i$.

Στην περίπτωση αυτή ισχύει $\omega^5 = 1$, άρα μπορούμε να γράψουμε τον F και σε απλούστερη μορφή και στη συνέχεια αντικαθιστώντας το ω να τον υπολογίσουμε με ακρίβεια δύο δεκαδικών ψηφίων:

$$F = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}$$

$$F \approx \begin{bmatrix} 0.45 & 0.45 & 0.45 & 0.45 & 0.45 \\ 0.45 & 0.14 + 0.43i & -0.36 + 0.26i & -0.36 - 0.26i & 0.14 - 0.43i \\ 0.45 & -0.36 + 0.26i & 0.14 - 0.43i & 0.14 + 0.43i & -0.36 - 0.26i \\ 0.45 & -0.36 - 0.26i & 0.14 + 0.43i & 0.14 - 0.43i & -0.36 + 0.26i \\ 0.45 & 0.14 - 0.43i & -0.36 - 0.26i & -0.36 + 0.26i & 0.14 + 0.43i \end{bmatrix}$$

Εύκολα βρίσκουμε ότι $\text{Tr} F = \frac{1}{\sqrt{5}}(\omega^0 + \omega^1 + \omega^4 + \omega^9 + \omega^{16}) = \frac{1}{\sqrt{5}}(1 + 2\omega + 2\omega^4) \approx 1$
 Για τις πολλαπλότητες των ιδιοτιμών $1, -1, i, -i$ θα έχουμε:

$$m(1, F) = \left[\frac{5+4}{4} \right] = \left[\frac{9}{4} \right] = 2$$

$$m(-1, F) = \left[\frac{5+2}{4} \right] = \left[\frac{7}{4} \right] = 1$$

$$m(i, F) = \left[\frac{5+1}{4} \right] = \left[\frac{6}{4} \right] = 1$$

$$m(-i, F) = \left[\frac{5-1}{4} \right] = \left[\frac{4}{4} \right] = 1$$

Θέτοντας $\phi = \frac{2\pi}{5}$, οι πίνακες C και S θα είναι:

$$C = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \cos \phi & \cos 2\phi & \cos 3\phi & \cos 4\phi \\ 1 & \cos 2\phi & \cos 4\phi & \cos \phi & \cos 3\phi \\ 1 & \cos 3\phi & \cos \phi & \cos 4\phi & \cos 2\phi \\ 1 & \cos 4\phi & \cos 3\phi & \cos 2\phi & \cos \phi \end{bmatrix} \approx \begin{bmatrix} 0.45 & 0.45 & 0.45 & 0.45 & 0.45 \\ 0.45 & 0.14 & -0.36 & -0.36 & 0.14 \\ 0.45 & -0.36 & 0.14 & 0.14 & -0.36 \\ 0.45 & -0.36 & 0.14 & 0.14 & -0.36 \\ 0.45 & 0.14 & -0.36 & -0.36 & 0.14 \end{bmatrix}$$

$$S = \frac{1}{\sqrt{5}} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \sin \phi & \sin 2\phi & \sin 3\phi & \sin 4\phi \\ 0 & \sin 2\phi & \sin 4\phi & \sin \phi & \sin 3\phi \\ 0 & \sin 3\phi & \sin \phi & \sin 4\phi & \sin 2\phi \\ 0 & \sin 4\phi & \sin 3\phi & \sin 2\phi & \sin \phi \end{bmatrix} \approx \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0.43 & 0.26 & -0.26 & -0.43 \\ 0 & 0.26 & -0.43 & 0.43 & -0.26 \\ 0 & -0.26 & 0.43 & -0.43 & 0.26 \\ 0 & -0.43 & -0.26 & 0.26 & 0.43 \end{bmatrix}$$

Οι I και I' για $N = 5$ έχουν ως εξής:

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, I' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Οπότε:

$$(I + I') = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, (I - I') = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

Μπορούμε,λοιπόν,τώρα να βρούμε και τους $B(1), B(2), B(3), B(4)$ του φασματικού θεωρήματος,σύμφωνα με το οποίο:

$$F = iB(1) - B(2) - iB(3) + B(4)$$

Για $\alpha = \frac{1}{2\sqrt{5}}$ και $\beta = \frac{1}{4}$,θα έχουμε:

$$B(1) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha \sin \phi + \beta & \alpha \sin 2\phi & \alpha \sin 3\phi & \alpha \sin 4\phi - \beta \\ 0 & \alpha \sin 2\phi & \alpha \sin 4\phi + \beta & \alpha \sin \phi - \beta & \alpha \sin 3\phi \\ 0 & \alpha \sin 3\phi & \alpha \sin \phi - \beta & \alpha \sin 4\phi + \beta & \alpha \sin 2\phi \\ 0 & \alpha \sin 4\phi - \beta & \alpha \sin 3\phi & \alpha \sin 2\phi & \alpha \sin \phi + \beta \end{bmatrix}$$

$$B(1) \approx \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0.46 & 0.13 & -0.13 & -0.46 \\ 0 & 0.13 & 0.04 & -0.04 & -0.13 \\ 0 & -0.13 & -0.04 & 0.04 & 0.13 \\ 0 & -0.46 & -0.13 & 0.13 & 0.46 \end{bmatrix}$$

$$B(2) = \begin{bmatrix} -\alpha + 2\beta & -\alpha & -\alpha & -\alpha & -\alpha \\ -\alpha & -\alpha \cos \phi + \beta & -\alpha \cos 2\phi & -\alpha \cos 3\phi & -\alpha \cos 4\phi + \beta \\ -\alpha & -\alpha \cos 2\phi & -\alpha \cos 4\phi + \beta & -\alpha \cos \phi + \beta & -\alpha \cos 3\phi \\ -\alpha & -\alpha \cos 3\phi & -\alpha \cos \phi + \beta & -\alpha \cos 4\phi + \beta & -\alpha \cos 2\phi \\ -\alpha & -\alpha \cos 4\phi + \beta & -\alpha \cos 3\phi & -\alpha \cos 2\phi & -\alpha \cos \phi + \beta \end{bmatrix}$$

$$B(2) \approx \begin{bmatrix} 0.28 & -0.22 & -0.22 & -0.22 & -0.22 \\ -0.22 & 0.18 & 0.18 & 0.18 & 0.18 \\ -0.22 & 0.18 & 0.18 & 0.18 & 0.18 \\ -0.22 & 0.18 & 0.18 & 0.18 & 0.18 \\ -0.22 & 0.18 & 0.18 & 0.18 & 0.18 \end{bmatrix}$$

$$B(3) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -\alpha \sin \phi + \beta & -\alpha \sin 2\phi & -\alpha \sin 3\phi & -\alpha \sin 4\phi - \beta \\ 0 & -\alpha \sin 2\phi & -\alpha \sin 4\phi + \beta & -\alpha \sin \phi - \beta & -\alpha \sin 3\phi \\ 0 & -\alpha \sin 3\phi & -\alpha \sin \phi - \beta & -\alpha \sin 4\phi + \beta & -\alpha \sin 2\phi \\ 0 & -\alpha \sin 4\phi - \beta & -\alpha \sin 3\phi & -\alpha \sin 2\phi & -\alpha \sin \phi + \beta \end{bmatrix}$$

$$B(3) \approx \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0.04 & -0.13 & 0.13 & -0.04 \\ 0 & -0.13 & 0.46 & -0.46 & 0.13 \\ 0 & 0.13 & -0.46 & 0.46 & -0.13 \\ 0 & -0.04 & 0.13 & -0.13 & 0.04 \end{bmatrix}$$

$$B(4) = \begin{bmatrix} \alpha + 2\beta & \alpha & \alpha & \alpha & \alpha \\ \alpha & \alpha \cos \phi + \beta & \alpha \cos 2\phi & \alpha \cos 3\phi & \alpha \cos 4\phi + \beta \\ \alpha & \alpha \cos 2\phi & \alpha \cos 4\phi + \beta & \alpha \cos \phi + \beta & \alpha \cos 3\phi \\ \alpha & \alpha \cos 3\phi & \alpha \cos \phi + \beta & \alpha \cos 4\phi + \beta & \alpha \cos 2\phi \\ \alpha & \alpha \cos 4\phi + \beta & \alpha \cos 3\phi & \alpha \cos 2\phi & \alpha \cos \phi + \beta \end{bmatrix}$$

$$B(4) \approx \begin{bmatrix} 0.72 & 0.22 & 0.22 & 0.22 & 0.22 \\ 0.22 & 0.32 & -0.18 & -0.18 & 0.32 \\ 0.22 & -0.18 & 0.32 & 0.32 & -0.18 \\ 0.22 & -0.18 & 0.32 & 0.32 & -0.18 \\ 0.22 & 0.32 & -0.18 & -0.18 & 0.32 \end{bmatrix}$$

Μετά από τις απαραίτητες αναγωγές για τον προσδιορισμό των γραμμικώς ανεξάρτητων στηλών των παραπάνω πινάκων προκύπτουν τα ιδιοανύσματα του μετασχηματισμού Fourier.

Στην ιδιοτιμή 1 με πολλαπλότητα 2, αντιστοιχούν τα ιδιοανύσματα:

$$f_1 \approx \begin{pmatrix} 0 \\ 1 \\ -1 \\ -1 \\ 0 \end{pmatrix}, f_2 \approx \begin{pmatrix} 1 \\ 0 \\ 0.62 \\ 0.62 \\ 0 \end{pmatrix}$$

Στην ιδιοτιμή -1 με πολλαπλότητα 1 αντιστοιχεί το

$$f_3 \approx \begin{pmatrix} 1 \\ -0.81 \\ -0.81 \\ -0.81 \\ -0.81 \end{pmatrix}$$

Στην ιδιοτιμή i με πολλαπλότητα 1 αντιστοιχεί το

$$f_4 \approx \begin{pmatrix} 0 \\ 1 \\ 0.28 \\ -0.28 \\ -1 \end{pmatrix}$$

Τέλος,στην ιδιοτιμή $-i$ με πολλαπλότητα 1 αντιστοιχεί το

$$f_5 \approx \begin{pmatrix} 0 \\ 1 \\ -3.52 \\ 3.52 \\ -1 \end{pmatrix}$$

Με εφαρμογή της μεθόδου Gram-Schmidt,ορθογωνοποιούμε τα παραπάνω και προκύπτει το σύνολο των ιδιοανυσμάτων του μετασχηματισμού Fourier διάστασης 5.

$$\tilde{f}_1 \approx \begin{pmatrix} 0 \\ 0.5 \\ -0.5 \\ -0.5 \\ 0.5 \end{pmatrix}, \tilde{f}_2 \approx \begin{pmatrix} 0.85 \\ 0.26 \\ 0.26 \\ 0.26 \\ 0.26 \end{pmatrix}, \tilde{f}_3 \approx \begin{pmatrix} 0.53 \\ -0.42 \\ -0.42 \\ -0.42 \\ -0.42 \end{pmatrix}, \tilde{f}_4 \approx \begin{pmatrix} 0 \\ 0.68 \\ 0.19 \\ -0.19 \\ -0.68 \end{pmatrix}, \tilde{f}_5 \approx \begin{pmatrix} 0 \\ 0.19 \\ -0.68 \\ 0.68 \\ -0.19 \end{pmatrix}$$

4. Μορφή και ιδιότητες του Twisted μετασχηματισμού Fourier

Ο Twisted κβαντικός μετασχηματισμός Fourier, τον οποίο θα μελετήσουμε στο πλαίσιο της συγκεκριμένης εργασίας, ως μία παραλλαγή του κβαντικού μετασχηματισμού Fourier σε ανεξάρτητα συστήματα εμφανίστηκε αρχικά σαν ένα καθαρά μαθηματικό αντικείμενο στην περιοχή των modular Αλγεβρών. Αποτελεί μη-αναγωγίσιμη αναπαράσταση της πεπερασμένης ομάδας $SL(2, \mathbb{Z}_{2^N})$, $N \in \mathbb{N}$, δηλαδή της ειδικής (τα στοιχεία της έχουν ορίζουσα ίση με 1) γραμμικής ομάδας τάξης 2 των ακεραίων modulo 2^N [9].

Η δράση του στοιχείου αυτού της $SL(2, \mathbb{Z}_{2^N})$, μέσω της αντίστοιχης αναπαράστασης σε πίνακα με διάσταση $2^{2N} \times 2^{2N}$, ταυτίζεται με τη δράση του τανυστικού γινομένου δύο μετασχηματισμών Fourier με τη διάσταση του καθενός να είναι $2^N \times 2^N$, επί έναν ακόμα μετασχηματισμό, ο οποίος εναλλάσσει τις θέσεις των στηλών τους. Σύμφωνα με τα όσα αναφέραμε σε προηγούμενο κεφάλαιο, σε επίπεδο Κβαντομηχανικής αυτό σημαίνει ότι εάν έχουμε δύο ανεξάρτητα συστήματα, το καθένα από τα οποία αναπαρίσταται σε χώρο Hilbert διάστασης 2^N , τότε ο Twisted Fourier δρα στο συνολικό χώρο Hilbert διάστασης 2^{2N} των δύο συστημάτων, εφαρμόζοντας το μετασχηματισμό Fourier σε κάθε ένα από αυτά, εναλλάσσοντας τις θέσεις τους.

