Εθνικο και Καποδιστριακο Πανεπιστημιο Αθηνων

Σχολη Θετικων Επιστημων

Μεταπτυχιακο Προγραμμα στην Λογικη και Θεωρια Αλγοριθμων και Υπολογισμου

Διπλωματικη Εργασια

Κβαντικός Κλασματικός Μετασχηματισμός Fourier σε Χώρους Φάσης $\mathbb{Z}_p \times \mathbb{Z}_p$

Βασίλειος William Καραγεώργος

Επιβλέποντες: Εμμανουήλ Φλωράτος, Καθηγητής ΕΚΠΑ
Ευάγγελος Ράπτης, Αναπληρωτής Καθηγητής ΕΚΠΑ

Αθηνα

Σεπτεμβριος 2009

Διπλωματικη Εργασια

Κβαντικός Κλασματικός Μετασχηματισμός Fourier σε Χώρους Φάσης $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$

Βασίλειος W. Καραγεώργος

Α.Μ.: 200609

Επιβλεποντες:

Εμμανουήλ Φλωράτος, Καθηγητής ΕΚΠΑ
Ευάγγελος Ράπτης, Αναπληρωτής Καθηγητής ΕΚΠΑ

Τετραμελης Επιτροπη:

Εμμανουήλ Φλωράτος, Καθηγητής ΕΚΠΑ
Κωνσταντίνος Δημητρακόπουλος, Καθηγητής ΕΚΠΑ
Ευάγγελος Ράπτης, Αναπληρωτής Καθηγητής ΕΚΠΑ
Δημήτριος Θηλυκός, Επίκουρος Καθηγητής ΕΚΠΑ

Αθηνα

Ιουνιος 2009

Περίληψη

Η διπλωματική αυτή εργασία εξετάζει το Διακριτό Κλασματικό Μετασχηματισμό Fourier (DFrFT) από τη σκοπιά της Κβαντικής Υπολογιστικής. Μελετώνται αρχικά οι διάφοροι εναλλακτικοί ορισμοί του μετασχηματισμού που υπάρχουν στην βιβλιογραφία και επισημαίνονται τα προβλήματά τους. Προτείνεται, κατόπιν, ένας νέος ορισμός βασισμένος στην κβάντωση Weyl ενός κατάλληλου φυσικού συστήματος, σε αναλογία με την περίπτωση του Διακριτού Μετασχηματισμού Fourier (DFT) και του αρμονικού ταλαντωτή. Προς το σκοπό αυτό, μελετάται η συμπεριφορά του κβαντικού ταλαντωτή Balian-Itzykson σε διακριτούς χώρους φάσης με τη δομή σωμάτων Galois $GF[p]$. Από τη μελέτη αυτή προκύπτουν κλειστοί τύποι για τον υπολογισμό κλασματικών δυνάμεων του μετασχηματισμού Fourier, υπό τη μορφή αναπαράστασης στοιχείων ομάδας. Εν κατακλείδι, γίνεται μια προσπάθεια να περιγραφεί ένα κβαντικό κύκλωμα όμοιο αυτού που χρησιμοποιείται για τον μετασχηματισμό Fourier στον αλγόριθμο του Shor, για τον αποδοτικό υπολογισμό των στοιχείων αυτών.

Θεματική Περιοχή: Κβαντική Υπολογιστική
Λέξεις Κλειδιά: μετασχηματισμός Fourier, διακριτοί χώροι φάσης, κβάντωση Weyl, κβαντικό κύκλωμα, ομάδες Lie

Abstract

In this thesis we examine the Discrete Fractional Fourier Transform (DFrFT) in the light of Quantum Computing. Initially, we study the alternative definitions of the transform that have been proposed in the existing bibliography and point out their deficits. Further on, we propose a new definition, based on the Weyl quantization of an appropriate physical system, in the same way the Discrete Fourier Transform (DFT) can be defined by means of the harmonic oscillator. To this end, we study the behaviour of the Balian-Itzykson quantum harmonic oscillator in discrete phase spaces with the structure of the Galois field $GF[p]$. From this study, we derive closed forms for fractional powers of the Fourier transform, in the form of group element representations. Finally, we attempt to describe a quantum circuit similar to the one used in the well known Shor algorithm which performs the Fourier transform, in order to efficiently compute said findings.

Subject Area: Quantum Computing
Keywords: Fourier transform, discrete phase spaces, Weyl quantization, quantum circuit, Lie groups

Στο Νίκο
που έφυγε νωρίς

Περιεχόμενα

1 Εισαγωγή **1**
1.1 Ο κλασματικός μετασχηματισμός Fourier 1
1.2 Μέθοδοι υπολογισμού 3
1.2.1 Υπολογισμός του FrFT 3
1.2.2 Υπολογισμός του DFrFT 5

2 Ο διακριτός FrFT **10**
2.1 Χώροι φάσης Galois 10
2.1.1 Κίνηση σε διακριτό κύκλο 10
2.1.2 Πρώτοι αριθμοί, συμπλεκτικές ομάδες και σώματα Galois . 12
2.2 Ο κβαντικός ταλαντωτής Balian-Itzykson (BI) 14
2.2.1 Η ομάδα Heisenberg-Weyl 14
2.2.2 Ο DFrFT στην μεταπλεκτική αναπαράσταση 18

3 Ο κβαντικός FrFT **23**
3.1 Περί κβαντικών υπολογιστών 23
3.2 Στοιχεία κβαντικής υπολογιστικής 24
3.2.1 Πύλες ενός qubit 26
3.2.2 Πύλες πολλαπλών qubit 28
3.3 Ο αλγόριθμος QFT 30
3.4 Κβαντικός υπολογισμός του DFrFT 33

4 Επίλογος **35**

5 Παράρτημα **36**

Συμβολισμοί

Παρακάτω παρατίθεται μία όσον το δυνατόν πλήρης λίστα από συμβολισμούς που χρησιμοποιούνται στο κείμενο ως προς το αλφάβητο και την γραμματοσειρά. Όπου χρησιμοποιείται συμβολισμός που διαφέρει από την λίστα αυτή ή που δεν αναφέρεται, το νόημά του θα είναι ξεκάθαρο από το ίδιο το κείμενο.

συναρτησιακά σύμβολα:	$f, g, h, \ldots$
μεταβλητές:	$i, j, k, \ldots, q, p, \ldots, x, y, z$
σώματα:	$GF[p^n], F$
σύνολα:	$\mathbb{R}, \mathbb{Z}, \ldots, T, V, \ldots$
ομάδες:	$\mathcal{G}, \mathcal{H}, \ldots, L, SL, O, SO, Sp, Mp$
στοιχεία ομάδων:	g, h, R
διανυσματικοί χώροι:	$\mathcal{V}, \mathcal{U}, \ldots$
διανύσματα:	$\mathbf{v}, \mathbf{u}, \ldots$
διανύσματα Dirac:	$\|u\rangle, \|v\rangle, \|q\rangle, \ldots$
πλειάδες:	$(a, b, \ldots)$
παραγόμενοι χώροι:	$< \mathbf{u}, \mathbf{v}, \ldots >$
άλγεβρες:	$\mathfrak{g}, \mathfrak{h}, \ldots$
πίνακες:	$\mathbf{H}, \mathbf{T}, \ldots$
τελεστές:	$\mathbf{H}, \mathbf{R}, \ldots, \hat{p}, \hat{q}, \ldots$
στοιχεία πινάκων, σταθερές:	$a, b, c, \ldots$
μετασχηματισμός Fourier:	$\mathcal{F}$

1 Εισαγωγή

Στο κεφάλαιο αυτό, κάνουμε μια συνοπτική παρουσίαση της έννοιας του κλασματικού μετασχηματισμού Fourier, δίνοντας τον ορισμό του και κάποιες σημαντικές ιδιότητές του που θα μας χρειαστούν. Εν συνεχεία, εξετάζουμε τις γνωστές μεθόδους υπολογισμού του, εστιάζοντας στο πρόβλημα έλλειψης ενός ακριβούς αλγορίθμου λογαριθμικής πολυπλοκότητας, όπως αυτός που υπάρχει για τον συνήθη μετασχηματισμό Fourier.

Τέλος, μελετάμε ιδιαίτερα την περίπτωση του διακριτού μετασχηματισμού, για τον οποίον εξετάζουμε τους διάφορους ορισμούς που έχουν προταθεί, και σκιαγραφούμε την πορεία που θα ακολοθήσουμε για να δώσουμε ένα νέο ορισμό.

1.1 Ο κλασματικός μετασχηματισμός Fourier

Η ιδέα κλασματικών δυνάμεων του μετασχηματισμού Fourier εμφανίζεται στην ευρύτερη μαθηματική βιβλιογραφία ήδη από το 1929 [31]. Αργότερα, χρησιμοποιείται στην επεξεργασία σήματος [1] αλλά και στην κβαντομηχανική [21], όπου ο Namias προσπαθεί με την βοήθειά του να επιλύσει εξισώσεις Shrödinger. Τελικά, όμως, είναι οι εφαρμογές του στην οπτική που τον εδραιώνουν την δεκαετία του '90, δίνοντας μια εναλλακτική μαθηματική ερμηνεία για την περίθλαση Fresnel [32].