Συγκεκριμένα, ο Twisted μετασχηματισμός Fourier γράφεται:

$$TF_{j_1 k_1; j_2 k_2} = \frac{1}{\sqrt{2^{2N}}} \omega^{j_1 k_2 + j_2 k_1},$$

όπου $\omega = e^{\frac{2\pi i}{2^N}}$, δηλαδή το κοινό ω των επιμέρους μετασχηματισμών Fourier που τον συνθέτουν. Οι δείκτες $j_1, k_1, j_2, k_2 = 0, 1, \dots, 2^N - 1$ αναφέρονται στα επιμέρους συστήματα 1 και 2, ενώ για το συνολικό σύστημα έχουμε τους δείκτες $j, k = 0, 1, \dots, 2^{2N} - 1$, οι οποίοι εκφράζονται μέσω των προηγούμενων ως εξής:

$$j = j_1 2^N + j_2$$

$$k = k_1 2^N + k_2$$

Ισοδύναμα:

$$j_2 = j \mod 2^N$$

$$j_1 = j - j_2 \mod 2^N$$

και

$$k_2 = k \mod 2^N$$

$$k_1 = k - k \mod 2^N$$

Μπορούμε,λοιπόν να γράψουμε τον TF διάστασης 2^{2N} μέσω των αντίστοιχων F ,διάστασης 2^N ως εξής:

$$TF = (F \otimes F)P, \quad (17)$$

όπου ο P είναι ο μετασχηματισμός που προκαλεί την εναλλαγή (twist) που προαναφέραμε,η οποία με όρους δεικτών έχει ως εξής: $j_1 k_1 + j_2 k_2 \xrightarrow{P} j_1 k_2 + j_2 k_1$.

Ο P ικανοποιεί τις παρακάτω ιδιότητες:

- $P^2 = I$,όπου I ο ταυτοτικός πίνακας.
- $P(A \otimes B) = (B \otimes A)P$,όπου A, B οποιοιδήποτε πίνακες.

Στηριζόμενοι στη σχέση (17) και στις ιδιότητες των P και F μπορούμε να δείξουμε ότι ο TF είναι συμμετρικός και μοναδιαίος.

- Ο TF είναι συμμετρικός.

$$TF \cdot TF^T = (F \otimes F)P \cdot [(F \otimes F)P]^T = (F \otimes F)P \cdot P^T(F^T \otimes F^T)$$

Όμως $P \cdot P^T = I$,οπότε:

$$TF \cdot TF^T = (F \otimes F) \cdot (F^T \otimes F^T) = F \cdot F^T \otimes F \cdot F^T = I \otimes I = I$$

- Ο TF είναι μοναδιαίος.

$$TF \cdot TF^\dagger = (F \otimes F)P \cdot [(F \otimes F)P]^\dagger = (F \otimes F)P \cdot P^\dagger(F^\dagger \otimes F^\dagger)$$

Όμως $P \cdot P^\dagger = I$,οπότε:

$$TF \cdot TF^\dagger = (F \otimes F) \cdot (F^\dagger \otimes F^\dagger) = F \cdot F^\dagger \otimes F \cdot F^\dagger = I \otimes I = I$$

Κλείνοντας την ενότητα αυτή παραθέτουμε τους πίνακες που αναπαριστούν τον Twisted μετασχηματισμό Fourier σε δύο διαφορετικές περιπτώσεις.

Στην πρώτη απλούστερη περίπτωση θεωρούμε ότι $N = 1$.Ο αντίστοιχος χώρος Hilbert θα είναι το ταυστικό γινόμενο δύο χώρων Hilbert με διάσταση $2^N = 2^1 = 2$ ο καθένας,οπότε η διάστασή του θα είναι $2^N \times 2^N = 2 \times 2 = 4$ και

το ω θα έχει την τιμή $\omega = e^{\frac{2\pi i}{2^N}} = e^{\frac{2\pi i}{2}} = -1$.

Επιπλέον, θα ισχύει ότι $\omega^{2^N} = \omega^2 = 1$.

Λαμβάνουμε:

$$TF = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega \\ 1 & \omega & 1 & \omega \\ 1 & \omega & \omega & \omega^2 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Στην περίπτωση όπου $N = 2$, ο χώρος Hilbert θα είναι διάστασης $2^N \times 2^N = 2^2 \times 2^2 = 16$ και το ω θα έχει την τιμή $\omega = e^{\frac{2\pi i}{2^N}} = e^{\frac{2\pi i}{4}} = i$.

Επιπλέον, θα ισχύει ότι $\omega^{2^N} = \omega^4 = 1$.

Συνεπώς, ο πίνακας θα έχει ως εξής:

$$TF = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^3 & \omega^3 & \omega^3 & \omega^3 \\ 1 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^4 & \omega^4 & \omega^4 & \omega^4 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\ 1 & 1 & 1 & 1 & \omega^3 & \omega^3 & \omega^3 & \omega^3 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^3 & 1 & \omega & \omega^2 & \omega^3 & 1 & \omega & \omega^2 & \omega^3 & 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega & \omega^2 & \omega^3 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^2 & \omega^3 & \omega^4 & \omega & \omega^3 & \omega^4 & \omega & \omega^2 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^2 & \omega^3 & \omega^4 & \omega & \omega^4 & \omega & \omega^2 & \omega^3 & \omega^2 & \omega^3 & \omega^4 & \omega \\ 1 & \omega & \omega^2 & \omega^3 & \omega^3 & \omega^4 & \omega & \omega^2 & \omega^2 & \omega^3 & \omega^4 & \omega & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^2 & 1 & \omega^2 & \omega^4 & \omega^2 & 1 & \omega^2 & \omega^4 & \omega^2 & 1 & \omega^2 & \omega^4 & \omega^2 \\ 1 & \omega^2 & \omega^4 & \omega^2 & \omega & \omega^3 & \omega & \omega^3 & \omega^2 & \omega^4 & \omega^2 & \omega^4 & \omega^3 & \omega & \omega^3 & \omega \\ 1 & \omega^2 & \omega^4 & \omega^2 & \omega^2 & \omega^4 & \omega^2 & \omega^4 & \omega^4 & \omega^2 & \omega^4 & \omega^2 & \omega^2 & \omega^4 & \omega^2 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^2 & \omega^3 & \omega & \omega^3 & \omega & \omega^2 & \omega^4 & \omega^2 & \omega^4 & \omega & \omega^3 & \omega & \omega^3 \\ 1 & \omega^3 & \omega^2 & \omega & 1 & \omega^3 & \omega^2 & \omega & 1 & \omega^3 & \omega^2 & \omega & 1 & \omega^3 & \omega^2 & \omega \\ 1 & \omega^3 & \omega^2 & \omega & \omega & \omega^4 & \omega^3 & \omega^2 & \omega^2 & \omega & \omega^4 & \omega^3 & \omega^3 & \omega^2 & \omega & \omega^4 \\ 1 & \omega^3 & \omega^2 & \omega & \omega^2 & \omega & \omega^4 & \omega^3 & \omega^4 & \omega^3 & \omega^2 & \omega & \omega^2 & \omega & \omega^4 & \omega^3 \\ 1 & \omega^3 & \omega^2 & \omega & \omega^3 & \omega^2 & \omega & \omega^4 & \omega^2 & \omega & \omega^4 & \omega^3 & \omega & \omega^4 & \omega^3 & \omega^2 \end{bmatrix}$$

Αντικαθιστώντας τις δυνάμεις του ω , γίνεται:

$$TF = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i \\ 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1 \\ 1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i \\ 1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & -i & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -i & -1 & i & i & 1 & -i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1 \\ 1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i \\ 1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1 \end{bmatrix}$$

5. Ιδιοτιμές και ιδιοανύσματα του Twisted μετασχηματισμού Fourier

Στην ενότητα αυτή θα προσδιορίσουμε τις ιδιοτιμές και τα ιδιοανύσματα του Twisted μετασχηματισμού Fourier εφαρμόζοντας την ίδια μέθοδο όπως και στις ενότητες (3.1) και (3.2), με την οποία προσδιορίσαμε τις ιδιοτιμές και τα ιδιοανύσματα του κανονικού μετασχηματισμού Fourier. Αρχικά, από την (17) και με τη βοήθεια των ιδιοτήτων του P υπολογίζουμε και τις υπόλοιπες δυνάμεις του TF , λαμβάνοντας επιπλέον υπόψιν ότι ο F είναι συμμετρικός.

Έχουμε:

$$TF^2 = (F \otimes F)P(F \otimes F)P = (F \otimes F)^2 P^2 = F^2 \otimes F^2 = I' \otimes I'$$

$$TF^3 = (F \otimes F)P(F^2 \otimes F^2) = (F^3 \otimes F^3)P$$

Όμως, για τον F^3 ισχύει ότι $F^3 = F^*$, άρα η τελευταία σχέση γίνεται:

$$TF^3 = (F^* \otimes F^*)P = TF^*,$$

εφόσον ισχύει:

$$TF^* = [(F \otimes F)P]^* = P^*(F \otimes F)^* = P(F^* \otimes F^*)$$

Παραπάνω χρησιμοποιήσαμε το ότι $P^* = P$, αφού ο P είναι πραγματικός πίνακας.

$$TF^4 = (TF^2)^2 = (F^2 \otimes F^2)^2 = F^4 \otimes F^4 = I \otimes I = I$$

Η τελευταία σχέση $TF^4 = I$ είναι εξαιρετικά χρήσιμη, καθώς μας πληροφορεί ότι οι ιδιοτιμές του TF είναι οι i , $-i$, -1 και 1 .

Συνεχίζουμε υπολογίζοντας τα ίχνη των παραπάνω πινάκων, με σκοπό να βρούμε τις πολλαπλότητες των ιδιοτιμών αυτών.

$$\text{Tr}TF = \frac{1}{2^N} \sum_{j_1=0}^{2^N-1} \sum_{j_2=0}^{2^N-1} \omega^{2j_1j_2}$$

Για να το προσδιορίσουμε ακριβώς, γράφουμε:

$$\begin{aligned}
\text{TrTF} &= \frac{1}{2^N} \sum_{j_1=0}^{2^N-1} \sum_{j_2=0}^{2^N-1} (\omega^{2j_1})^{j_2} \\
&= \frac{1}{2^N} \sum_{j_1=0}^{2^N-1} \left(1 + \omega^{2j_1} + (\omega^{2j_1})^2 + \dots + (\omega^{2j_1})^{2^N-1} \right) \\
&= \frac{1}{2^N} \sum_{j_1=0}^{2^N-1} \frac{(\omega^{2j_1})^{2^N} - 1}{\omega^{2j_1} - 1},
\end{aligned}$$

ως άθροισμα όρων γεωμετρικής προόδου.

Για $j_1 = 0$ και $j_1 = \frac{2^N}{2}$ το τελευταίο κλάσμα δεν ορίζεται, αφού ο παρονομαστής γίνεται μηδέν. Συνεπώς, πρέπει να ξεχωρίσουμε αυτούς τους δύο προσθετέους.

Το άθροισμα $\left(1 + \omega^{2j_1} + (\omega^{2j_1})^2 + \dots + (\omega^{2j_1})^{2^N-1} \right)$ για $j_1 = 0$ και για $j_1 = \frac{2^N}{2}$ παίρνει την τιμή 2^N , ενώ το άθροισμα που απομένει είναι μηδέν.

Τελικά:

$$\text{TrTF} = \frac{1}{2^N} (2^N + 2^N) = 2,$$

για κάθε N .

$$\text{TrTF}^2 = \text{Tr}(F^2 \otimes F^2) = \text{Tr}F^2 \cdot \text{Tr}F^2 = (\text{Tr}F^2)^2 = 2^2 = 4,$$

αφού μας ενδιαφέρουν μόνο άρτιες διαστάσεις.

$$\text{TrTF}^3 = \text{TrTF}^* = (\text{TrTF})^* = 2$$

$$\text{TrTF}^4 = \text{Tr}(F^4 \otimes F^4) = \text{Tr}F^4 \cdot \text{Tr}F^4 = (\text{Tr}F^4)^2 = 2^{2N}$$

Από τα παραπάνω και δεδομένου ότι εν γένει ισχύει:

$$\text{tr}F^s = \sum_{i=1}^N \lambda_i^s,$$

προκύπτει το σύστημα των εξισώσεων από τη λύση του οποίου υπολογίζουμε τις πολλαπλότητες των ιδιοτιμών του TF :

$$m(1) - m(-1) + im(i) - im(-i) = 2$$

$$m(1) + m(-1) - m(i) - m(-i) = 4$$

$$m(1) - m(-1) - im(i) + im(-i) = 2$$

$$m(1) + m(-1) + m(i) + m(-i) = 2$$

Επιλύοντάς το λαμβάνουμε τελικά:

$$m(1, TF) = 2^{2N-2} + 2$$

$$m(-1, TF) = 2^{2N-2}$$

$$m(i, TF) = 2^{2N-2} - 1$$

$$m(-i, TF) = 2^{2N-2} - 1$$

Για να βρούμε τα ιδιοανύσματα του TF , ξεκινάμε εφαρμόζοντας το φασματικό θεώρημα, γνωρίζοντας πλέον ότι οι ιδιοτιμές του είναι οι $i, -i, -1$ και 1 .

$$TF = iTB(1) - TB(2) - iTB(3) + TB(4)$$

Για τους $TB(j)$ ισχύει εξ ορισμού ότι $TB(j)TB(k) = TB(j)\delta_{jk}$, $j, k = 1, 2, 3, 4$, οπότε για τις υπόλοιπες δυνάμεις του TF θα έχουμε:

$$TF^2 = -TB(1) + TB(2) - TB(3) + TB(4)$$

$$TF^3 = -iTB(1) - TB(2) + iTB(3) + TB(4)$$

$$TF^4 = TB(1) + TB(2) + TB(3) + TB(4) = I$$

Το γραμμικό αυτό σύστημα είναι το ίδιο με αυτό που είχε προκύψει και για τις δυνάμεις του F ως προς τους $B(j)$, και λύνοντάς το προκύπτουν οι $TB(j)$ ως εξής:

$$TB(1) = \frac{I - iTF - TF^2 + iTF^3}{4} \quad (18)$$

$$TB(2) = \frac{I - TF + TF^2 - TF^3}{4} \quad (19)$$

$$TB(3) = \frac{I + iTF - TF^2 - iTF^3}{4} \quad (20)$$

$$TB(4) = \frac{I + TF + TF^2 + TF^3}{4} \quad (21)$$

Ακολουθούμε κι εδώ την ίδια διαδικασία όπως και για τον F και γράφουμε:

$$\begin{aligned}
TF_{j_1 k_1; j_2 k_2} &= \frac{1}{2^N} \omega^{j_1 k_2 + j_2 k_1} \\
&= \frac{1}{2^N} e^{\frac{2\pi i}{2^N} (j_1 k_2 + j_2 k_1)} \\
&= \frac{1}{2^N} \left(\cos \left[\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1) \right] + i \sin \left[\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1) \right] \right)
\end{aligned}$$

Θέτοντας:

$$\begin{aligned}
TC_{j_1 k_1; j_2 k_2} &= \frac{1}{2^N} \cos \left[\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1) \right] \\
TS_{j_1 k_1; j_2 k_2} &= \frac{1}{2^N} \sin \left[\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1) \right]
\end{aligned}$$

ο TF μπορεί να γραφεί:

$$TF = TC + iTS \quad (22)$$

Στη συνέχεια εκφράζουμε και τις υπόλοιπες δυνάμεις του TF ως προς τους TC και TS .

$$TF^2 = (TC + iTS)^2 = TC^2 - TS^2 + i(TC \cdot TS + TS \cdot TC)$$

Όμως, έχουμε δείξει ότι $TF^2 = F^2 \otimes F^2 = I' \otimes I'$, όπου ο I' είναι πραγματικός πίνακας, άρα:

$$TF^2 = TC^2 - TS^2 \quad (23)$$

$$TF^3 = TF^* = TC - iTS \quad (24)$$

Τέλος,

$$TF^4 = I$$

Λύνοντας τις (22) και (24) ως προς TC, TS έχουμε:

$$TC = \frac{TF + TF^*}{2}$$

$$TS = \frac{TF - TF^*}{2i}$$

με τη βοήθεια των οποίων μπορούμε να αποδείξουμε όμοια με την ενότητα (3.2) τα εξής:

$$TC^3 = TC$$

$$TS^3 = TS$$

Επανερχόμενοι στις (18)-(21) μπορούμε να υπολογίσουμε πλέον τους $TB(j)$ μέσω των TC και TS . Προκύπτουν οι σχέσεις:

$$TB(1) = \frac{1}{2}TS + \frac{1}{4}(I - (TC^2 - TS^2))$$

$$TB(2) = -\frac{1}{2}TC + \frac{1}{4}(I + (TC^2 - TS^2))$$

$$TB(3) = -\frac{1}{2}TS + \frac{1}{4}(I - (TC^2 - TS^2))$$

$$TB(4) = \frac{1}{2}TC + \frac{1}{4}(I + (TC^2 - TS^2))$$

Ισοδύναμα, το $(j_1, k_1; j_2, k_2)$ στοιχείο των παραπάνω πινάκων θα δίνεται από τις:

$$[TB(1)]_{j_1, k_1; j_2, k_2} = \frac{1}{2^{N+1}} \sin\left(\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) + \frac{1}{4} \left(\delta_{j_1 2^N + j_2, k_1 2^N + k_2} - \frac{1}{2^{2N+2}} \cos\left(\frac{4\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) \right)$$

$$[TB(2)]_{j_1, k_1; j_2, k_2} = -\frac{1}{2^{N+1}} \cos\left(\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) + \frac{1}{4} \left(\delta_{j_1 2^N + j_2, k_1 2^N + k_2} + \frac{1}{2^{2N+2}} \cos\left(\frac{4\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) \right)$$

$$[TB(3)]_{j_1, k_1; j_2, k_2} = -\frac{1}{2^{N+1}} \sin\left(\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) + \frac{1}{4} \left(\delta_{j_1 2^N + j_2, k_1 2^N + k_2} - \frac{1}{2^{2N+2}} \cos\left(\frac{4\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) \right)$$

$$[TB(4)]_{j_1, k_1; j_2, k_2} = \frac{1}{2^{N+1}} \cos\left(\frac{2\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) + \frac{1}{4} \left(\delta_{j_1 2^N + j_2, k_1 2^N + k_2} - \frac{1}{2^{2N+2}} \cos\left(\frac{4\pi}{2^N} (j_1 k_2 + j_2 k_1)\right) \right)$$

Για τις παραπάνω χρησιμοποιήσαμε την τριγωνομετρική ταυτότητα:

$$\cos^2 \phi - \sin^2 \phi = \cos 2\phi$$

Άμεσα προκύπτει ότι $TFTB(j) = i^j TB(j)$, οπότε οι μη-μηδενικές στήλες του $TB(j)$ θα είναι ιδιοανύσματα του TF που θα αντιστοιχούν στην ιδιοτιμή i^j . Το πλήθος των γραμμικώς ανεξάρτητων σε κάθε περίπτωση θα δίνεται από τις αντίστοιχες πολλαπλότητες των ιδιοτιμών που βρήκαμε νωρίτερα.

Πιο συγκεκριμένα, όπως και στην αντίστοιχη ενότητα για τα ιδιοανύσματα του F , αν συνδυάσουμε τις τέσσερις τελευταίες σχέσεις για τους $TB(j)$ με τις σχέσεις που δίνουν τις πολλαπλότητες των ιδιοτιμών του TF και λάβουμε επιπλέον υπόψιν ότι οι ιδιοτιμές των TC και TS είναι 1, -1 ή 0, αφού $TC^3 = TC$ και

$TS^3 = TS$, ενώ οι ιδιοτιμές των $TB(j)$ είναι 1 ή 0 για κάθε j , αφού $TB(j)TB(k) = TB(j)\delta_{jk}$, $j, k = 1, 2, 3, 4$ προκύπτουν τα εξής:

$$\text{Tr}TB(1) = m(1, TB(1)) = m(1, TS) = m(i, TF) = 2^{2N-2} - 1$$

$$\text{Tr}TB(2) = m(1, TB(2)) = m(-1, TC) = m(-1, TF) = 2^{2N-2}$$

$$\text{Tr}TB(3) = m(1, TB(3)) = m(-1, TS) = m(-i, TF) = 2^{2N-2} - 1$$

$$\text{Tr}TB(4) = m(1, TB(4)) = m(1, TC) = m(1, TF) = 2^{2N-2} + 2$$

Τελικά, το σύνολο των ιδιοανυσμάτων του TF που αντιστοιχούν στην ιδιοτιμή i^j θα είναι το σύνολο των $m(1, TB(j))$ γραμμικώς ανεξάρτητων στηλών του $TB(j)$ που μπορούν και πάλι να ορθογωνοποιηθούν με τη μέθοδο *Gram-Schmidt*.

5.1. Εφαρμογή για $N = 2$

Στη συγκεκριμένη ενότητα θα παραθέσουμε το τελικό αποτέλεσμα που προκύπτει από την εφαρμογή της παραπάνω διαδικασίας στην περίπτωση που έχουμε δύο συστήματα διάστασης 2^N με $N = 2$ το κάθε ένα. Ο αντίστοιχος πίνακας που αναπαριστά τον Twisted κβαντικό μετασχηματισμό Fourier έχει ήδη υπολογιστεί στο Κεφάλαιο 4.

Το ίχνος του TF είναι 2 και οι πολλαπλότητες των ιδιοτιμών $1, -1, i$ και $-i$ είναι αντίστοιχα 6, 4, 3 και 3.

Στην ιδιοτιμή 1 αντιστοιχούν τα ιδιοανύσματα:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -2 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ -2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Στην ιδιοτιμή -1 αντιστοιχούν τα ιδιοανύσματα:

$$\begin{pmatrix} -\frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ -\frac{1}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ \frac{1}{2} \\ 0 \\ -\frac{1}{2} \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Στην ιδιοτιμή i αντιστοιχούν τα ιδιοανύσματα:

$$\begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ -1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ -1 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Στην ιδιοτιμή $-i$ αντιστοιχούν τα ιδιοανύσματα:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \\ -1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \\ -1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

5.2. Σχέση μεταξύ των ιδιοανυσμάτων του μετασχηματισμού Fourier και του Twisted μετασχηματισμού Fourier

Στην ενότητα αυτή, θα δείξουμε με ποιό τρόπο μπορούμε να κατασκευάσουμε ιδιοανύσματα του Twisted μετασχηματισμού Fourier διάστασης 2^{2N} , τα οποία θα είναι ορθογώνια μεταξύ τους, εάν διαθέτουμε ορθογώνια μεταξύ τους ιδιοανύσματα του μετασχηματισμού Fourier, διάστασης 2^N [8][5, IV], [7].

Έστω, λοιπόν, $\{|e_k\rangle\}$, $k = 0, 1, \dots, 2^N - 1$ το σύνολο των ιδιοανυσμάτων του μετασχηματισμού Fourier διάστασης 2^N , τα οποία είναι ορθογώνια μεταξύ τους.

Θα ισχύουν:

$$F|e_k\rangle = i^k |e_k\rangle$$

$$\langle e_k, e_m \rangle = \delta_{k,m}$$

Το σύνολο $\{|e_k\rangle \otimes |e_l\rangle\}$, $k, l = 0, 1, \dots, 2^N - 1$ αποτελεί ορθοκανονική βάση του χώρου Hilbert διάστασης 2^{2N} , σύμφωνα με αυτά που γνωρίζουμε για το ταυσιτικό γινόμενο των χώρων Hilbert.

Η δράση του Twisted μετασχηματισμού Fourier σε αυτά θα έχει ως εξής:

$$TF|e_k\rangle\otimes|e_l\rangle = (F\otimes F)P|e_k\rangle\otimes|e_l\rangle = F\otimes F|e_l\rangle\otimes|e_k\rangle = i^l|e_l\rangle\otimes i^k|e_k\rangle = i^{l+k}|e_l\rangle\otimes|e_k\rangle$$

Ορίζουμε:

$$|\tilde{e}_{k,l}^+\rangle = \frac{|e_k\rangle\otimes|e_l\rangle + |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}}$$

$$|\tilde{e}_{k,l}^-\rangle = \frac{|e_k\rangle\otimes|e_l\rangle - |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}}$$

Εύκολα ελέγχουμε ότι τα $|\tilde{e}_{k,l}^+\rangle, |\tilde{e}_{k,l}^-\rangle$ είναι ορθογώνια μεταξύ τους:

$$\langle\tilde{e}_{k,l}^+, \tilde{e}_{k,l}^+\rangle = 1$$

$$\langle\tilde{e}_{k,l}^-, \tilde{e}_{k,l}^-\rangle = 1$$

$$\langle\tilde{e}_{k,l}^+, \tilde{e}_{k,l}^-\rangle = 0$$

$$\langle\tilde{e}_{k,l}^-, \tilde{e}_{k,l}^+\rangle = 0$$

Μένει να δείξουμε ότι είναι και ιδιοανύσματα του TF .

$$TF|\tilde{e}_{k,l}^+\rangle = TF\frac{|e_k\rangle\otimes|e_l\rangle + |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(i^{l+k}|e_l\rangle\otimes|e_k\rangle + i^{k+l}|e_k\rangle\otimes|e_l\rangle)$$

$$TF|\tilde{e}_{k,l}^+\rangle = i^{k+l}\frac{|e_k\rangle\otimes|e_l\rangle + |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}} = i^{k+l}|\tilde{e}_{k,l}^+\rangle$$

$$TF|\tilde{e}_{k,l}^-\rangle = TF\frac{|e_k\rangle\otimes|e_l\rangle - |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(i^{l+k}|e_l\rangle\otimes|e_k\rangle - i^{k+l}|e_k\rangle\otimes|e_l\rangle)$$

$$TF|\tilde{e}_{k,l}^-\rangle = -i^{k+l}\frac{|e_k\rangle\otimes|e_l\rangle - |e_l\rangle\otimes|e_k\rangle}{\sqrt{2}} = -i^{k+l}|\tilde{e}_{k,l}^-\rangle$$

Άρα, πράγματι, τα $\left| \tilde{e}_{k,l}^+ \right\rangle$ είναι ιδιοανύσματα του TF που αντιστοιχούν στην ιδιοτιμή i^{k+l} , ενώ τα $\left| \tilde{e}_{k,l}^- \right\rangle$ είναι ιδιοανύσματα του TF που αντιστοιχούν στην ιδιοτιμή $-i^{k+l}$, $k, l = 0, 1, \dots, 2^N - 1$.