Ο λόγος για την επιτυχία του αυτή στην οπτική, παράλληλα με μια απλή φυσική ερμηνεία του, μπορεί να γίνει κατανοητός από το εξής παράδειγμα [6]. Έστω ένα σύστημα το οποίο αποτελείται από μια σημειακή πηγή στα αριστερά, η οποία φωτίζει ένα αντικείμενο, αφού η ακτινοβολία της περάσει πρώτα από ένα δίκτυο από φακούς. Τότε, είναι ευρέως γνωστό ότι σε κάποια συγκεκριμένα σημεία στα δεξιά, παρατηρούνται είδωλα τα οποία είναι μετασχηματισμοί Fourier του αρχικού ειδώλου του αντικειμένου. Σε άλλα σημεία μακρύτερα, παρατηρούνται είδωλα τα οποία είναι ανεστραμμένες εικόνες του αρχικού, παρακάτω άλλα που είναι ο αντίστροφος μετασχηματισμός Fourier του αρχικού ειδώλου κ.ο.κ.. Αυτά τα παραλλαγμένα είδωλα όλα παράγονται εφαρμόζοντας τον μετασχηματισμό Fourier στο αρχικό είδωλο, μετά την 2^η δύναμή του, την 3^η (που ταυτίζεται με τον αντίστροφο μετασχηματισμό) κ.ο.κ.. Από την άλλη, οι εικόνες που μπορεί να κανείς να παρατηρήσει στα ενδιάμεσα σημεία, είναι είδωλα που παράγονται εφαρμόζοντας κλασματικές δυνάμεις του μετασχηματισμού στο αρχικό είδωλο.

Μπορούμε λοιπόν να πούμε ότι ο κλασματικός μετασχηματισμός Fourier (FrFT) αποτελεί μια γενίκευση του συνήθους μετασχηματισμού Fourier. Ως γνωστόν, για μια συνάρτηση $f(t)$, αν ο μετασχηματισμός Fourier συμβολίζεται με $\mathcal{F}(f)$, τότε με $\mathcal{F}^2(f) = \mathcal{F}(\mathcal{F}(f))$ εννοούμε τον μετασχηματισμό του μετασχηματισμού Fourier της f, δηλαδή την δεύτερη δύναμη του μετασχηματισμού και εν γένει με $\mathcal{F}^n(f)$ τη n-οστή δύναμη του μετασχηματισμού. Αντίστοιχα, με $\mathcal{F}^{-n}(f)$ εννοούμε τη n-οστή δύναμη του αντίστροφου μετασχηματισμού. Ο FrFT γενικεύει τον παραπάνω ορισμό σε περιπτώσεις μη-ακεραίων δυνάμεων $n = 2a/\pi, \forall a \in \mathbb{R}$. Αποτελεί συνεπώς έναν γραμμικό μετασχηματισμό που μπορεί να μετασχηματίσει μια συνάρτηση σε ένα ενδιάμεσο πεδίο ορισμού μεταξύ χρόνου και συχνότητας.

Πιο συγκεκριμένα, έχουμε τον εξής ορισμό

Ορισμός 1.1. Για κάθε $a \in \mathbb{R}$, ορίζεται ο κλασματικός μετασχηματισμός Fourier

$$\mathcal{F}_a(f)(\omega) = \int_{-\infty}^{\infty} K_a(\omega,t)f(t)dt \quad (1.1)$$

$$= \sqrt{\frac{1-i\cot(a)}{2\pi}}\, e^{i\cot(a)\omega^2/2}\int_{-\infty}^{\infty} e^{i\csc(a)\omega t + i\cot(a)t^2/2}f(t)dt \quad (1.2)$$

όπου

$$K_a(\omega,t) = C_a\exp[-i\pi(2\frac{\omega t}{\sin a} - (t^2+\omega^2)\cot a)] \quad (1.3)$$

είναι ο πυρήνας του μετασχηματισμού και $C_a = \sqrt{1-i\cot a}$. Ειδικότερα, αν $2a/\pi = n \in \mathbb{Z}$, τότε $\mathcal{F}_a(f) = \mathcal{F}^{2a/\pi}(f)$

Έπεται άμεσα το εξής πόρισμα

Πόρισμα 1.1. *Για* $a, b \in \mathbb{R}$

i) $\mathcal{F}_{a+b}(f) = \mathcal{F}_a(\mathcal{F}_b(f)) = \mathcal{F}_b(\mathcal{F}_a(f))$

ii) Αν $a = \pi/2$*, τότε ο FrFT* $\mathcal{F}_a$ *ταυτίζεται με τον μετασχηματισμό Fourier*

iii) Αν $a/\pi = n \in \mathbb{Z}$, $\mathcal{F}_a(f) = \begin{cases} f(t) & n = 2k \\ f(-t) & n = 2k+1 \end{cases}$ *, αφού* $\mathcal{F}^2(f) = f(-t)$

iv) $\mathcal{F}_a(\delta(t-\gamma)) = K_a(\omega,\gamma)$

Εξάλλου, ορίζουμε την *συνάρτηση τάσης μεταβολής*[1] η οποία παίζει ιδιαίτερο ρόλο στην θεωρία Fourier

Ορισμός 1.2. Συνάρτηση τάσης μεταβολής είναι μια συνάρτηση η οποία σαρώνει ένα διάστημα του πεδίου συχνότητας $[\omega_0, \omega_1]$ μέσα σε ένα συγκεκριμένο χρονικό διάστημα $[t_0, t_1]$. Αν η σάρωση είναι γραμμική, τότε έχει την μορφή $e^{i\pi(\chi t+\gamma)t}$ όπου χ είναι ο ρυθμός σάρωσης.

Κάνουμε τώρα τις εξής παρατηρήσεις

Παρατήρηση 1.1. :

- Δεδομένου ότι ο FrFT είναι γραμμικός, το (iv) του πορίσματος (1.1) είναι μια συνάρτηση τάσης μεταβολής με ρυθμό σάρωσης $\cot a$, όπως φαίνεται από την σχέση (1.3) και τον ορισμό 1.2.
- $t^2\cot a - 2t\omega\csc a + \omega^2\cot a = t^2(\cot a - \csc a) + (t-\omega)^2\csc a + \omega^2(\cot a - \csc a)$

Άρα ο FrFT μπορεί να θεωρηθεί σαν μια συνέλιξη τάσης μεταβολής με ρυθμό σάρωσης $\csc a$ μεταξύ δύο πολλαπλασιασμών τάσης μεταβολής με ρυθμό σάρωσης $\cot a$ [6]

Ο συνήθης μετασχηματισμός Fourier μετασχηματίζει μια συνάρτηση από το πεδίο ορισμού του χρόνου στο πεδίο ορισμού της συχνότητας ή αντίστροφα. Καθότι γραμμικός, μπορεί να θεωρηθεί ως μια στροφή γωνίας $\pm\pi/2$ στο φασικό χώρο αντίστοιχα. Κατ' επέκτασιν, ο FrFT $\mathcal{F}_a$ μπορεί να ιδωθεί ως μια στροφή γωνίας a στο χώρο αυτό. Συνεπώς, εισάγεται η έννοια του FrFT ως τελεστή στροφής. Η έννοια αυτή μπορεί να γενικευτεί ακόμα περισσότερο, με την εισαγωγή των *γραμμικών κανονικών μετασχηματισμών*, οι οποίοι επιτρέπουν και άλλες πράξεις στο φασικό χώρο πέραν των στροφών.

[1] chirp function

Ορισμός 1.3. Οι γραμμικοί κανονικοί μετασχηματισμοί είναι μια οικογένεια ολοκληρωτικών μετασχηματισμών με τέσσερεις παραμέτρους και μπορούν να ιδωθούν ως στοιχεία της ομάδας SL_2. Αν $\mathcal{D}(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, τότε ο αντίστοιχος μετασχηματισμός $\mathcal{X}_g$ ορίζεται ως

$$\mathcal{X}_g(f)(\omega) = \begin{cases} \sqrt{-i}\, e^{-i\pi \frac{d}{b}\omega^2} \int_{-\infty}^{\infty} e^{-i2\pi \frac{1}{b}\omega t + i\pi \frac{a}{b} t^2} f(t)dt, & b \neq 0 \\ \sqrt{d}\, e^{-i\pi c d \omega^2} f(d\omega), & b = 0 \end{cases} \tag{1.4}$$

Ορισμός 1.4. Για κάθε $a \in \mathbb{R}$, ορίζεται ο τελεστής στροφής

$$\hat{\mathbf{F}}_a = \begin{bmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{bmatrix} \in SO(2,\mathbb{R}) \subset SL(2,\mathbb{R}) \tag{1.5}$$

που αντιστοιχεί σε στροφή γωνίας a στο επίπεδο.

Από τις σχέσεις (1.1) και (1.4) βλέπουμε ότι ο FrFT είναι ειδική περίπτωση γραμμικού κανονικού μετασχηματισμού για παράμετρο το στοιχείο της ομάδας SL_2 του ορισμού 1.4. Στο Κεφ.2, θα δούμε αναλυτικότερα πώς ο ορισμός αυτός συνδέει τον FrFT με τα ελλειπτικά στοιχεία της ομάδος SL_2 ή ισοδύναμα με τα στοιχεία της ομάδος SO_2

Όπως στην περίπτωση του συνήθη μετασχηματισμού Fourier, έτσι και στην περίπτωση του FrFT, όταν έχουμε να κάνουμε με διακριτές μεταβλητές στο πεδίο ορισμού της συνάρτησης που μας απασχολεί, ορίζεται ο διακριτός μετασχηματισμός (DFrFT).