Τέλος, υπολογίζοντας το πλήθος των $\left| \tilde{e}_{k,l}^+ \right\rangle, \left| \tilde{e}_{k,l}^- \right\rangle$ επιβεβαιώνουμε ότι με τον τρόπο αυτό προκύπτουν όλα τα ιδιοανύσματα του TF διάστασης 2^{2N} .

Τα $\left| \tilde{e}_{k,l}^+ \right\rangle$ είναι $\frac{2^N(2^N+1)}{2}$ το πλήθος, ενώ τα $\left| \tilde{e}_{k,l}^- \right\rangle$ είναι $\frac{2^N(2^N-1)}{2}$.

Προσθέτοντας, λαμβάνουμε τα 2^{2N} ιδιοανύσματα του TF διάστασης 2^{2N} .

Μέρος II.

Ο κβαντικός μετασχηματισμός Fourier και ο Twisted κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική

6. Σύντομη εισαγωγή στην Κβαντική Πληροφορική

6.1. Γενικά περί Κβαντικής Πληροφορικής

Τις τελευταίες δεκαετίες, η Κβαντική Πληροφορική αποτελεί πεδίο συστηματικής έρευνας, καθώς υπόσχεται το σχεδιασμό κβαντικών αλγορίθμων και υπολογιστών που θα επιλύουν ικανοποιητικά, προβλήματα τα οποία είναι εξαιρετικά δυσεπίλυτα σε κλασικούς υπολογιστές. Ο συνδυασμός Πληροφορικής και Κβαντομηχανικής προέκυψε ως αποτέλεσμα δύο διαφορετικών διαδικασιών. Από τη μία, υπήρχε το πρακτικό πρόβλημα που προέκυπτε κατά τη χρήση των transistors στερεάς κατάστασης στους κλασικούς υπολογιστές. Από τη στιγμή που εμφανίστηκαν έως και σήμερα, οι διαστάσεις τους έχουν μειωθεί ιδιαίτερα, με αποτέλεσμα τα κβαντικά φαινόμενα που εμφανίζονται να γίνονται όλο και πιο σημαντικά και να επηρεάζουν τη λειτουργία τους. Συνεπώς, δεν είναι δυνατόν να αγνοηθούν και το ερώτημα που ανέκυψε είναι το κατά πόσον μπορούν πλέον να σχεδιαστούν λειτουργικά κυκλώματα. Η απάντηση είναι ότι μπορούν, αρκεί να αλλάξουν δραστικά οι αρχές σχεδιασμού τους. Ένας τρόπος είναι ο επανασχεδιασμός να γίνεται ώστε η ίδια η πληροφορία να μεταδίδεται κβαντομηχανικά. Ο κβαντικός υπολογιστής είναι αχρι-

βώς η μηχανή,η οποία υλοποιεί τέτοια κυκλώματα.

Από την άλλη πλευρά,επικρατούσε το καθαρά θεωρητικό ενδιαφέρον,σχετικά με το πώς μπορεί να γενικευτεί η σύνδεση μεταξύ Πληροφορικής και Φυσικής στο πεδίο της Κβαντομηχανικής.

Επιπλέον,υπήρχε η ανάγκη για γρηγορότερους υπολογιστές που θα λύνουν με αποτελεσματικό τρόπο (δηλαδή,οι αντίστοιχοι αλγόριθμοι να λύνουν ένα πρόβλημα σε χρόνο πολυωνυμικό σε σχέση με το μέγεθός του),προβλήματα τα οποία οι κλασικοί υπολογιστές δεν μπορούν να λύσουν ικανοποιητικά,όπως το πρόβλημα του διακριτού λογαρίθμου,το πρόβλημα της εύρεσης των πρώτων παραγόντων ενός ακεραίου,καθώς και το πρόβλημα της αναζήτησης εντός μίας μη δομημένης βάσης δεδομένων.

Όπως ακριβώς τα κλασσικά υπολογιστικά συστήματα συντίθενται από συστήματα δύο καταστάσεων,τα λεγόμενα bits,έτσι και τα κβαντικά υπολογιστικά συστήματα συντίθενται από αντίστοιχα συστήματα δύο καταστάσεων,τα qubits.Η διαφορά μεταξύ bit και qubit είναι ότι,ενώ ένα bit μπορεί να βρίσκεται είτε στην κατάσταση 0 είτε στην κατάσταση 1,ένα qubit μπορεί ταυτόχρονα να βρίσκεται και στις δύο καταστάσεις,με διαφορετικό πλάτος πιθανότητας για την κάθε μία.Συνεπώς,για να προσδιορίσουμε πλήρως ένα qubit,πρέπει να προσδιορίσουμε τα πλάτη πιθανότητας των δύο καταστάσεων,δηλαδή χρειαζόμαστε δύο μιγαδικούς αριθμούς,σε αντίθεση με την κλασική περίπτωση που αρκεί ένα bit πληροφορίας. Αντιλαμβανόμαστε,λοιπόν,ότι το βασικό πλεονέκτημα ενός κβαντικού υπολογιστή που μπορούμε να αξιοποιήσουμε είναι ακριβώς αυτός ο εσωτερικός παραλληλισμός,ο οποίος επιτρέπει να εκτελούνται ταυτόχρονα πολλαπλές υπολογιστικές διαδικασίες. Το πρόβλημα,όμως,που ανακύπτει είναι ότι,ενώ όλες οι απαντήσεις των υπολογιστικών διαδικασιών βρίσκονται εντός του συστήματος,λόγω της ευαισθησίας του ως προς την παρατήρηση(βλ.“κατάρρευση” της κυματοσυνάρτησης) δεν υπάρχει εύκολος τρόπος να εξάγουμε κάθε φορά όλες αυτές τις πληροφορίες.Συνεπώς,οι κβαντικοί αλγόριθμοι θα πρέπει να σχεδιάζονται ώστε να μη χρειάζεται να γίνει κάποια παρατήρηση προτού ολοκληρωθεί η εκάστοτε υπολογιστική διαδικασία.Για το λόγο αυτό αμφισβητήθηκε το κατά πόσον,σε πρακτικό επίπεδο,ένας κβαντικός υπολογιστής είναι όντως γρηγορότερος από έναν κλασικό.Εν τέλει,ο σχεδιασμός των γρήγορων κβαντικών αλγορίθμων αναζήτησης και παραγοντοποίησης ανέδειξε την αποτελεσματικότητα των κβαντικών υπολογιστών.

6.2. Κβαντικά bits (qubits), κβαντικές πύλες και κβαντικά κυκλώματα

6.2.1. Κβαντικά bits (qubits)

Οποιοδήποτε κβαντικό σύστημα δύο καταστάσεων μπορεί να χρησιμοποιηθεί ως qubit. Για παράδειγμα, ένα ηλεκτρόνιο με τις δύο καταστάσεις του spin του, (πάνω και κάτω) ή ένα φωτόνιο με τις δύο καταστάσεις της πόλωσής του (οριζόντια και κάθετη). Θεωρούμε τις πιθανές καταστάσεις στις οποίες μπορεί να βρεθεί ένα qubit όταν μετρηθεί να είναι οι $|0\rangle$ και $|1\rangle$, σε αντιστοιχία με τις κλασσικές 0 και 1 για το bit. Οι καταστάσεις αυτές είναι οι καταστάσεις βάσης και αναπαρίστανται από τα διανύσματα βάσης ενός χώρου Hilbert διάστασης 2 ως εξής:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ένα qubit στη γενική του μορφή είναι η γραμμική υπέρθεση των καταστάσεων βάσης

$$|k\rangle = \alpha |0\rangle + \beta |1\rangle,$$

όπου α και β είναι το πλάτος πιθανότητας το σύστημα να βρεθεί στην κατάσταση $|0\rangle$ και $|1\rangle$ αντίστοιχα. Όπως ήδη γνωρίζουμε τα α και β είναι, εν γένει, μιγαδικοί αριθμοί, με $|\alpha|^2$ να είναι η πιθανότητα το σύστημα μετά τη μέτρηση να βρεθεί στην κατάσταση $|0\rangle$ και $|\beta|^2$ η πιθανότητα να βρεθεί στην κατάσταση $|1\rangle$. Επίσης, ικανοποιούν τη σχέση:

$$|\alpha|^2 + |\beta|^2 = 1,$$

η οποία εξασφαλίζει ότι οι $|0\rangle$ και $|1\rangle$ είναι οι μοναδικές καταστάσεις στις οποίες μπορεί να βρεθεί το σύστημα. Η αναπαράστασή του στο χώρο Hilbert διάστασης 2 θα είναι

$$|k\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Στα κλασικά υπολογιστικά συστήματα οι πληροφορίες δίνονται στη μορφή σειρών bits (string bits), οι οποίες αποτελούνται από περισσότερα από ένα bit, εν γένει N το πλήθος. Εντελώς ανάλογα και στην κβαντική περίπτωση έχουμε συστήματα με N qubits, τα οποία αναπαρίστανται σε χώρο Hilbert 2^N διαστάσεων

(αφού το κάθε qubit αναπαρίσταται σε διδιάστατο χώρο Hilbert) και οι αντίστοιχες καταστάσεις προκύπτουν από το ταυστικό γινόμενο των επιμέρους N qubits. Παρακάτω, φαίνεται πώς προκύπτουν οι καταστάσεις βάσης συστημάτων 2 και 3 qubits, σύμφωνα με αυτά που έχουμε αναφέρει για το ταυστικό γινόμενο χώρων Hilbert. Στην περίπτωση ενός συστήματος με 2 qubits τα διανύσματα βάσης θα είναι:

$$|0\rangle = |0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle = |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|2\rangle = |1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |3\rangle = |1\rangle \otimes |1\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Για ένα σύστημα με 3 qubits τα διανύσματα βάσης θα είναι:

$$|0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle = |001\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|2\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = |010\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |3\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{aligned}
|4\rangle &= |1\rangle \otimes |0\rangle \otimes |0\rangle = |100\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, & |5\rangle &= |1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\
|6\rangle &= |1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, & |7\rangle &= |1\rangle \otimes |1\rangle \otimes |1\rangle = |111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
\end{aligned}$$

6.2.2. Κβαντικές πύλες

Όταν σκοπεύουμε να σχεδιάσουμε υπολογιστικά συστήματα χρειαζόμαστε και κάποιες πύλες, με τη βοήθεια των οποίων “κτίζουμε” τους αλγόριθμους. Στην κλασική Πληροφορική τέτοιες πύλες είναι για παράδειγμα οι NOT, NAND και NOR. Κι ενώ η πρώτη χρησιμοποιείται και στην κβαντική Πληροφορική, οι άλλες δύο δεν μπορούν να χρησιμοποιηθούν, καθώς, αν θεωρήσουμε τους αντίστοιχους πίνακες μετασχηματισμού, θα δούμε ότι αυτοί δεν είναι μοναδιαίοι (unitary). Η απαίτηση να είναι μοναδιαίος ένας μετασχηματισμός για να μπορεί να εφαρμοστεί σε έναν κβαντικό αλγόριθμο, προκύπτει από δύο πολύ σημαντικά χαρακτηριστικά της κβαντομηχανικής δομής. Το πρώτο είναι ότι σε κάθε μετάβαση πρέπει να διατηρείται η συνολική πιθανότητα ίση με 1 και το δεύτερο είναι ότι η εξέλιξη ενός κβαντικού συστήματος είναι γραμμική ως προς τα πλάτη πιθανότητας. Σε συνδυασμό, λοιπόν, αυτές οι δύο ιδιότητες επιβάλλουν οι boolean πύλες που γίνονται δεκτές να είναι μόνον οι *αντιστρέψιμες* (αντιστρέψιμη πύλη είναι αυτή για την οποία μπορούμε να ανακτήσουμε την τιμή στην είσοδο, εάν γνωρίζουμε την τιμή στην έξοδο). Παράδειγμα αντιστρέψιμης πύλης είναι η NOT, ενώ η NAND είναι μη αντιστρέψιμη. Γενικά, έχει αποδειχθεί ότι οποιαδήποτε υπολογιστική διαδικασία σε έναν κλασικό υπολογιστή μπορεί να υλοποιηθεί εξίσου αποτελεσματικά από έναν κβαντικό υπολογιστή με συγκρίσιμο hardware. Αυτό σημαίνει ότι κάθε bo-

olean συνάρτηση που υπολογίζεται από έναν κλασικό υπολογιστή με τη βοήθεια NAND και NOR πυλών, μπορεί να υπολογιστεί και από ένα κβαντικό κύκλωμα που έχει περίπου το ίδιο μέγεθος και αποτελείται εξ' ολοκλήρου από αντιστρέψιμες πύλες. Αμέσως παρακάτω, παρουσιάζονται τρεις βασικές κβαντικές πύλες που θα χρησιμοποιήσουμε αργότερα.