Ορισμός 1.5. Ο διακριτός κλασματικός μετασχηματισμός Fourier ενός διανύσματος $f = (f(0), \ldots, f(N-1))$ ορίζεται ως το διάνυσμα $f_a = \mathbf{F}_a f$, δηλαδή το διάνυσμα με στοιχεία

$$[f_a]_j = \mathbf{F}_a f = \sum_{i=0}^{N-1} [\mathbf{F}_a]_{ji} [f]_i, \quad j = 0, 1, \ldots, N-1 \tag{1.6}$$

όπου $\mathbf{F}_a = \mathbf{E}\mathbf{\Lambda}^{2a/\pi}\mathbf{E}^\dagger$, με $\mathbf{F} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^\dagger$ μια ανάλυση ιδιοτιμών του πίνακα $\mathbf{F}$ του διακριτού μετασχηματισμού Fourier (DFT)

Ο DFrFT μπορεί να χρησιμοποιηθεί ως προσέγγιση του συνεχούς FrFT όταν το N είναι επαρκώς μεγάλο. Πέραν όμως της μεθόδου αυτής υπάρχουν και άλλες, βασισμένες στον FFT, προσεγγιστικές μέθοδοι για τον υπολογισμό του FrFT τις οποίες θα δούμε παρακάτω.

1.2 Μέθοδοι υπολογισμού

1.2.1 Υπολογισμός του FrFT

Παρ' όλη την ευρεία διάδοση που τυγχάνει τις τελευταίες δεκαετίες ο FrFT, δεν υπάρχουν παρά μόνον δύο ανοικτοί αλγόριθμοι για τον γρήγορο υπολογισμό του. Αμφότεροι οι αλγόριθμοι βασίζονται στον FFT, τον γνωστό αλγόριθμο για τον υπολογισμό του συνήθη DFT με πολυπλοκότητα $O(NlogN)$, αντί της προφανής $O(N^2)$ από τον ορισμό. Πρέπει να σημειωθεί, όμως, ότι κανείς από τους δύο δεν είναι το κλασματικό αντίστοιχο του FFT· μια τέτοια μέθοδος, η οποία θα άξιζε το

όνομα FFrFT, μένει ακόμα να βρεθεί. Αντ' αυτού, πρόκειται για προσεγγιστικές λύσεις, με περιορισμένη και συχνά - ανάλογα με την εφαρμογή - μη αποδεκτή ακρίβεια [6].

Οι δύο εν λόγω αλγόριθμοι ονομάζονται `fracF` [24] και `fractf` [23]. Η γενική ιδέα έχει ως εξής· βάσει της παρατήρησης 1.1 γράφουμε τον FrFT με την μορφή συνέλιξης μεταξύ δύο πολλαπλασιασμών τάσης μεταβολής[2].

$$\mathcal{F}_a(f)(\omega) = C_a e^{-i\pi \tan(a/2)\omega^2} \int_{-\infty}^{\infty} e^{i\pi \csc a(\omega - t)^2} [e^{-i\pi \tan(a/2)t^2}] f(t) dt \qquad (1.7)$$

Μια πρώτη προσέγγιση έγκειται στον περιορισμό των συναρτήσεων στο διάστημα $[-\Delta/2, \Delta/2]$, όπου $\Delta^2 = N$ το πλήθος των δειγμάτων της συνάρτησης f που θέλουμε να μετασχηματίσουμε. Τότε, σε δεύτερη φάση, μπορούμε να περιορίσουμε το ολοκλήρωμα του μετασχηματισμού στο διάστημα $[-\Delta, \Delta]$, παίρνοντας τουλάχιστον $2N$ δείγματα της συνέλιξης [24]. Η διαδικασία αυτή μας δίνει μια διακριτή προσέγγιση του FrFT, μετατρέποντας το ολοκλήρωμα σε άθροισμα με όρια από $-N$ έως $N-1$. Έτσι, για το σημείο $\omega_k = k/2\Delta$

$$\mathcal{F}_a(f)(\omega_k) \simeq \frac{C_a}{2\Delta} e^{-i\pi\omega_k^2 \tan(a/2)} \sum_{l=-N}^{N-1} g(k-l)h(l) \qquad (1.8)$$

όπου $t_k = k/2\Delta$ και

$$g(k) = e^{i\pi t_k^2 \csc a}, \quad h(k) = e^{-i\pi t_k^2 \tan(a/2)} f(t_k) \qquad (1.9)$$

Από την στιγμή που η διακριτή προσεγγιστική μορφή της σχέσης (1.8) έχει την μορφή συνέλιξης, μπορούμε να χρησιμοποιήσουμε τον FFT και να υπολογίσουμε τον μετασχηματισμό σε χρόνο $O(NlogN)$· εξού και η ονομασία *γρήγορος προσεγγιστικός κλασματικός μετασχηματισμός Fourier* για την διαδικασία.

Πρέπει να πούμε ότι ενώ και οι δύο αλγόριθμοι βασίζονται στην ίδια γενική ιδέα, έχουν κάποιες διαφορές στην υλοποίηση. Μια σημαντική διαφορά μεταξύ των δύο αλγορίθμων έχει να κάνει με τα όρια στο κατά προσέγγισιν άθροισμα· τα όρια δεν είναι συμμετρικά, ενώ το διάστημα δειγματοληψίας έχει θεωρηθεί άρτιο $(2N)$. Αυτό κάνει φυσικό να προτιμήσουμε ένα διάστημα δειγματοληψίας περιττού μήκους, πράγμα που γίνεται στον `fractf`, εν αντιθέσει με τον `fracF`.

Εξάλλου, ο FFT ορίζεται ως ο μετασχηματισμός ενός διανύσματος της μορφής $(f(0), \ldots, f(N-1))$, ενώ ο προσεγγιστικός κλασματικός αλγόριθμος που περιγράψαμε, δρα πάνω σε διανύσματα της μορφής $(f(-N), \ldots, f(N-1))$. Αυτό σημαίνει ότι η εν λόγω διαδικασία δεν θα δώσει τα ίδια αποτελέσματα με τον FFT στην περίπτωση $2a/\pi \in \mathbb{Z}$ όπως θα θέλαμε. Το πρόβλημα αυτό αντιμετωπίζεται την περίπτωση του `fracF` διακρίνοντας περιπτώσεις για την παράμετρο a, ενώ στον `fractf` επιχειρείται μια κυκλική μετάθεση του σήματος μέτρου περίπου ίσου με το μισό του μήκους του σήματος. Αυτό σημαίνει, μιας και για τον αλγόριθμο αυτόν το μήκος του σήματος θεωρείται περιττό, ότι υπεισέρχεται μια ασυμμετρία η οποία θα συντελεί σε πρόσθετες διαφορές στα αποτελέσματα μεταξύ των δύο αλγορίθμων

Τέλος, γνωρίζουμε ότι ο μετασχηματισμός Fourier έχει περίοδο ίση με 4, δηλ. $\mathcal{F}^4 = \mathcal{F}$ [22]. Αυτό σημαίνει ότι υπολογίζοντας τον FrFT για τιμές του $n \equiv 2a/\pi \pmod 4$, και χρησιμοποιώντας την ιδιότητα (i) από το πόρισμα 1.1,

[2] Η μορφή αυτή είναι γνωστή στον χώρο της ανάλυσης σήματος ως *chirp z-transform*[4]

μπορούμε να ανάγουμε το διάστημα της παραμέτρου n σε διάστημα μήκους 2. Οι δύο αλγόριθμοι, με μερικούς πρόσθετους ελέγχους για την τιμή του n και με την βοήθεια της παραπάνω παρατήρησης, ανάγουν εν τέλη την παράμετρο n στο διάστημα $(0.5, 1.5)$ στην περίπτωση του `fracF` και στον $[0.5, 1.5]$ στην περίπτωση του `fractf`. Η διαφορά στα ανοικτά/κλειστά όρια του διαστήματος αυτού επιφέρει διαφορές στα αποτελέσματα όταν η παράμετρος n έχει τιμή κοντά στα όρια.

1.2.2 Υπολογισμός του DFrFT

Στην παράγραφο 1.1 δώσαμε έναν ορισμό (1.5) για την διακριτή μορφή του μετασχηματισμού Fourier. Έχουν προταθεί διάφοροι εναλλακτικοί ορισμοί για τον DFrFT, ο καθένας με τα προτερήματά του, όπως συμβατότητα με τον FFT [4, 24] και τα μειονεκτήματά του, με κυριότερο αυτό της μη-μοναδιαιότητας. Ο ορισμός που δώσαμε βασίζεται στην αρχική δουλειά των Pei και Yeh [25] και την μετέπειτα δουλειά των Candan, Kutay και Ozaktas [8]. Τον διαλέξαμε γιατί είναι ο μόνος γνωστός ορισμός ο οποίος πληροί της προϋποθέσεις που χρειάζονται για να ισχύει το πόρισμα 1.1 και να είναι ο τελεστής του μετασχηματισμού μοναδιαίος· ως εκ τούτου, αποτελεί τον πιο «φυσικό» ορισμό που έχει την ίδια σχέση με τον FrFT που έχει ο DFT με τον συνήθη μετασχηματισμό Fourier.

Στην περίπτωσή μας λοιπόν, το βασικό πρόβλημα έγκειται στο να υπολογίσουμε τον πίνακα $\mathbf{F}^n$, $n = 2a/\pi$, όπου

$$\mathbf{F} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix}, \quad \omega = e^{-2i\pi/N} \tag{1.10}$$

είναι ο πίνακας που αναπαριστά τον μετασχηματισμό Fourier, όταν αυτός είναι ορισμένος ως μοναδιαίος τελεστής επί του $L^2(\mathbb{R}^n)$, γνωστός και ως πίνακας *Vandermonde* των ριζών της μονάδος. Εν γένει, η εύρεση της n-οστής δύναμής του για μη ακέραιες τιμές είναι επίπονη διαδικασία που υλοποιείται με την μέθοδο της ανάλυσης ιδιοτιμών (*βλ.* ορισμό 1.5). Είναι εύκολο να δει κανείς ότι αν $\mathbf{A} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger$, τότε για $n \in \mathbb{Z}$, $\mathbf{A}^n = \mathbf{V}\mathbf{\Lambda}^n\mathbf{V}^\dagger$. Η σχέση αυτή μπορεί να γενικευτεί και στην περίπτωση που το n δεν είναι ακέραιος, για να ορίσουμε κλασματικές δυνάμεις πινάκων, αφού προφανώς όταν $\mathbf{\Lambda} = \mathrm{diag}(\lambda_{ii})$, $\mathbf{\Lambda}^n = \mathrm{diag}(\lambda_{ii}^n)$.

Καθότι οι ιδιοτιμές του $\mathbf{F}$ είναι γνωστές και ίσες με

$$\left\{ (-i)^n \;\middle|\; n = 0, 1, 2, \dots, N-2, K, \quad K = \begin{cases} N-1, & N \text{ άρτιο} \\ N, & N \text{ περιττό} \end{cases} \right\} \tag{1.11}$$

ο διαγώνιος πίνακας $\mathbf{\Lambda}$ της ανάλυσης ιδιοτιμών βρίσκεται αμέσως. Απομένει η εύρεση των ιδιοδιανυσμάτων του εν λόγω πίνακα, τα οποία είναι διακριτά ανάλογα των συναρτήσεων Hermite, δηλαδή των ιδιοσυναρτήσεων του συνήθη μετασχηματισμού Fourier υπό την μοναδιαία αναπαράστασή του [26]. Οι συναρτήσεις Hermite ψ_n ορίζονται ως

$$\psi_n(x) = \frac{2^{1/4}}{\sqrt{n!}} e^{-\pi x^2} H(2x\sqrt{\pi}) \tag{1.12}$$

όπου $H_n(x)$ είναι τα πολυώνυμα Hermite τα οποία ικανοποιούν την σχέση [35]

$$H_n'' - 2xH_n' + 2nH_n = 0 \tag{1.13}$$

Συνεπώς, τα ιδιοδιανύσματα ψ_k του $\mathbf{F}^n$ θα πρέπει να προσεγγίζουν τις συναρτήσεις Hermite [6]

$$[\psi_k]_x = \frac{2^{1/4}}{\sqrt{k!}} e^{-\pi x^2} H(2x\sqrt{\pi}) \tag{1.14}$$

Μια δυσκολία που έγκειται στην εύρεση των ιδιοδιανυσμάτων είναι ότι επειδή οι ιδιοτιμές είναι εκφυλισμένες και υπάρχουν μόνον τέσσερεις διαφορετικές, η επιλογή των ιδιοδιανυσμάτων δεν είναι μονοσήμαντη, αν και θέλουμε να είναι ορθογώνια και να έχουν την ίδια συμμετρία με τα αντίστοιχα πολυώνυμα Hermite. Η δυσκολία επιλύεται με το να υπολογίσουμε την ανάλυση ιδιοτιμών ενός πίνακα $\mathbf{H}$ τον οποίον κατασκευάζουμε έτσι ώστε να έχει μόνο μη-εκφυλισμένες ιδιοτιμές - και άρα ορθογώνια ιδιοδιανύσματα - και που να αντιμετατίθεται με τον $\mathbf{F}$ - άρα θα έχουν κοινά ιδιοδιανύσματα. Αποδεικνύεται [8] ότι ο πίνακας αυτός είναι η αναπαράσταση του τελεστή

$$\mathbf{H} = \pi(\mathbf{U}^2 + \mathbf{D}^2) \tag{1.15}$$

όπου $\mathbf{D}$ είναι ο διαφορικός τελεστής

$$\mathbf{D}f(x) = (i2\pi)^{-1} df(x)/dx \tag{1.16}$$

και $\mathbf{U}$ είναι ο τελεστής μετατόπισης

$$\mathbf{U}f(x) = xf(x), \text{ ή ισοδύναμα } \mathbf{U} = \mathcal{F}\mathbf{D}\mathcal{F}^{-1} \tag{1.17}$$

Μπορούμε να προσεγγίσουμε τον τελεστή $\mathbf{D}$ ως

$$\mathbf{D}^2 \simeq \mathbf{S}^{-1} - 2\mathbf{I} + \mathbf{S}, \quad \mathbf{S}f(k) = f(k+1), \quad k = 0, 1, \ldots, N-1 \tag{1.18}$$

ή ως [7]

$$\mathbf{D}^2 \simeq \sum_{p=1}^{m} (-1)^{p-1} \frac{|(p-1)!|^2}{(2p)!} (\delta^2)^p \tag{1.19}$$

αν θέλουμε προσεγγίσεις μεγαλύτερης τάξης, όπου η παράμετρος m δίνει την τάξη της προσέγγισης, η οποία είναι $2m$. Τότε για τον $\mathbf{U}$ έχουμε

$$\mathbf{U} = \mathbf{F}\mathbf{D}\mathbf{F}^{-1} \simeq \mathbf{M}^{-1} - 2\mathbf{I} + \mathbf{M}, \quad \begin{array}{r} \mathbf{M}f(k) = e^{ik2\pi/N} f(k), \\ k = 0, 1, \ldots, N-1 \end{array} \tag{1.20}$$

Από τις σχέσεις (1.15), (1.18) και (1.20) τελικά έχουμε

$$[Hf]_k \simeq f(k-1) + 2(\cos\frac{2k\pi}{N} - 2)f(k) + f(k+1) \tag{1.21}$$

ή αλλιώς

$$\mathbf{H} = \begin{pmatrix} 2 & 1 & 0 & \ldots & 0 & 1 \\ 1 & 2\cos\frac{2\pi}{N} & 1 & \ldots & 0 & 0 \\ 0 & 1 & 2\cos 2\frac{2\pi}{N} & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \ldots & 1 & 2\cos(N-1)\frac{2\pi}{N} \end{pmatrix} - 4\mathbf{I}_N \tag{1.22}$$

Χάριν της συμμετρίας των ιδιοδιανυσμάτων ψ_n - άρτια ή περιττά, ανάλογα με την αντίστοιχη τιμή του n - η ανάλυση του $\mathbf{H}$ μπορεί να γραφεί

$$\mathbf{V}\mathbf{H}\mathbf{V}^\dagger = \begin{pmatrix} \mathbf{E} & \\ & \mathbf{O} \end{pmatrix} \tag{1.23}$$

όπου $\mathbf{E}$ είναι ο πίνακας με στήλες τα άρτια ιδιοδιανύσματα, $\mathbf{O}$ αυτός με τα περιττά και

$$\mathbf{V} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & & \\ & \mathbf{I}_r & \mathbf{J}_r \\ & \mathbf{J}_r & -\mathbf{I}_r \end{pmatrix}, \quad r = (N-1)/2 \tag{1.24}$$

αν το N είναι περιττό, ενώ αν είναι άρτιο

$$\mathbf{V} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & & & \\ & \mathbf{I}_r & & \mathbf{J}_r \\ & & 1 & \\ & \mathbf{J}_r & & -\mathbf{I}_r \end{pmatrix}, \quad r = (N-2)/2 \tag{1.25}$$

με $\mathbf{J}_r$ τον αντιμοναδιαίο $r \times r$ πίνακα. Τότε, αν οι αναλύσεις των $\mathbf{E}$ και $\mathbf{O}$ είναι

$$\mathbf{E} = \mathbf{V}_e \mathbf{\Lambda}_e \mathbf{V}_e^\dagger \quad \text{και} \quad \mathbf{O} = \mathbf{V}_o \mathbf{\Lambda}_o \mathbf{V}_o^\dagger \tag{1.26}$$

θα έχουμε

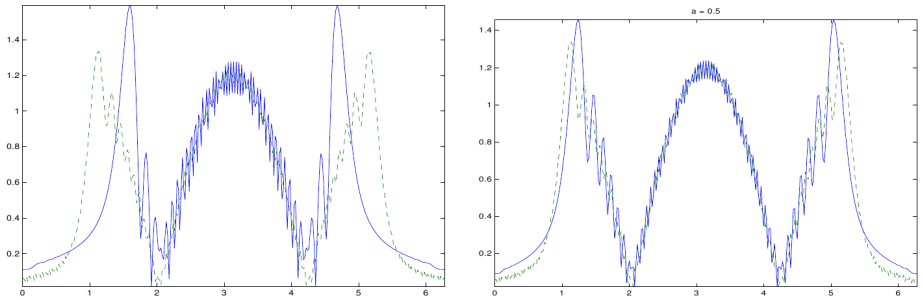
$$\mathbf{G}\mathbf{H}\mathbf{G}^\dagger = \begin{pmatrix} \mathbf{\Lambda}_e & \\ & \mathbf{\Lambda}_o \end{pmatrix}, \quad \mathbf{G} = \mathbf{V} \begin{pmatrix} \mathbf{V}_e & \\ & \mathbf{V}_o \end{pmatrix} \tag{1.27}$$

Με άλλα λόγια, οι στήλες του πίνακα $\mathbf{G}$ είναι τα ιδιοδιανύσματα που θέλαμε.