- ΠΥΛΗ HADAMARD

Η πύλη HADAMARD δέχεται στην είσοδό της ένα qubit και το μετασχηματίζει σε γραμμικό συνδυασμό των $|0\rangle$ και $|1\rangle$.

Αναπαρίσταται από τον πίνακα:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

και η δράση της στις καταστάσεις βάσης δίνεται από τις σχέσεις:

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

οι οποίες συνοπτικά γράφονται:

$$H|k\rangle = \frac{1}{\sqrt{2}} \left((-1)^k |k\rangle + |1-k\rangle \right) \quad (25)$$

Μια ισοδύναμη μορφή της (25) είναι η εξής:

$$H|k\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\pi k} |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + e^{2i\pi 0.k} |1\rangle) \quad (26)$$

Εύκολα βλέπουμε ότι ο μετασχηματισμός αυτός είναι μοναδιαίος (αφού οι στηλές του είναι ορθοκανονικές) και επιπλέον ότι ισχύει $H = H^{-1} \iff HH = I$ (self-inverse).

Αξίζει, τέλος να σημειώσουμε ότι ο κβαντικός μετασχηματισμός Fourier αποτελεί μια φυσιολογική γενίκευση της πύλης HADAMARD που επιτρέπει τον προσδιορισμό της πληροφορίας που βρίσκεται κωδικοποιημένη εντός της φάσης μιας κβαντικής κατάστασης, όπως θα δούμε στο επόμενο κεφάλαιο.

- ΠΥΛΗ ΜΕΤΑΤΟΠΙΣΗΣ ΦΑΣΗΣ (phase shift)

Η πύλη μετατόπισης φάσης $B_N = B\left(\frac{2\pi}{2^N}\right)$ δέχεται στην είσοδό της ένα qubit και το πολλαπλασιάζει με μία φάση $e^{i2\pi/2^N}$, όπως φαίνεται από την αναπαράστασή της σε πίνακα:

$$B_N = \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^N} \end{bmatrix}$$

Υπενθυμίζουμε ότι ο αριθμός $e^{i2\pi/2^N}$ είναι η ρίζα της μονάδας τάξης 2^N . Η δράση της στα στοιχεία της βάσης δίνεται από τις σχέσεις:

$$B_N |0\rangle = |0\rangle$$

$$B_N |1\rangle = e^{i2\pi/2^N} |1\rangle$$

οι οποίες συνοψίζονται στην:

$$B_N |k\rangle = e^{i2\pi k/2^N} |k\rangle \quad (27)$$

Η πύλη μετατόπισης φάσης χρησιμοποιείται και με 2 qubits στην είσοδό της, το ένα εκ των οποίων χρησιμοποιείται ως qubit ελέγχου (control qubit) και το άλλο ως qubit-στόχος (target qubit). Στην περίπτωση αυτή, εάν το qubit ελέγχου είναι το $|0\rangle$, τότε η πύλη μετατόπισης φάσης -η οποία πλέον ονομάζεται Control Phase Shift και συμβολίζεται με $C - B_N$ -αφήνει και τα δύο qubits ίδια, ενώ εάν το qubit ελέγχου είναι το $|1\rangle$, τότε προσδίδει στο qubit-στόχο, φάση ίση με $e^{i2\pi/2^N}$, όπως και πριν και αφήνει ίδιο το qubit ελέγχου.

Η αναπαράστασή της σε πίνακα πλέον θα είναι:

$$C - B_N = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i2\pi/2^N} \end{bmatrix}$$

Εύκολα ελέγχουμε ότι ο μετασχηματισμός μετατόπισης φάσης είναι επίσης μοναδιαίος, ως οφείλει.

- ΠΥΛΗ ΑΝΤΙΣΤΡΟΦΗΣ QUBITS (SWAP)

Τέλος, έχουμε την πύλη SWAP, η οποία δέχεται στην είσοδό της δύο qubits και εναλλάσσει τις θέσεις τους στο κύκλωμα. Δηλαδή:

$$\text{SWAP} |k_1 k_2\rangle = |k_2 k_1\rangle$$

Ο πίνακας που την αναπαριστά έχει ως εξής:

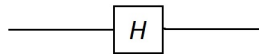
$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Η SWAP υλοποιείται από 3 διαδοχικές πύλες Control Not(οι οποίες είναι γνωστές από την κλασική Πληροφορική και χρησιμοποιούνται και στην κβαντική) που χρησιμοποιούν τα δύο qubits εναλλάξ ως ελέγχου και στόχο. Ο πίνακας που αναπαριστά μία πύλη Control Not είναι:

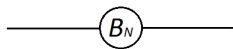
$$\text{C-NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Τέλος, παραθέτουμε το συμβολισμό των παραπάνω πυλών στα κβαντικά κυκλώματα.

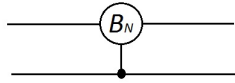
- HADAMARD



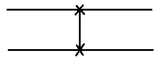
- PHASE SHIFT



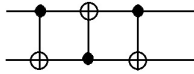
- CONTROL-PHASE SHIFT



- SWAP



- $\text{SWAP} \equiv 3 \text{ CONTROL-NOT}$



6.2.3. Κβαντικά Κυκλώματα

Το μοντέλο των κβαντικών κυκλωμάτων περιλαμβάνει qubits τα οποία μεταφέρονται κατά μήκος συρμάτων και ένα πεπερασμένο διακριτό σύνολο από κβαντικές πύλες (δηλαδή μοναδιαίους μετασχηματισμούς) οι οποίες δρουν σε αυτά. Σημειώνουμε ότι το σύρμα σε ένα κβαντικό κύκλωμα δεν αντιστοιχεί απαραίτητα σε φυσικό σύρμα, αλλά μπορεί να αντιστοιχεί σε χρονικό διάστημα που μεσολαβεί ή σε κάποιο σωματίδιο, όπως π.χ. ένα φωτόνιο, το οποίο κινείται στο χώρο από μία θέση σε μία άλλη. Τα qubits διαδίδονται με το πέρασμα του χρόνου κατά μήκος των συρμάτων από αριστερά προς τα δεξιά. Μία κβαντική πύλη δέχεται στην είσοδό της N qubits τα οποία μεταφέρονται από N σύρματα και N άλλα σύρματα οδηγούν τα N qubits της εξόδου της, μακριά από αυτήν.

Τέλος, θα αναφέρουμε κάποια χαρακτηριστικά των κλασικών κυκλωμάτων, τα οποία όμως δεν παρουσιάζονται στα κβαντικά κυκλώματα. Κατ' αρχάς στα κβαντικά κυκλώματα δεν επιτρέπεται να υπάρχουν βρόχοι, δηλαδή ένα τμήμα του κυκλώματος να τροφοδοτεί ένα άλλο. Λέμε, λοιπόν, ότι τα κβαντικά κυκλώματα είναι **ακυκλικά**. Επίσης, στα κλασικά κυκλώματα δύο σύρματα μπορούν να ενωθούν σε ένα (*FANIN*), κάτι το οποίο δεν μπορεί να συμβεί στα κβαντικά, εφ' όσον η διαδικασία αυτή δεν είναι αντιστρέψιμη (δηλαδή, ο αντίστοιχος μετασχηματισμός δεν είναι μοναδιαίος). Επιπλέον, και η αντίστροφη διαδικασία (*FANOUT*), κατά την οποία παράγονται αντίγραφα ενός bit, δεν επιτρέπεται σε ένα κβαντικό κύκλωμα. Για την ακρίβεια ισχύει το εξής θεώρημα (*no-cloning theorem*):

Θεώρημα 2. Έστω ένα qubit στην κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Είναι αδύνατον να σχεδιαστεί μηχανή, η οποία για όλες τις δυνατές καταστάσεις $|\psi\rangle$, να μπορεί να δεχθεί την $|\psi\rangle$ και να δημιουργήσει δύο αντίγραφα αυτής $|\psi\rangle \otimes |\psi\rangle$, δηλαδή να “κλωνοποιήσει” την κβαντική κατάσταση.

7. Ο κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική

7.1. Εφαρμογές του κβαντικού αλγορίθμου

Όπως έχουμε ήδη αναφέρει, ένας κβαντικός υπολογιστής μπορεί να λύσει αποτελεσματικά κάποια προβλήματα, τα οποία δεν λύνονται από κλασικό υπολογιστή. Μία από τις βασικές κατηγορίες κβαντικών αλγορίθμων είναι αυτοί που λύνουν προβλήματα με πολυπλοκότητα υπερπολυωνυμικά μικρότερη από αυτήν του αντίστοιχου καλύτερου γνωστού κλασικού αλγορίθμου. Η πλειονότητα αυτών κάνει χρήση του κβαντικού μετασχηματισμού Fourier, ο οποίος είναι ένας αποτελεσματικός αλγόριθμος που εκτελεί το μετασχηματισμό Fourier κβαντομηχανικών πλατών πιθανότητας. Η αποτελεσματικότητα αυτών των αλγορίθμων βασίζεται στο ότι ο μετασχηματισμός Fourier μπορεί να υλοποιηθεί από ένα αποτελεσματικό κβαντικό κύκλωμα, όπως ανακαλύφθηκε από τον Peter Shor.

Πριν περάσουμε στη μελέτη του, που είναι και το βασικό αντικείμενο του κεφαλαίου αυτού, θα αναφέρουμε τα προβλήματα των οποίων την επίλυση διευκολύνει και παρουσιάζουν ιδιαίτερο ενδιαφέρον.

- **Εκτίμηση Φάσης**

Το πρόβλημα εκτίμησης φάσης θεωρείται θεμελιώδες πρόβλημα αυτής της κατηγορίας, καθώς ο σχεδιασμός του κβαντικού αλγορίθμου που το επιλύει μας οδηγεί άμεσα και φυσιολογικά στον κβαντικό μετασχηματισμό Fourier. Στο πρόβλημα αυτό, για μία κατάσταση

$$|k\rangle = \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} e^{2\pi i \omega j} |j\rangle,$$

καλούμαστε να βρούμε μία καλή εκτίμηση της παραμέτρου φάσης ω . Για την ακρίβεια, ο αλγόριθμος αυτός είναι η εκτέλεση του αντίστροφου κβαντικού μετασχηματισμού Fourier, ο οποίος μας δίνει, πράγματι, μια πολύ καλή εκτίμηση για την ω .

Επιπλέον, η επίλυση αρκετών σημαντικών προβλημάτων, ανάγεται στην επίλυση αυτού, όπως για παράδειγμα η **Εύρεση της Περιόδου μιας Περιοδικής Κατάστασης**, η **Προσέγγιση των Ιδιοτιμών ενός Μοναδιαίου Τελεστή**, καθώς και η **Εύρεση Τάξης ενός Ακεραίου**. Τέλος εάν ο αλγόριθμος εκτίμησης φάσης συνδυαστεί με τον κβαντικό αλγόριθμο αναζήτησης του Grover προκύπτει ένας αποτελεσματικός

κβαντικός αλγόριθμος για τη *Μέτρηση Λύσεων σε Προβλήματα Αναζήτησης*.

- **Εύρεση των Πρώτων Παραγόντων ενός Ακεραίου**

Το πρόβλημα αυτό είναι ένα πολύ “διάσημο” πρόβλημα Μαθηματικών, στο οποίο καλούμαστε για κάποιον ακέραιο N να βρούμε θετικούς ακεραίους $p_1, p_2, \dots, p_l, r_1, r_2, \dots, r_l$,

όπου οι p_i είναι διαφορετικοί μεταξύ τους πρώτοι αριθμοί ώστε το N να γράφεται στη μορφή: $N = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_l^{r_l}$.

Η πολυπλοκότητα του καλύτερου μέχρι τώρα γνωστού κλασικού αλγορίθμου για αυτό είναι πολύ μεγάλη: $\exp(O(N^{\frac{1}{3}} (\log N)^{\frac{2}{3}} N))$, καθιστώντας το πρόβλημα της παραγοντοποίησης -ακόμα και σχετικά μικρών ακεραίων- εξαιρετικά δυσεπίλυτο. Για το λόγο αυτό, το σύστημα κρυπτογραφίας RSA που χρησιμοποιείται ευρέως, βασίζει την ασφάλειά του σε αυτήν ακριβώς τη διαπίστωση, ότι δηλαδή, είναι δύσκολο για έναν κλασικό υπολογιστή να παραγοντοποιήσει μεγάλους ακεραίους. Το 1994 ο Peter Shor δημοσίευσε ένα άρθρο-σταθμό [10] για την Κβαντική Πληροφορική στο οποίο παρουσίασε τον *αποτελεσματικό* κβαντικό αλγόριθμο παραγοντοποίησης, βασιζόμενος στο ότι το πρόβλημα της εύρεσης των πρώτων παραγόντων ενός ακεραίου μπορεί να αναχθεί στο πρόβλημα εύρεσης τάξης ενός ακεραίου. Σε αντίθεση με την κλασική περίπτωση, ο κβαντικός αλγόριθμος παραγοντοποίησης έχει *εκθετικά μικρότερη πολυπλοκότητα*: $O(N^2 \log N \log \log N)$.