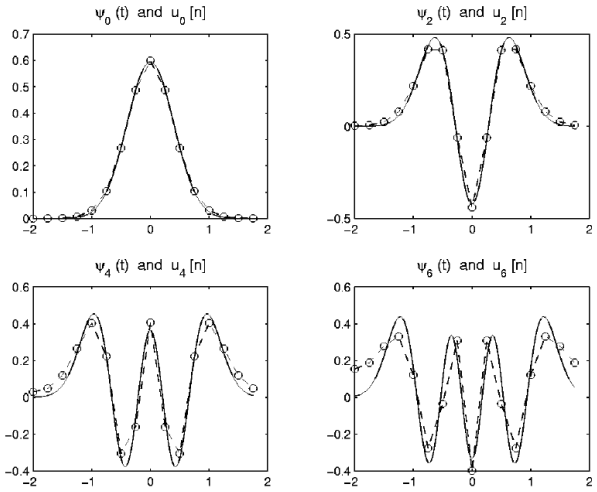
Η παραπάνω διαδικασία μπορεί να περιγραφεί αλγοριθμικά ως εξής

1. Υπολογίζουμε τον πίνακα $\mathbf{H}$
2. Υπολογίζουμε τον πίνακα μετασχηματισμού $\mathbf{V}$
3. Υπολογίζουμε τους πίνακες $\mathbf{E}$ και $\mathbf{O}$ από την ανάλυση $\mathbf{V}\mathbf{H}\mathbf{V}^\dagger$
4. Υπολογίζουμε τα ιδιοδιανύσματα $\mathbf{V}_e$ και $\mathbf{V}_o$ των $\mathbf{E}$ και $\mathbf{O}$
5. Μετασχηματίζουμε τα αποτελέσματα του παραπάνω βήματος με τον πίνακα $\mathbf{V}$ στον πίνακα $\mathbf{G}$
6. Ανακατανέμουμε τις στήλες του πίνακα $\mathbf{G}$ έτσι ώστε να ταιριάζουν με τις αντίστοιχες ιδιοτιμές $(-i)^n$
7. Υπολογίζουμε τον πίνακα $\mathbf{F}_a = \mathbf{G}\mathbf{\Lambda}^{2\alpha/\pi}\mathbf{G}^\dagger$

Η πολυπλοκότητα του αλγορίθμου αυτού, καθορίζεται από τα βήματα που κάνουν ανάλυση ιδιοτιμών, άρα είναι $O(N^3)$. Είναι σημαντικά μεγαλύτερη από αυτή των μεθόδων που βασίζονται στο FFT, όπως αυτές που στηρίζονται σε εναλλακτικούς ορισμούς και η διακριτή προσέγγιση που κάναμε στην προηγούμενη παράγραφο για τον FrFT. Αν κάνουμε, όμως, μια αντιπροσωπευτική σύγκριση αποτελεσμάτων μεταξύ του αλγορίθμου αυτού και του προσεγγιστικού αλγορίθμου, βλέπουμε (σχ. 1.1) ότι η απόκλιση του τελευταίου είναι ιδιαίτερα αισθητή



Σχ. 1.1: Η απόλυτη τιμή του FrFT $\mathcal{F}^{0.5}(\cos)(x)$ (διακεκομμένη γραμμή) και του DFrFT $\mathbf{F}^{0.5}(\cos)(x)$ (συνεχής γραμμή), για $x \in [0, 2\pi]$ με βήμα 0.02. Στα αριστερά για τάξη προσέγγισης 4 και στα αριστερά 60.



Σχ. 1.2: Σύγκριση των συναρτήσεων Hermite $\psi_0, \psi_2, \psi_4, \psi_6$ με τα αντίστοιχα ιδιοδιανύσματα του πίνακα του DFrFT.

για μικρή τάξη προσέγγισης, ενώ τείνει να εξαλειφθεί μόνον όταν αυξάνουμε σημαντικά την τάξη προσέγγισης. Ακόμα, παρατηρούμε ότι η μέγιστη απόκλιση εντοπίζεται κοντά στα όρια του πεδίου τιμών, κάτι που το περιμέναμε από τις προσεγγίσεις των ορίων και τις μεταθέσεις στα διανύσματα του σήματος που κάναμε. Άρα λοιπόν, όταν η εφαρμογή απαιτεί μεγαλύτερη ακρίβεια από αυτήν που μπορεί να δώσει ο προσεγγιστικός αλγόριθμος και χρειαζόμαστε της ιδιότητες του πορίσματος 1.1, αναγκαστικά θα πρέπει να βασιστούμε στον ορισμό 1.5 του DFrFT, για τον οποίον μια λύση μικρότερης πολυπλοκότητας θα ήταν ποθητή.

Αν και στην αρχή της παραγράφου δικαιολογήσαμε την επιλογή του συγκεκριμένου ορισμού για τον DFrFT με το επιχείρημα ότι είναι η πιο φυσική επέκταση του ορισμού του συνεχή μετασχηματισμού με τις καλές ιδιότητες που θέλαμε, δεν παύει να είναι ένας ad hoc προσεγγιστικός ορισμός. Η επιλογή των ιδιοδιανυσμάτων ως προσέγγιση των συναρτήσεων Hermite δεν δικαιολογείται παρά μόνο διαισθητικά και δεν άρει τον εκφυλισμό των ιδιοτιμών του πίνακα του μετασχηματισμού Fourier. Εξάλλου, στο σχήμα 1.2 βλέπουμε μια αντιπροσωπευτική σύγκριση των συναρτήσεων Hermite με τα αντίστοιχα ιδιοδιανύσματα του πίνακα του DFrFT, όπου η εγγενώς προσεγγιστική φύση του ορισμού γίνεται αισθητή.

Από την άλλη, γνωρίζουμε ότι οι ιδιοκαταστάσεις του κβαντικού αρμονικού ταλαντωτή, ικανοποιούν τη σχέση [35]

$$\psi_n(x) \propto e^{-x^2/2} H_n(x) \tag{1.28}$$

Η σχέση (1.28) είναι στην ουσία ίδια με την σχέση (1.12) που δίνει τις ιδιοσυναρτήσεις του συνεχούς μετασχηματισμού Fourier. Έτσι λοιπόν, εφαρμόζοντας την κβάντωση Weyl στον φασικό χώρο του αρμονικού ταλαντωτή, ο μετασχηματισμός Weyl του ομομορφισμού βηματικής χρονικής εξέλιξης προκύπτει με φυσικό τρόπο να είναι ο διακριτός μετασχηματισμός Fourier. Στο κεφάλαιο που ακολουθεί θα επιχειρήσουμε να δώσουμε έναν νέο ορισμό για τον DFrFT, ο οποίος θα είναι εγγενώς ακριβής, μελετώντας το κατάλληλο φυσικό σύστημα και εφαρμόζοντας αναλυτικά την παραπάνω διαδικασία.

2 Ο διακριτός FrFT

Στο κεφάλαιο αυτό, εξετάζουμε τον μαθηματικό φορμαλισμό που περιγράφει την κίνηση ενός σωματίου σε έναν διακριτό κύκλο, υπό διακριτό χρόνο. Θα δούμε ότι τέτοια συστήματα περιγράφονται από χώρους φάσης με την δομή σωμάτων Galois και θα εστιαστούμε σε ένα συγκεκριμένο τέτοιο σύστημα, τον ταλαντωτή Balian-Itzykson, που είναι μια παραλλαγή του κβαντικού αρμονικού ταλαντωτή. Μελετώντας την άλγεβρα της ομάδας που περιγράφει την φυσική του, θα καταλήξουμε σε μια αναπαράσταση του διακριτού κλασματικού μετασχηματισμού Fourier μέσα από τους τελεστές που δρουν στον φασικό χώρο, όπως πρώτος σημείωσε ο H. Weyl. Η αναπαράσταση αυτή του DFrFT θα αποτελέσει τον νεό ορισμό που δίνουμε για τον μετασχηματισμό και θα είναι το έναυσμα για την μελέτη ενός κβαντικού κυκλώματος για τον υπολογισμό του.