Η ανακάλυψη αυτή του Shor είναι τεράστιας επιστημονικής αξίας, αφού κατάφερε να λύσει ένα πρόβλημα για το οποίο δεν υπήρχε ικανοποιητική λύση έως τότε. Πέραν αυτού, όμως, το γεγονός ότι το σύστημα κρυπτογραφίας RSA δεν είναι πλέον ασφαλές, έστρεψε το ενδιαφέρον της βιομηχανίας στην Κβαντική Πληροφορική με σκοπό να αναπτυχθεί και ο κλάδος της Κβαντικής Κρυπτογραφίας, ο οποίος θα παρέχει ασφαλή κβαντικά συστήματα κρυπτογραφίας. Δικαίως, λοιπόν, αυτή η ανακάλυψη του Shor θεωρείται κομβική στην εξέλιξη της Κβαντικής Πληροφορικής.

Στη συνέχεια, ο Shor και πάλι, κατάφερε να σχεδιάσει έναν αποτελεσματικό κβαντικό αλγόριθμο για την επίλυση του προβλήματος του **Διακριτού Λογαρίθμου στο \mathbb{Z}_p^*** , το οποίο ανάγεται στο πρόβλημα της παραγοντοποίησης και αποτελεί επίσης τη βάση κλασικών κρυπτοσυστημάτων, λόγω της μη-επιλυσιμότητάς του από κλασικό υπολογιστή.

Τέλος, ο συνδυασμός των κβαντικών αλγορίθμων για το πρόβλημα εύρεσης τάξης και διακριτού λογαρίθμου οδηγεί στο σχεδιασμό κβαντικού αλγορίθ-

μου που επιλύει αποτελεσματικά το πρόβλημα των **Κρυμμένων Υποομάδων**, εάν περιοριστούμε σε πεπερασμένες αβελιανές ομάδες. Ο σχεδιασμός αλγορίθμου που θα το επιλύει και για μη-αβελιανές ομάδες είναι υπό μελέτη.

Κλείνοντας αυτήν την ενότητα, οφείλουμε να επισημάνουμε και κάτι ακόμα που δικαιολογεί τη θεμελιώδη θέση που κατέχει ο κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική. Γνωρίζουμε ότι εκμεταλλεύεται την ισχύ του κβαντικού παραλληλισμού, ώστε να πετύχει μία εκθετική αύξηση της ταχύτητας του περίφημου κλασικού γρήγορου μετασχηματισμού Fourier. Από τη στιγμή που ο κλασικός γρήγορος μετασχηματισμός Fourier έχει ποικίλες εφαρμογές, έχουμε λόγο να πιστεύουμε ότι κάποια στιγμή θα γίνεται ακόμα ευρύτερη χρήση και του κβαντικού μετασχηματισμού Fourier, παρά το ότι προς το παρόν συναντώνται δυσκολίες κατά την εφαρμογή του.

7.2. Παραγοντοποίηση του κβαντικού μετασχηματισμού Fourier

Η δράση του κβαντικού μετασχηματισμού Fourier στα διανύσματα βάσης ενός συστήματος με N qubits περιγράφεται από τη σχέση:

$$F |k\rangle = \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} \omega^{k \cdot j} |j\rangle \quad (28)$$

όπου

$$\omega = e^{2\pi i/2^N} \quad (29)$$

Σημειώνουμε εδώ ότι ο κβαντικός μετασχηματισμός Fourier επεκτείνεται γραμμικά σε αυθαίρετες υπερθέσεις των καταστάσεων της βάσης. Σε μορφή πίνακα έχει ως εξής:

$$F = \frac{1}{\sqrt{2^N}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{2^N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(2^N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^N-1} & \omega^{2(2^N-1)} & \dots & \omega^{(2^N-1)(2^N-1)} \end{bmatrix}$$

Για παράδειγμα, εάν έχουμε ένα σύστημα με 2 qubits, ο χώρος Hilbert είναι διάστασης 4, το $\omega = e^{2\pi i/2^2} = i$ και ο πίνακας του μετασχηματισμού Fourier θα είναι:

$$F = \frac{1}{\sqrt{2^2}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

ενώ για ένα σύστημα με 3 qubits ο χώρος Hilbert είναι διάστασης 8, το $\omega = e^{2\pi i/2^3} = \sqrt[3]{i}$ και ο πίνακας του μετασχηματισμού Fourier προκύπτει να είναι:

$$F = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & \omega^8 & \omega^4 & \omega^8 & \omega^4 & \omega^8 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & \omega^8 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}$$

Αντικαθιστώντας τις δυνάμεις του ω λαμβάνουμε:

$$F = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \sqrt{i} & i & i\sqrt{i} & -1 & -\sqrt{i} & -i & -i\sqrt{i} \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & i\sqrt{i} & -i & 1 & -1 & -i\sqrt{i} & i & -\sqrt{i} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\sqrt{i} & i & -i\sqrt{i} & -1 & 1 & -i & i\sqrt{i} \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -i\sqrt{i} & -i & -\sqrt{i} & -1 & i\sqrt{i} & i & \sqrt{i} \end{bmatrix}$$

Στη συνέχεια, θα δείξουμε πώς ο μετασχηματισμός Fourier μπορεί να γραφεί διαφορετικά, ώστε να δρά εναλλακτικά στα qubits $|0\rangle$ και $|1\rangle$ και όχι στα διανύσματα της βάσης του χώρου Hilbert διάστασης 2^N , όπως φαίνεται στη μορφή (28). Η μετατροπή αυτή είναι ουσιώδης ώστε να καταφέρουμε να σχεδιάσουμε το κβαντικό κύκλωμα. Ισοδυναμεί με την ανάλυση του χώρου Hilbert της μηχανής που θα το υλοποιήσει, σε ένα ταχυστικό γινόμενο χώρων λίγων διαστάσεων, εν προκειμένω των διδιάστατων χώρων των qubits. Θεωρούμε ότι πάντα υπάρχει μία τέτοια ανάλυση σε υποσυστήματα, στην οποία ανταποκρίνονται οι κβαντικές πύλες, καθώς κάθε φορά δρουν μόνο σε έναν μικρό αριθμό υποσυστημάτων. Από

μαθηματικής άποψης, αυτό το χαρακτηριστικό των πυλών είναι κρίσιμο, ώστε να καταφέρουμε να διατυπώσουμε ένα σαφή ορισμό της έννοιας της κβαντικής πολυπλοκότητας. Όσον αφορά στη Φυσική, ο βασικός λόγος για μια φυσιολογική ανάλυση σε υποσυστήματα είναι η locality (‘τοπικότητα’), δηλαδή το ότι εφικτές κβαντικές πύλες είναι αυτές που δρουν σε μία φραγμένη περιοχή του χώρου, έτσι ώστε ο υπολογιστής να αποτελείται από υποσυστήματα που αλληλεπιδρούν μόνο με τα γειτονικά τους.

Αρχικά, γράφουμε τα διανύσματα βάσης ενός συστήματος N qubits στη δυαδική τους μορφή, κάνοντας χρήση των qubits $|0\rangle$ και $|1\rangle$. Θα έχουμε:

$$|k\rangle = |k_0\rangle \otimes |k_1\rangle \otimes \dots \otimes |k_{N-1}\rangle = |k_0 k_1 \dots k_{N-1}\rangle$$

και

$$|j\rangle = |j_0\rangle \otimes |j_1\rangle \otimes \dots \otimes |j_{N-1}\rangle = |j_0 j_1 \dots j_{N-1}\rangle$$

όπου $k_m = 0$ ή 1 και $j_l = 0$ ή 1 ,
ενώ $k = 0, 1, \dots, 2^N - 1$ και $j = 0, 1, \dots, 2^N - 1$.

Συνοπτικά:

$$k = \sum_{m=0}^{N-1} k_m \cdot 2^{N-m-1} \quad (30)$$

και

$$j = \sum_{l=0}^{N-1} j_l \cdot 2^{N-l-1} \quad (31)$$

Αντικαθιστώντας από την (31), ο παράγοντας φάσης $\omega^{k \cdot j}$ γίνεται:

$$\omega^{k \cdot j} = \omega^{k \cdot \sum_{l=0}^{N-1} j_l \cdot 2^{N-l-1}} = \prod_{l=0}^{N-1} \omega^{k \cdot 2^{N-l-1}} \cdot j_l \quad (32)$$

Η (28) με τη βοήθεια της (32):

$$\begin{aligned}
F|k\rangle &= \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} \prod_{l=0}^{N-1} \omega^{k \cdot j_l \cdot 2^{N-l-1}} |j\rangle \\
&= \frac{1}{\sqrt{2^N}} \sum_{j_0=0}^1 \sum_{j_1=0}^1 \cdots \sum_{j_{N-1}=0}^1 \prod_{l=0}^{N-1} \omega^{k \cdot j_l \cdot 2^{N-l-1}} |j_0 j_1 \cdots j_{N-1}\rangle \\
&= \frac{1}{\sqrt{2^N}} \bigotimes_{l=0}^{N-1} \sum_{j_l=0}^1 \omega^{k \cdot j_l \cdot 2^{N-l-1}} |j_l\rangle \\
&= \frac{1}{\sqrt{2^N}} \bigotimes_{l=0}^{N-1} \left(|0\rangle + \omega^{k \cdot 2^{N-l-1}} |1\rangle \right) \tag{33}
\end{aligned}$$

Στην (33) ο παράγοντας φάσης $\omega^{k \cdot 2^{N-l-1}}$, αντικαθιστώντας από την (30) γίνεται:

$$e^{\frac{2\pi i}{2^N} (\sum_{m=0}^{N-1} k_m \cdot 2^{N-m-1}) 2^N \cdot 2^{-l-1}} = e^{2\pi i (\sum_{m=0}^{N-1} k_m \cdot 2^{N-m-l-2})} \tag{34}$$

Αναπτύσσοντας το άθροισμα:

$$\begin{aligned}
\sum_{m=0}^{N-1} k_m \cdot 2^{N-l-m-2} &= k_0 \cdot 2^{N-l-2} + k_1 \cdot 2^{N-l-3} + \\
&\dots + k_{N-l-2} \cdot 2^0 + k_{N-l-3} \cdot 2^{-1} + \dots + k_{N-1} \cdot 2^{-N}
\end{aligned}$$

παρατηρούμε ότι για $N-m-l-2 > 0$ έχουμε ακέραιους όρους στον εκθέτη, οπότε αυτοί που συνεισφέρουν στο άθροισμα και θα παραμείνουν θα είναι οι όροι για $m \geq N-l-1$ (δυαδικοί κλασματικοί όροι), δηλαδή:

$$e^{2\pi i \sum_{m=0}^{N-1} k_m \cdot 2^{N-l-m-2}} = e^{2\pi i \sum_{m=N-l-1}^{N-1} k_m \cdot 2^{N-l-m-2}}$$

Κάνοντας χρήση του τελευταίου αποτελέσματος στην (33) έχουμε:

$$\begin{aligned}
F|k\rangle &= \frac{1}{\sqrt{2^N}} \left(|0\rangle + e^{2\pi i k_{N-1} \cdot 2^{-1}} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i (k_{N-2} \cdot 2^{-1} + k_{N-1} \cdot 2^{-2})} |1\rangle \right) \\
&\quad \otimes \dots \otimes \left(|0\rangle + e^{2\pi i (k_0 \cdot 2^{-1} + k_1 \cdot 2^{-2} + \dots + k_{N-1} \cdot 2^{-N})} |1\rangle \right)
\end{aligned}$$

Για λόγους συντομίας και απλοποίησης της γραφής, γράφουμε τα αθροίσματα που εμφανίζονται στους εκθέτες στη μορφή δυαδικών κλασμάτων, οπότε:

$$F|k\rangle = \frac{1}{\sqrt{2^N}} (|0\rangle + e^{2\pi i 0.k_{N-1}} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.k_{N-2}k_{N-1}} |1\rangle) \\ \otimes \dots \otimes (|0\rangle + e^{2\pi i 0.k_0k_1k_2\dots k_{N-1}} |1\rangle)$$

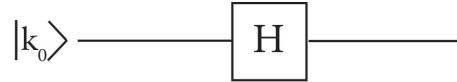
Τέλος, έχοντας υπόψιν ότι $\sqrt{2^N} = N\sqrt{2}$ και ότι το παραπάνω τανυστικό γινόμενο έχει N παράγοντες, λαμβάνουμε το ζητούμενο, δηλαδή την τελική μορφή της δράσης του μετασχηματισμού Fourier στα qubits $|0\rangle$ και $|1\rangle$:

$$F|k\rangle = \bigotimes_{l=0}^{N-1} \frac{|0\rangle + e^{2\pi i 0.k_{N-l-1}\dots k_{N-1}} |1\rangle}{\sqrt{2}} \quad (35)$$

7.3. Κβαντικά Κυκλώματα που υλοποιούν τον κβαντικό μετασχηματισμό Fourier

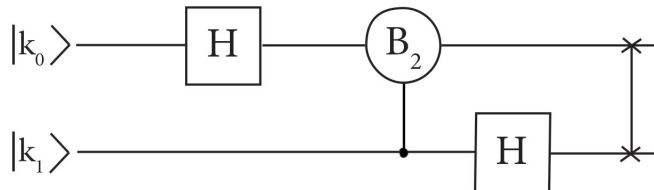
Παρακάτω έχουν σχεδιαστεί τα κβαντικά κυκλώματα που υλοποιούν τον κβαντικό μετασχηματισμό Fourier στην περίπτωση ενός, δύο, τριών, τεσσάρων και N qubits. Κάτω από το καθένα, προς επαλήθευση, φαίνεται αναλυτικά πως προκύπτει η έξοδός τους, η οποία είναι σε συμφωνία με τη δράση του μετασχηματισμού, όπως αυτή φαίνεται στην (35).

• 1 qubit



$$\text{Input: } |k_0\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_0} |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_0} |1\rangle}{\sqrt{2}} : \text{Output}$$

• 2 qubits



Για το πρώτο qubit:

$$\text{Input: } |k_0\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C - B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1}|1\rangle}{\sqrt{2}} : \text{Output}$$

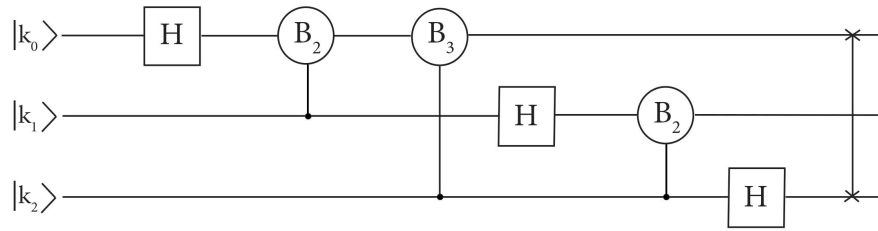
Για το δεύτερο qubit:

$$\text{Input: } |k_1\rangle \xrightarrow{C - B_2} |k_1\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0 \cdot k_1}|1\rangle}{\sqrt{2}} : \text{Output}$$

Συνολικά:

$$\text{Input: } |k_0\rangle \otimes |k_1\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1}|1\rangle}{\sqrt{2}} \xrightarrow{\text{SWAP}} \frac{|0\rangle + e^{2i\pi 0 \cdot k_1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1}|1\rangle}{\sqrt{2}} : \text{Output}$$

• 3 qubits



Για το πρώτο qubit:

$$\text{Input: } |k_0\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C - B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C - B_3} \frac{|0\rangle + e^{i\frac{\pi}{4}k_2}e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1 k_2}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το δεύτερο qubit:

$$\text{Input: } |k_1\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_1}|1\rangle}{\sqrt{2}} \xrightarrow{C - B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_2}e^{i\pi k_1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0 \cdot k_1 k_2}|1\rangle}{\sqrt{2}} : \text{Output}$$

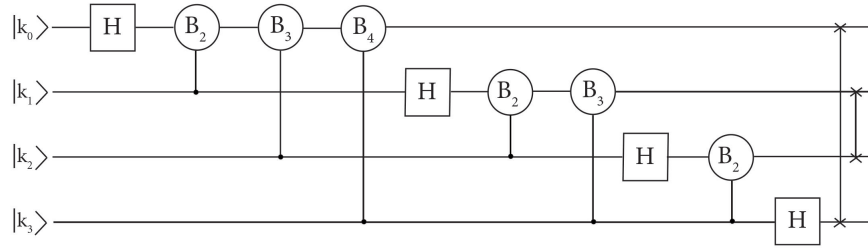
Για το τρίτο qubit:

$$\text{Input: } |k_2\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_2}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0 \cdot k_2}|1\rangle}{\sqrt{2}} : \text{Output}$$

Συνολικά:

$$\text{Input: } |k_0\rangle \otimes |k_1\rangle \otimes |k_2\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1 k_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1 k_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_2}|1\rangle}{\sqrt{2}} \xrightarrow{\text{SWAP}} \frac{|0\rangle + e^{2i\pi 0 \cdot k_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1 k_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0 k_1 k_2}|1\rangle}{\sqrt{2}} : \text{Output}$$

• 4 qubits



Για το πρώτο qubit:

$$\text{Input: } |k_0\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_3} \frac{|0\rangle + e^{i\frac{\pi}{4}k_2}e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_4} \frac{|0\rangle + e^{i\frac{\pi}{8}k_3}e^{i\frac{\pi}{4}k_2}e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_0k_1k_2k_3}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το δεύτερο qubit:

$$\text{Input: } |k_1\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_1}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_2}e^{i\pi k_1}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_3} \frac{|0\rangle + e^{i\frac{\pi}{4}k_3}e^{i\frac{\pi}{2}k_2}e^{i\pi k_1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_1k_2k_3}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το τρίτο qubit:

$$\text{Input: } |k_2\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_2}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_3}e^{i\pi k_2}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_2k_3}|1\rangle}{\sqrt{2}} : \text{Output}$$

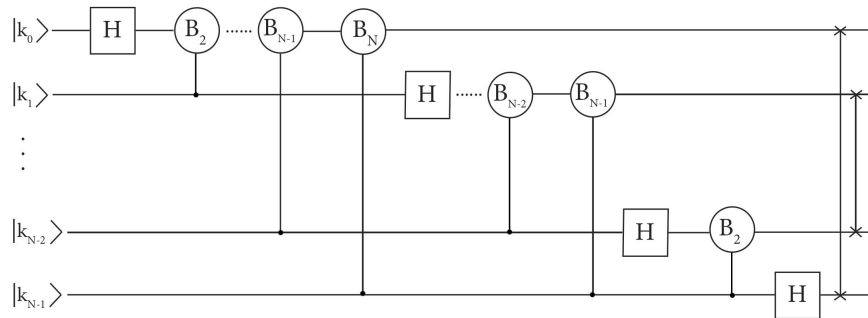
Για το τέταρτο qubit:

$$\text{Input: } |k_3\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_3}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_3}|1\rangle}{\sqrt{2}} : \text{Output}$$

Συνολικά:

$$\begin{aligned} \text{Input: } |k_0\rangle \otimes |k_1\rangle \otimes |k_2\rangle \otimes |k_3\rangle &\rightarrow \frac{|0\rangle + e^{2i\pi 0.k_0k_1k_2k_3}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_1k_2k_3}|1\rangle}{\sqrt{2}} \otimes \\ &\frac{|0\rangle + e^{2i\pi 0.k_2k_3}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_3}|1\rangle}{\sqrt{2}} \xrightarrow{\text{SWAP}} \frac{|0\rangle + e^{2i\pi 0.k_3}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_2k_3}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_1k_2k_3}|1\rangle}{\sqrt{2}} \otimes \\ &\frac{|0\rangle + e^{2i\pi 0.k_0k_1k_2k_3}|1\rangle}{\sqrt{2}} : \text{Output} \end{aligned}$$

• N qubits



Για το πρώτο qubit:

$$\text{Input: } |k_0\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_3} \dots \xrightarrow{C-B_N} \frac{|0\rangle + e^{i\frac{\pi}{2^{N-1}}k_{N-1}} \dots e^{i\frac{\pi}{2}k_1}e^{i\pi k_0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_0k_1\dots k_{N-1}}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το δεύτερο qubit:

$$\text{Input: } |k_1\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_1}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_2}e^{i\pi k_1}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_3} \dots \xrightarrow{C-B_{N-1}} \frac{|0\rangle + e^{i\frac{\pi}{2^{N-2}}k_{N-1}} \dots e^{i\frac{\pi}{2}k_2}e^{i\pi k_1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_1k_2\dots k_{N-1}}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το (N-1)-οστό qubit:

$$\text{Input: } |k_{N-2}\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_{N-2}}|1\rangle}{\sqrt{2}} \xrightarrow{C-B_2} \frac{|0\rangle + e^{i\frac{\pi}{2}k_{N-1}}e^{i\pi k_{N-2}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_{N-2}k_{N-1}}|1\rangle}{\sqrt{2}} : \text{Output}$$

Για το N-οστό qubit:

$$\text{Input: } |k_{N-1}\rangle \xrightarrow{H} \frac{|0\rangle + e^{i\pi k_{N-1}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2i\pi 0.k_{N-1}}|1\rangle}{\sqrt{2}} : \text{Output}$$

Συνολικά:

$$\begin{aligned} \text{Input: } & |k_0\rangle \otimes |k_1\rangle \dots \otimes |k_{N-2}\rangle \otimes |k_{N-1}\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0.k_0k_1\dots k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_1k_2\dots k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \\ & \dots \otimes \frac{|0\rangle + e^{2i\pi 0.k_{N-2}k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_{N-1}}|1\rangle}{\sqrt{2}} \xrightarrow{\text{SWAP}} \frac{|0\rangle + e^{2i\pi 0.k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_{N-2}k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \\ & \dots \otimes \frac{|0\rangle + e^{2i\pi 0.k_1k_2\dots k_{N-1}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0.k_0k_1\dots k_{N-1}}|1\rangle}{\sqrt{2}} : \text{Output} \end{aligned}$$

Όσον αφορά τη δράση της πύλης SWAP στη γενική περίπτωση των N qubits, περιγράφεται ως εξής:

- Αν το N είναι άρτιος, τότε εναλλάσσει το qubit $|k_0\rangle$ με το $|k_{N-1}\rangle$, το $|k_1\rangle$ με το $|k_{N-2}\rangle$, ... και το $\left|k_{\frac{N}{2}}\right\rangle$ με το $\left|k_{\frac{N}{2}+1}\right\rangle$
- Αν το N είναι περιττός, εναλλάσσει το qubit $|k_0\rangle$ με το $|k_{N-1}\rangle$, το $|k_1\rangle$ με το $|k_{N-2}\rangle$, ..., το $\left|k_{\frac{N}{2}}\right\rangle$ με το $\left|k_{\frac{N}{2}+2}\right\rangle$, ενώ το $\left|k_{\frac{N}{2}+1}\right\rangle$, παραμένει ως έχει.

• Πολυπλοκότητα του κβαντικού αλγορίθμου

Κλείνοντας αυτήν την ενότητα, ας ελέγξουμε τι συμβαίνει με την πολυπλοκότητα του αλγορίθμου που υπολογίζει τον κβαντικό μετασχηματισμό Fourier και υλοποιείται από τα παραπάνω κυκλώματα.

Στο πρώτο qubit εφαρμόζουμε μία πύλη Hadamard και $N - 1$ πύλες ελεγχόμενης μετατόπισης φάσης, δηλαδή N στο σύνολο πύλες. Περνώντας στο δεύτερο qubit, χρειαζόμαστε και πάλι μία πύλη Hadamard και $N - 2$, αυτή τη φορά, πύλες ελεγχόμενης μετατόπισης φάσης, δηλαδή $N - 1$ στο σύνολο πύλες. Συνεχίζοντας με τον ίδιο τρόπο, βλέπουμε ότι απαιτούνται $N + (N - 1) + (N - 2) + \dots + 1 = \frac{N(N+1)}{2}$ πύλες συν τις πύλες αντιστροφής των qubits, οι οποίες είναι το πολύ $\frac{N}{2}$ στο σύνολο. Λαμβάνοντας υπόψη και ότι κάθε πύλη SWAP αποτελείται από τρεις CONTROL-NOT πύλες, καταληγουμε στο ότι τελικά η πολυπλοκότητα του αλγορίθμου που εκτελεί τον κβαντικό μετασχηματισμό Fourier προκύπτει να είναι $O(N^2)$.

Σε αντίθεση με αυτό το αποτέλεσμα, ο καλύτερος κλασικός αλγόριθμος που υπολογίζει τον διακριτό μετασχηματισμό Fourier 2^N στοιχείων έχει πολυπλοκότητα $O(N \cdot 2^N)$.

Αυτό σημαίνει ότι ο κβαντικός αλγόριθμος έχει εκθετικά μικρότερη πολυπλοκότητα από τον αντίστοιχο κλασικό.

8. Ο Twisted κβαντικός μετασχηματισμός Fourier στην Κβαντική Πληροφορική

Από τη στιγμή που ο Twisted κβαντικός μετασχηματισμός Fourier αποτελεί γενίκευση του κβαντικού μετασχηματισμού Fourier, μπορούμε να γενικεύσουμε αντίστοιχα και την εφαρμογή του τελευταίου σε επίπεδο Κβαντικής Πληροφορικής, κάνοντας χρήση της twisted εκδοχής του. Πιο συγκεκριμένα, φαίνεται άμεσα ότι ο Twisted κβαντικός μετασχηματισμός Fourier θα μπορούσε να χρησιμοποιηθεί σε εφαρμογές που περιλαμβάνουν δύο ανεξάρτητα μεταξύ τους κβαντικά συστήματα με N qubits το κάθε ένα. Τέτοιου είδους εφαρμογές συναντώνται, για παράδειγμα, στην περιοχή της Τοπολογικής Κβαντικής Πληροφορικής (Topological Quantum Computing) [1, Κεφ.9].