2.1 Χώροι φάσης Galois

2.1.1 Κίνηση σε διακριτό κύκλο

Έστω ένα σωμάτιο που κινείται σε ένα διακριτό κύκλο αποτελούμενο από έναν πεπερασμένο αριθμό N ισαπεχουσών θέσεων. Αν εξετάσουμε το σύστημα «στροβοσκοπικά», δηλαδή υπό διακριτό χρόνο σε ισαπέχουσες στιγμές, τότε ο κλασικός φασικός χώρος του σωματίου αυτού είναι ένα δισδιάστατο τοροειδές πλέγμα $N \times N$. Η κλασική μηχανική της κίνησης περιγράφεται από κάποιον επαναλαμβανόμενο κανονικό μετασχηματισμό επί του φασικού χώρου και αν υποθέσουμε ότι το σωμάτιο εκτελεί κάποιας μορφής αρμονική ταλάντωση, τότε η Χαμιλτονιανή του είναι τετραγωνική ως προς την θέση και την ορμή και άρα ο μετασχηματισμός είναι γραμμικός. Αντίστοιχα, η κβαντομηχανική του συστήματος θα περιγράφεται από έναν μοναδιαίο μετασχηματισμό εξέλιξης.

Συγκεκριμένα, κατατέμνουμε τον παραμετρικό χώρο του τόρου $\mathbb{T}^2 = \mathcal{S}^1 \times \mathcal{S}^1$ σε δύο διακριτούς κύκλους

$$\begin{aligned} \mathbb{Z}_N &= \{0, 1, \ldots, N-1\}, \\ \mathcal{S}^1_N &\equiv \tfrac{4\pi}{N}\mathbb{Z}_N \end{aligned} \tag{2.1}$$

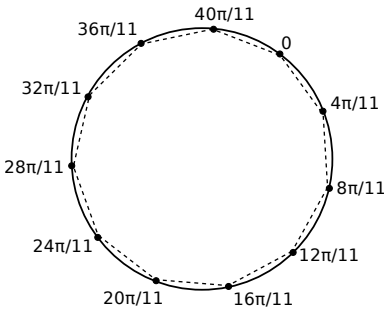
που αντιπροσωπεύουν την ορμή και την θέση αντίστοιχα του σωματίου επί του κύκλου στις θέσεις με γωνία $0, 4\pi/N, \ldots, 4\pi(N-1)/N$. Τότε ο διακριτός τόρος $\mathbb{T}^2_N$ που προκύπτει, περιγράφει τον εν λόγω φασικό χώρο και με τις κατάλληλες μονάδες ($\Delta q = \Delta p = 1$) μπορεί να κωδικοποιηθεί από τα ζεύγη ακεραίων [11]

$$\mathbb{T}^2_N = \{(m, n) | m, n = 0, 1, 2, \ldots, N-1\} \tag{2.2}$$

Πριν προχωρήσουμε παρακάτω, θα δώσουμε μερικούς απαραίτητους ορισμούς.

Ορισμός 2.1. Έστωσαν πολλαπλότητες M, N και ισομορφισμός $f : M \to N$. Τότε η f ονομάζεται *διαφορομορφισμός* αν αυτή και η αντίστροφή της είναι λείες.

Ορισμός 2.2. Έστω πολλαπλότητα M και κλειστή, μη-εκφυλισμένη 2-μορφή ω. Τότε η πλειάδα (M, ω) ονομάζεται *συμπλεκτική πολλαπλότητα* και η ω ονομάζεται *συμπλεκτική μορφή*.



Σχ. 2.1: Ο διακριτός κύκλος S^1_{11} ως γεωμετρικός χώρος θέσης, με 11 πλεγματικά στοιχεία. Σημειώνεται ότι το 11 είναι πρώτος αριθμός και ότι $p = 4k - 1$, όπου $p = 11$ και $k = 3$.

Αν X_i είναι μια βάση του εφαπτομενικού χώρου ενός οποιουδήποτε σημείου της M, ο πίνακας $\Omega_{ij} = \omega(X_i, X_j)$ είναι μη-μοναδιακός, δηλαδή $\det \Omega \neq 0$. Σημειώνεται ότι στον φορμαλισμό της κλασικής μηχανικής, οι φασικοί χώροι αποτελούν συμπλεκτικές πολλαπλότητες.

Ορισμός 2.3. Έστωσαν συμπλεκτικές πολλαπλότητες $(M_1, \omega_1), (M_2, \omega_2)$. Ο ομομορφισμός $f : M_1 \to M_2$ ονομάζεται *συμπλεκτομορφισμός* αν είναι διαφορομορφισμός και $f^*\omega_2 = \omega_1$, όπου $(f^*\omega)(\mathbf{x}) \equiv \omega(f(\mathbf{x}))$ η *υποχώρηση*[3] της ω υπό της f

Οι κανονικοί μετασχηματισμοί, αποτελούν μια ειδική περίπτωση συμπλεκτομορφισμών, όπως φαίνεται από τον παρακάτω ορισμό

Ορισμός 2.4. Έστω φασικός χώρος $M =< \mathbf{e_{q_1}}, \ldots, \mathbf{e_{q}}_n, \mathbf{e_{p_1}}, \ldots, \mathbf{e_{p}}_n, \mathbf{e_t} >$ και συμπλεκτομορφισμός $f : M \to M$, τέτοιος ώστε $f(\mathbf{q}, \mathbf{p}, t) = (\mathbf{q}', \mathbf{p}', t)$ και που να διατηρεί την μορφή των Χαμιλτονιανών εξισώσεων. Τότε ο f ονομάζεται *κανονικός μετασχηματισμός ή Χαμιλτονιανός συμπλεκτομορφισμός*

Μια σημαντική ιδιότητα των κανονικών μετασχηματισμών αποτελεί το θεώρημα του Liouville για την Χαμιλτονιανή Μηχανική το οποίο και θα χρειαστούμε παρακάτω

Θεώρημα 2.1. *Το μέτρο του φασικού χώρου διατηρείται σταθερό κατά μήκος των τροχιών του συστήματος που περιγράφει ο χώρος αυτός.*

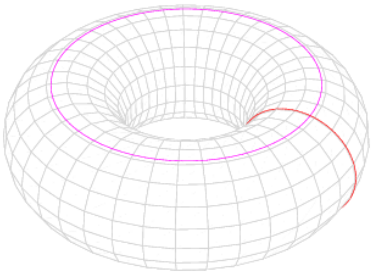
Άμεσο πόρισμα του παραπάνω θεωρήματος είναι το εξής, το οποίο επίσης καλείται εναλλακτικά ως θεώρημα Liouville

Πόρισμα 2.1. *Ο όγκος σε ένα φασικό χώρο διατηρείται σταθερός υπό τη δράση κανονικών μετασχηματισμών, δηλ.* $\int d\mathbf{q}d\mathbf{p} = \int d\mathbf{q}'d\mathbf{p}'$

Επιστρέφοντας στη συζήτηση περί της κίνησης σε διακριτό κύκλο, παρατηρούμε ότι ένας γραμμικός κανονικός μετασχηματισμός του φασικού χώρου (q, p) περιγράφεται από 2×2 πίνακες $\mathbf{T}$

$$\begin{pmatrix} q_2 \\ p_2 \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} \tag{2.3}$$

[3] Ελεύθερη απόδοση του αγγλικού όρου *pullback*



Σχ. 2.2: Ο διακριτός τόρος $\mathbb{T}^2_{39} = \mathcal{S}^1_{39} \times \mathbb{Z}_{39}$ ως γινόμενο δύο κύκλων.

Από το θεώρημα του Liouville υπό την μορφή του πορίσματος 2.1 συνεπάγεται ότι

$$\det \mathbf{T} = T_{11}T_{22} - T_{12}T_{21} \equiv 1 \pmod{N} \tag{2.4}$$

Εξάλλου, απαραίτητη συνθήκη για να διατηρείται η περιοδικότητα του πλέγματος $\Delta q \times \Delta p$ του φασικού χώρου είναι οι πίνακες T να χαρτογραφούν πλεγματικά σημεία μόνο σε πλεγματικά σημεία. Με το σύστημα μονάδων που υιοθετήσαμε ($\Delta q = \Delta p = 1$), αυτό σημαίνει ότι τα στοιχεία των πινάκων πρέπει να είναι ακέραιοι αριθμοί[16]. Διαφαίνεται λοιπόν, ότι οι πίνακες T που περιγράφουν την κλασική φυσική εξέλιξη του συστήματος μπορούν να αποτελέσουν, με πράξη τον πολλαπλασιασμό πινάκων modulo N, την κατάλληλη αναπαράσταση της ομάδας $SL_2(\mathbb{Z}_N)$ των γραμμικών κανονικών μετασχηματισμών αυτού του φασικού χώρου, αρκεί να εξασφαλίσουμε την ύπαρξη αντιστρόφου.

2.1.2 Πρώτοι αριθμοί, συμπλεκτικές ομάδες και σώματα Galois

Προς τον σκοπό αυτό, υποθέτουμε ότι ο αριθμός N των πλεγματικών σημείων είναι πρώτος, $N = p$, αφού ο αντίστροφος ενός ακεραίου modulo N είναι μοναδικός αν και μόνο αν ο N είναι πρώτος[2]. Τότε, το σύνολο των ακεραίων

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\} \tag{2.5}$$

είναι κλειστό υπό τις συνήθεις αριθμητικές πράξεις. Μαζί με αυτές, αποτελεί το απλούστερο από τα πεπερασμένα σώματα Galois $GF[p^n]$ με $n = 1$.

Συνεπώς, λαμβάνοντας υπ' όψιν όλες τις παραπάνω συνθήκες, οι πίνακες T αποτελούν αναπαράσταση της ειδικής γραμμικής ομάδας $SL(2, \mathbb{Z}_p)$, αλλά και της συμπλεκτικής ομάδας $Sp(2n, \mathbb{Z}_p)$ με $n = 1$ [5, 13, 27][4]. Μια επιλογή για τους γεννήτορες της $SL(2, \mathbb{Z}_p)$ είναι η εξής

$$g_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} g & 0 \\ 0 & g^{-1} \end{pmatrix}, g_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2.6}$$

όπου g είναι το θεμελιακό στοιχείο της πολλαπλασιαστικής ομάδας $GF^*[p] = GF[p]\backslash\{0\}$[2]. Αντί του g_3 μπορεί κανείς να επιλέξει το θεμελιακό στοιχείο R_0 της αβελιανής υποομάδας $O(2, \mathbb{Z}_p)$ της $SL(2, \mathbb{Z}_p)$, των πινάκων που αντιμετατίθενται με το g_3[5]

$$O(2, \mathbb{Z}_p) := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a^2 + b^2 \equiv 1 \pmod{p} \right\} = \{R_0, R_0^2, \ldots, R_0^{4k}\} \tag{2.7}$$

[4] Τυγχάνει για $n = 1$, οι ομάδες SL_2 και Sp_{2n} να είναι ταυτίζονται

Παρατηρούμε ότι κάθε θεμελιακό στοιχείο R_0 έχει περίοδο $4k$, όπου $p = 4k \pm 1$, που είναι η τάξη της κυκλικής ομάδας $O(2, \mathbb{Z}_p)$.

Τα τρία θεμελιακά στοιχεία της $SL(2, \mathbb{Z}_p)$, καθότι είναι κανονικοί μετασχηματισμοί φυσικής εξέλιξης, αντιπροσωπεύουν από ένα είδος φυσικής κίνησης· το g_1 αντιπροσωπεύει ελεύθερη κίνηση, το g_2 υπερβολική και το τρίτο, R_0, ταλαντωτική όπως θα δούμε παρακάτω, με περιόδους p, $p-1$ και $4k$ [16, 5]. Σημειώνεται ότι από το θεώρημα Lagrange της θεωρίας ομάδων, οι περίοδοι των στοιχείων της $SL(2, \mathbb{Z}_p)$ πρέπει να διαιρούν την τάξη της $p(p^2-1)$, άρα θα πρέπει να διαιρούν το p, το $p-1$ ή το $p+1$[16]. Από τα τρία παραπάνω είδη φυσικής κίνησης, θα μας απασχολήσει η χβαντομηχανική του τελευταίου, R_0, του επονομαζόμενου «αρμονικού ταλαντωτή» Balian-Itzykson[5].

Είδαμε ότι το θεμελιακό στοιχείο R_0 της $O(2, \mathbb{Z}_p)$ (2.7), έχει περίοδο $4k$, όπου $p = 4k \pm 1 \Rightarrow k = \frac{p \pm 1}{4}$. Διακρίνουμε τις δύο περιπτώσεις για τις δυνατές τιμές του k βάσει του p [3]

- $p = 4k + 1$

Στην περίπτωση αυτή, το R_0 και συνεπώς όλα τα στοιχεία της $O(2, \mathbb{Z}_p)$ είναι διαγωνίσιμα από τον πίνακα P, όπως θα δείξουμε ευθέως:

$$\begin{pmatrix} a - tb & 0 \\ 0 & a + tb \end{pmatrix} = P^{-1} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} P \tag{2.8}$$

όπου

$$P = \frac{1}{\sqrt{2t}} \begin{pmatrix} 1 & 1 \\ t & -t \end{pmatrix} \tag{2.9}$$

και $t^2 \equiv -1 \pmod{p}$. Παρατηρούμε ότι $t = [\frac{1}{2}(p-1)]!$ είναι λύση στο $GF[p]$ και ότι $2t = (1+t)^2$, ώστε $\sqrt{2t} = 1 + t \in GF[p]$

Επιλέγουμε

$$a - tb = g, \quad a + tb = g^{-1} \tag{2.10}$$

όπου g είναι το θεμελιακό στοιχείο της $GF^*[p]$. Τότε, τα

$$a_0 = \tfrac{1}{2}(g + g^{-1}), \quad b_0 = \tfrac{g^{-1} - g}{2t} \tag{2.11}$$

αποτελούν τα στοιχεία του R_0:

$$R_0 = \begin{pmatrix} a_0 & b_0 \\ -b_0 & a_0 \end{pmatrix} \tag{2.12}$$

Από την στιγμή που το R_0 είναι διαγωνίσιμο, δεν διαφέρει ουσιαστικά από τον g_2 (σχ. 2.6) και συνεπώς δεν έχουμε πραγματική ταλαντωτική κίνηση.

- $p = 4k - 1$

Στην περίπτωση αυτή, έχουμε «πραγματικές» στροφές με «μιγαδικές» ιδιοτιμές. Από την χαρακτηριστική εξίσωση για το R_0

$$|R_0^n - \lambda I| = 0 \Rightarrow \lambda = a_0 \pm i b_0 \tag{2.13}$$

διακρίνουμε την περίπτωση $\lambda = a_0 - i b_0$. Πρόκειται για τις ιδιοτιμές των στοιχείων της υποομάδας $SO(2, \mathbb{Z}_p)$ γνωστή και ως ομάδα στροφών. Η άλλη περίπτωση

αφορά τα στοιχεία της O_2 που δεν ανήκουν στην SO_2, τα οποία δεν αντιπροσωπεύουν «πραγματικές» στροφές, αλλά ανακλάσεις και δεν αποτελούν ομάδα. Οι ιδιοτιμές της $SO(2,\mathbb{Z}_p)$ ανήκουν στην τετραγωνική επέκταση του $GF[p]$ [19]

$$GF[p^2] = \{0, 1, 2, \ldots, p^2 - 1\} \tag{2.14}$$

η οποία μπορεί να ορισθεί εναλλακτικά ως το ισόμορφο σώμα

$$GF[p^2] = \{a - ib | a, b \in GF[p], i^2 = -1\} \tag{2.15}$$

Παρατηρούμε επίσης ότι το $GF[p^2]$ είναι ισόμορφο και με τον τόρο $\mathbb{T}_p^2$. Πάνω στο $GF[p^2]$ δρα η $SO(2,\mathbb{Z}_p)$ μέσω πολλαπλασιασμού

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \rightarrow (a - ib)(x + iy) \tag{2.16}$$

ή, σε τελεστική μορφή

$$\mathbf{R_0}|u\rangle = (a - ib)|u\rangle \tag{2.17}$$

όπου $|u\rangle$ είναι στοιχείο του διανυσματικού χώρου $\mathcal{V} = (GF[p^2], \mathbb{C})$. Έχουμε δηλαδή έναν τελεστή στροφής $\mathbf{R_0}$ για τον φασικό μας χώρο, πράγμα που επιβεβαιώνει τον προηγούμενό μας ισχυρισμό ότι το στοιχείο R_0 αντιπροσωπεύει ταλαντωτική κίνηση.

Συνεπώς, ο γεννήτορας R_0 της $O(2,\mathbb{Z}_p)$ μπορεί να θεωρηθεί ως ο ομομορφισμός βηματικής χρονικής εξέλιξης στον φασικό χώρο $\mathbb{T}_N^2$ (2.2) που αντιστοιχεί σε αρμονικό ταλαντωτή π.χ. μέσα σε εξωτερικό μαγνητικό πεδίο[16]. Τον ταλαντωτή αυτόν θα αποκαλούμε «ταλαντωτή BI».

2.2 Ο κβαντικός ταλαντωτής Balian-Itzykson (BI)

2.2.1 Η ομάδα Heisenberg-Weyl

Όπως με κάθε κβαντομηχανικό σύστημα, έτσι και με τον ταλαντωτή BI, η μελέτη της άλγεβρας που το διέπει μας επιτρέπει να εξάγουμε συμπεράσματα για τις ιδιότητές του. Στην προκειμένη περίπτωση, θα εστιαστούμε στην μελέτη της άλγεβρας της επονομαζόμενης ομάδας Heisenberg-Weyl (HW). Η ομάδα αυτή έχει πολλούς διαφορετικούς ισοδύναμους ορισμούς· θα χρησιμοποιήσουμε αυτόν που σχετίζεται με τους συμπλεκτικούς διανυσματικούς χώρους, καθότι είναι ο γενικότερος και άπτεται καλλίτερα στην έως τώρα ανάλυσή μας.

Ορισμός 2.5. Έστω διανυσματικός χώρος $\mathcal{V}$ και μη-εκφυλισμένη αντισυμμετρική διγραμμική μορφή ω. Τότε η πλειάδα $(\mathcal{V}, \omega)$ ονομάζεται *συμπλεκτικός διανυσματικός χώρος*.

Πόρισμα 2.2. *Για μια συγκεκριμένη αναπαράσταση ενός συμπλεκτικού διανυσματικού χώρου, οι ιδιότητες της διγραμμικής μορφής ω του ορισμού 2.5 συνεπάγονται ότι ο πίνακας που την αναπαριστά πρέπει να είναι αντισυμμετρικός και μη-μοναδιαίος.*

Από τα παραπάνω, μπορούμε να κάνουμε την εξής παρατήρηση.

Παρατήρηση 2.1. Αν ένας συμπλεκτικός διανυσματικός χώρος $\mathcal{V}$ είναι πεπερασμένων διαστάσεων, τότε η διάστασή του πρέπει να είναι άρτια.