8.1. Παραγοντοποίηση του Twisted κβαντικού μετασχηματισμού Fourier

Έστω ότι έχουμε δύο ανεξάρτητα κβαντικά συστήματα 1 και 2, κάθε ένα από τα οποία αποτελείται από N qubits. Η δράση του Twisted κβαντικού μετασχηματισμού Fourier στα διανύσματα βάσης $|k^1 k^2\rangle$ του χώρου Hilbert διάστασης 2^{2N} που περιλαμβάνει και τα δύο συστήματα δίνεται από τη σχέση:

$$TF |k^1 k^2\rangle = \frac{1}{\sqrt{2^{2N}}} \sum_{j^1=0}^{2^N-1} \sum_{j^2=0}^{2^N-1} \omega^{j^1 k^2 + j^2 k^1} |j^1 j^2\rangle, \quad (36)$$

όπου $|k^1\rangle$ και $|k^2\rangle$ είναι τα διανύσματα βάσης των επιμέρους χώρων Hilbert διάστασης 2^N που αντιστοιχούν στα συστήματα 1 και 2.

Στο Κεφάλαιο 4 έχουμε υπολογίσει τους πίνακες που τον αναπαριστούν σε χώρο Hilbert διάστασης $2^N \times 2^N = 2^{2N}$ για $N = 1$ και $N = 2$, δηλαδή στην περίπτωση που έχουμε δύο ανεξάρτητα συστήματα με $N = 1$ και $N = 2$ qubits το κάθε ένα, αντίστοιχα. Εφαρμόζοντας τις ιδιότητες του τανυστικού γινομένου για τα ανεξάρτητα συστήματα 1 και 2, μπορούμε να γράψουμε ισοδύναμα την (36) ως εξής:

$$TF |k^1 k^2\rangle = \frac{1}{2^N} \sum_{j^1=0}^{2^N-1} \omega^{j^1 k^2} |j^1\rangle \otimes \sum_{j^2=0}^{2^N-1} \omega^{j^2 k^1} |j^2\rangle$$

Από την τελευταία σχέση μπορούμε άμεσα να λάβουμε την παραγοντοποιημένη μορφή του TF , η οποία μας δίνει τη δράση του στα $|0\rangle$ και $|1\rangle$, με εφαρμογή της

(35) στα δύο επιμέρους συστήματα. Προκύπτει:

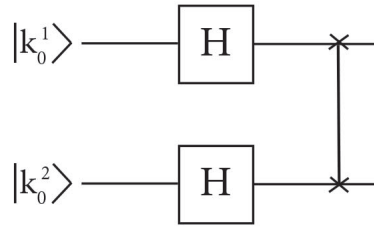
$$\text{TF} |k^1 k^2\rangle = \bigotimes_{l_1=0}^{N-1} \frac{|0\rangle + e^{2\pi i 0 \cdot k_{N-l_1-1}^2 \dots k_{N-1}^2} |1\rangle}{\sqrt{2}} \otimes \bigotimes_{l_2=0}^{N-1} \frac{|0\rangle + e^{2\pi i 0 \cdot k_{N-l_2-1}^1 \dots k_{N-1}^1} |1\rangle}{\sqrt{2}} \quad (37)$$

Βάσει αυτής μπορούμε πλέον να προχωρήσουμε στο σχεδιασμό των κβαντικών κυκλωμάτων που υλοποιούν τον Twisted κβαντικό μετασχηματισμό Fourier.

8.2. Κβαντικά Κυκλώματα που υλοποιούν τον Twisted κβαντικό μετασχηματισμό Fourier

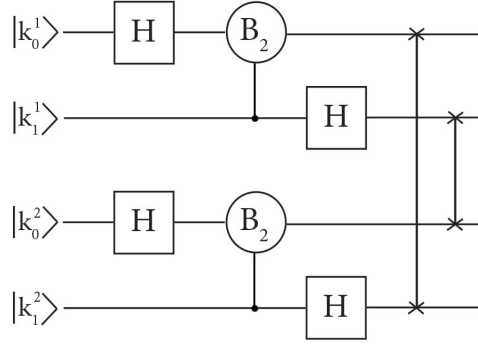
Στην ενότητα αυτή παρουσιάζουμε τα κβαντικά κυκλώματα που υλοποιούν τον Twisted κβαντικό μετασχηματισμό Fourier στην περίπτωση που τα δύο συστήματα απαρτίζονται από 1,2,3 και N qubits το κάθε ένα, αντίστοιχα. Ακριβώς κάτω από τα κυκλώματα φαίνεται η είσοδος και η έξοδος τους, προς επαλήθευση του ότι είναι σε συμφωνία με τη δράση του μετασχηματισμού, όπως φαίνεται στην (37). Όπως θα δούμε, τα κυκλώματα αυτά αποτελούνται από δύο επιμέρους κυκλώματα, ένα για το κάθε σύστημα, τα οποία είναι πανομοιότυπα με τα αντίστοιχα του κβαντικού μετασχηματισμού Fourier. Η μοναδική διαφορά είναι στην εφαρμογή της πύλης SWAP, η οποία πλέον εναλλάσσει τις θέσεις των qubits μεταξύ των επιμέρους κυκλωμάτων, όπως άλλωστε αναμένουμε, δεδομένης της δράσης του.

• 2 συστήματα του ενός qubit



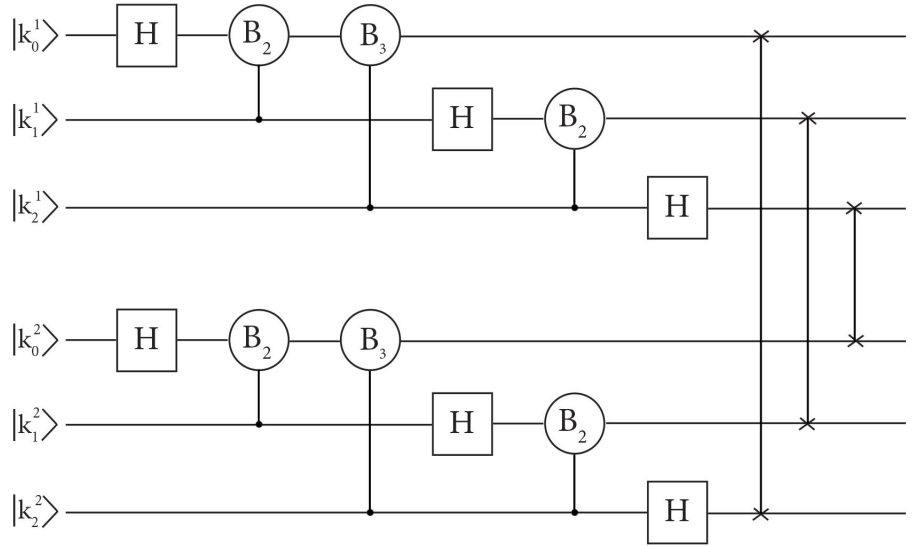
$$\text{Input: } |k_0^1\rangle \otimes |k_0^2\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^1} |1\rangle}{\sqrt{2}} : \text{Output}$$

• 2 συστήματα των δύο qubits



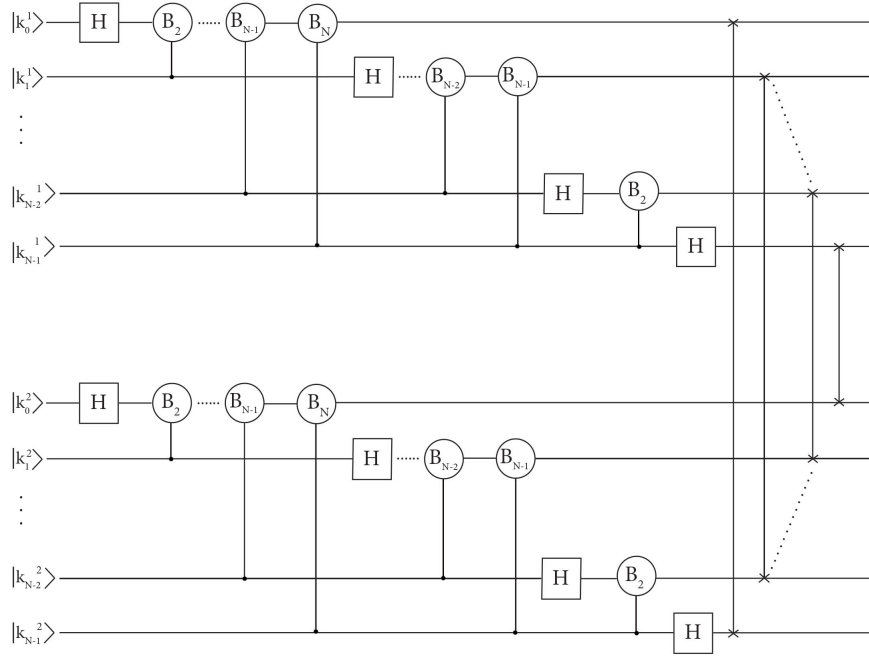
Input: $|k_0^1 k_1^1\rangle \otimes |k_0^2 k_1^2\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^2 k_1^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^1} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^1 k_1^1} |1\rangle}{\sqrt{2}}$:Output

• 2 συστήματα των τριών qubits



Input: $|k_0^1 k_1^1 k_2^1\rangle \otimes |k_0^2 k_1^2 k_2^2\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_2^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^2 k_2^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^2 k_1^2 k_2^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_2^1} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^1 k_2^1} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^1 k_1^1 k_2^1} |1\rangle}{\sqrt{2}}$:Output

• 2 συστήματα των N qubits



$$\begin{aligned} \text{Input: } & |k_0^1 k_1^1 \dots k_{N-2}^1 k_{N-1}^1\rangle \otimes |k_0^2 k_1^2 \dots k_{N-2}^2 k_{N-1}^2\rangle \rightarrow \frac{|0\rangle + e^{2i\pi 0 \cdot k_{N-1}^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_{N-2}^2 k_{N-1}^2} |1\rangle}{\sqrt{2}} \otimes \\ & \dots \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^2 k_2^2 \dots k_{N-2}^2 k_{N-1}^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^2 k_1^2 \dots k_{N-2}^2 k_{N-1}^2} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_{N-1}^1} |1\rangle}{\sqrt{2}} \otimes \\ & \frac{|0\rangle + e^{2i\pi 0 \cdot k_{N-2}^1 k_{N-1}^1} |1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_1^1 k_2^1 \dots k_{N-2}^1 k_{N-1}^1} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2i\pi 0 \cdot k_0^1 k_1^1 \dots k_{N-2}^1 k_{N-1}^1} |1\rangle}{\sqrt{2}} : \text{Output} \end{aligned}$$

Όσον αφορά τη δράση της πύλης SWAP στη γενική περίπτωση των N qubits, εναλλάσσει το qubit $|k_0^1\rangle$ με το $|k_{N-1}^2\rangle$, το $|k_1^1\rangle$ με το $|k_{N-2}^2\rangle$, ..., το $|k_{N-2}^1\rangle$ με το $|k_1^2\rangle$ και το $|k_{N-1}^1\rangle$ με το $|k_0^2\rangle$.

Αναφορές

- [1] John Preskill, *Lecture Notes for Physics 219/Computer Science 219: Quantum Computation*. California Institute of Technology, Updated Version, 2004.
- [2] Phillip Kaye, Raymond Laflamme, Michele Mosca, *An Introduction to Quantum Computing*. Oxford University Press, 2007.
- [3] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [4] Amnon Yariv, *An Introduction to Theory and Applications of Quantum Mechanics*. John Wiley and Sons, 1982.
- [5] M.L. Mehta, *Eigenvalues and Eigenvectors of the finite Fourier Transform*. J. Math. Phys. **28**, 781 (1987).
- [6] I. Schur, Nachr. K. Gesell, Wiss. Goettingen, Math.-Phys. Kl. **1921**, 147
- [7] Bradley W. Dickinson, Kenneth Steiglitz, *Eigenvectors and Functions of the Discrete Fourier Transform*. IEEE Transactions on Acoustics, Speech and Signal Processing, Vol. 30, No. 1 (1982).
- [8] G.G. Athanasiu, E.G. Floratos and S. Nicolis, *Holomorphic Quantization on the Torus and Finite Quantum Mechanics*. arXiv:hep-th/9509098v2, 10 Nov 1996.
- [9] Wolfgang Eholzer, *On the Classification of Modular Fusion Algebras*. Commun. Math. Phys. **172**, 623-659 (1995).
- [10] Peter Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).
- [11] Lov K. Grover, *Searching with Quantum Computers*. arXiv:quant-ph/0011118, 30 Nov 2000.
- [12] Lov K. Grover, *From Schroedinger's Equation to the Quantum Search Algorithm*. arXiv:quant-ph/0109116, 22 Sep 2001.

- [13] Haim Brezis, *Συναρτησιακή Ανάλυση, Θεωρία και Εφαρμογές*. Μετάφραση-Επιμέλεια: Δ. Κραββαρίτης, Ι. Χρυσοβέργης. Πανεπιστημιακές Εκδόσεις Ε.Μ.Π., 1997.
- [14] Σωτήριος Καρανάσιος, *Θεωρία Τελεστών και Εφαρμογές*. Έκδοση Πρώτη, Αθήνα 2009.
- [15] Εμμανουήλ Φλωράτος, *Σημειώσεις από τις παραδόσεις του μεταπτυχιακού μαθήματος "Εισαγωγή στους Κβαντικούς Υπολογιστές"*. Τμήμα Φυσικής, ΕΚΠΑ, χειμερινό εξάμηνο 2009-2010.
- [16] www.wikipedia.org