Αυτό συνεπάγεται άμεσα αφού κάθε αντισυμμετρικός πίνακας έχει μηδενική ορίζουσα αν είναι περιττής διάστασης και ημιθετική αν είναι άρτιας, ενώ κάθε μη-μοναδιαίος πίνακας έχει μη-μηδενική ορίζουσα. Αυτός είναι και ο λόγος που οι συμπλεκτικές ομάδες συμβολίζονται με $Sp(2n)$. Μπορούμε τώρα να προχωρήσουμε στον ορισμό της ομάδας Heisenberg-Weyl [15].

Ορισμός 2.6. Έστω συμπλεκτικός διανυσματικός χώρος $(\mathcal{V}, \omega)$, διάστασης $2n$ και σώμα F. Τότε η ομάδα HW επί του χώρου αυτού ορίζεται ως

$$\mathcal{H}^n(\mathcal{V}) = (V \times F, \circ) : (\mathbf{v}_1, t_1) \circ (\mathbf{v}_2, t_2) = (\mathbf{v}_1 + \mathbf{v}_2, t_1 + t_2 + \frac{1}{2}\omega(\mathbf{v}_1, \mathbf{v}_2)) \quad (2.18)$$

Ως γνωστόν, σε κάθε χώρο Hilbert, όπως ο $\mathcal{V}$, μπορούμε να χρησιμοποιήσουμε την ανάλυση Gram-Schmidt για να βρούμε μια ορθοκανονική βάση [14]. Με μια παραλλαγή της μεθόδου αυτής, εκμεταλλευόμενοι το γεγονός της παρατήρησης 2.1, μπορούμε μια βρούμε μια τέτοια βάση, η οποία χωρίζει τον χώρο $\mathcal{V}$ σε δύο «ίσους» υποχώρους. Τέτοιες βάσεις ονομάζονται *βάσεις Darboux* [20] και είναι της μορφής $(\mathbf{e}_{q_1}, \ldots, \mathbf{e}_{q_n}, \mathbf{e}_{p_1}, \ldots, \mathbf{e}_{p_n})$, όπου

$$\omega(\mathbf{e}_{q_i}, \mathbf{e}_{p_j}) = \delta_{ij} \quad (2.19)$$

εφόσον θέσουμε, ως είθισται,

$$\boldsymbol{\omega} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \quad (2.20)$$

Συνεπώς, για τον διανυσματικό χώρο HW $\mathcal{H}^n$, που προκύπτει από την ομάδα $\mathcal{H}^n(\mathcal{V})$ επί σώματος F θα ισχύει

$$\begin{aligned} \mathcal{H}^n &= < \mathbf{e}_{q_1}, \ldots, \mathbf{e}_{q_n}, \mathbf{e}_{p_1}, \ldots, \mathbf{e}_{p_n}, \mathbf{e}_t > \\ &= < (\mathbf{e}_{q_1}, \ldots, \mathbf{e}_{q_n}) > \oplus < (\mathbf{e}_{p_1}, \ldots, \mathbf{e}_{p_n}) > \oplus < \mathbf{e}_t > \end{aligned} \quad (2.21)$$

άρα ένα τυχαίο διάνυσμα του χώρου θα είναι

$$\mathbf{v} = \sum_i q_i \mathbf{e}_{q_i} + \sum_j p_j \mathbf{e}_{p_j} + t\mathbf{e}_t \quad (2.22)$$

και συνεπώς ο πολλαπλασιαστικός κανόνας της ομάδας γίνεται

$$(\mathbf{q}_1, \mathbf{p}_1, t_1) \circ (\mathbf{q}_2, \mathbf{p}_2, t_2) = (\mathbf{q}_1 + \mathbf{q}_2, \mathbf{p}_1 + \mathbf{p}_2, t_1 + t_2 + \frac{1}{2}(\mathbf{q}_1\mathbf{p}_2 - \mathbf{q}_2\mathbf{p}_1) \quad (2.23)$$

όπου $\mathbf{q}_i, \mathbf{p}_j$ είναι τα διανύσματα $(q_1, \ldots, q_n)_i, (p_1, \ldots, p_n)_j$.

Παρατηρούμε ότι η εξίσωση (2.21) συμπίπτει με αυτήν για τον φασικό χώρο στον ορισμό 2.4, πράγμα που δεν είναι τυχαίο, αφού προφανώς η υποκείμενη πολλαπλότητα της ομάδας HW είναι συμπλεκτική. Αυτό μας οδηγεί στο να αναγνωρίσουμε τα διανύσματα $\mathbf{e}_q$ και $\mathbf{e}_p$ ως μοναδιαία διανύσματα θέσης και ορμής αντίστοιχα, ενώ το $\mathbf{e}_t$ ως μοναδιαίο διάνυσμα χρόνου. Εξάλλου, αφού οι συμπλεκτικές πολλαπλότητες είναι εξ ορισμού διαφορίσιμες, η ομάδα HW είναι μια ομάδα Lie και άρα είναι εφοδιασμένη με μια άλγεβρα Lie $\mathfrak{h}_n$. Από την σχέση (2.18) προκύπτει άμεσα η σχέση μετάθεσης για τα στοιχεία της $\mathcal{H}^n(\mathcal{V})$

$$[(\mathbf{v}_1, t_1), (\mathbf{v}_2, t_2)] = \omega(\mathbf{v}_1, \mathbf{v}_2) \quad (2.24)$$

ή σε συνδυασμό με τις σχέσεις (2.19) και (2.21)

$$\begin{array}{l} [\mathbf{e}_{q_i}, \mathbf{e}_{p_j}] = \delta_{ij} \\ [\mathbf{r}, \mathbf{s}] = 0, \qquad \text{σε κάθε άλλη περίπτωση} \end{array} \tag{2.25}$$

Ας σημειώσουμε ότι από την αντιστοιχία της σχέσης (2.21) με τον ορισμό 2.4 οι αντίστοιχες σχέσεις μετάθεσης για τα στοιχεία της $\mathfrak{h}_n$ θα είναι οι κανονικές σχέσεις μετάθεσης Heisenberg.

Προχωρώντας τώρα στην ανάλυσή μας περί του ταλαντωτή BI, θα ξεκινήσουμε από τις επιτρεπτές καταστάσεις του συστήματος. Αυτές δίδονται από μιγαδικές συναρτήσεις $\psi : \mathcal{S}_p^1 \to \mathbb{C}$ όπως συνεπάγεται από τις εξισώσεις (2.2), (2.15) και (2.16) και άρα σχηματίζουν έναν $p-$διάστατο καταστατικό χώρο, τον διακριτό κύκλο $GF[p]$ [5, 11].

$$|\psi\rangle = \begin{pmatrix} \psi(\theta_0) \\ \psi(\theta_1) \\ \vdots \\ \psi(\theta_{p-1}) \end{pmatrix}, \quad \theta_k = \tfrac{4\pi}{p}k, \quad k = 0, 1, 2, \ldots, p-1 \tag{2.26}$$

Οι σωματιδιακές καταστάσεις

$$|\theta_k\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad k = 0, 1, 2, \ldots, p-1 \tag{2.27}$$

είναι οι ιδιοκαταστάσεις του τελεστή θέσης $\mathbf{Q}$

$$\mathbf{Q} = \frac{4\pi}{p} \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & \ddots & \\ & & & p-1 \end{pmatrix} \tag{2.28}$$

ενώ οι καταστάσεις

$$|k\rangle = \mathbf{F}|\theta_k\rangle = \tfrac{1}{\sqrt{p}} \sum_{j=0}^{p-1} w^{kj} |\theta_j\rangle, \quad k = 0, 1, 2, \ldots, p-1 \tag{2.29}$$

είναι οι ιδιοκαταστάσεις του τελεστή της ορμής $\mathbf{P} = \mathbf{F}\mathbf{Q}\mathbf{F}^{-1}$, όπου

$$F_{jk} = \tfrac{q}{\sqrt{p}} w^{jk}, \quad j, k = 0, 1, 2, \ldots, p, \quad w = e^{2\pi i/p} \tag{2.30}$$

είναι ο μετασχηματισμός Fourier. Αντί των τελεστών θέσης/ορμής $\mathbf{Q}, \mathbf{P}$ θα προτιμήσουμε να δουλέψουμε με τους «ισοδύναμους» τελεστές *μετατόπισης*[5] θέσης/ορμής, που είναι τα εκθετικά των κανονικών τελεστών και οι οποίοι ολισθαίνουν κατά μία θέση την κατάσταση στον αντίστοιχο χώρο. Για τον χώρο της ορμής $\mathbb{Z}_p$, αυτός δίνεται από την σχέση

$$\mathbf{S}_P = e^{i\frac{4\pi}{p}\mathbf{P}} \tag{2.31}$$

[5] shift, translation operators

και δρώντας με αυτόν πάνω στις καταστάσεις (2.29) βρίσκουμε

$$\mathbf{S}_P = \begin{pmatrix} 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \tag{2.32}$$

Αντίστοιχα, ο τελεστής μετατόπισης για τον χώρο θέσης $\mathcal{S}_p^1$

$$\mathbf{S}_Q = e^{\frac{p}{4\pi}\mathbf{Q}} \tag{2.33}$$

βρίσκεται να είναι

$$\mathbf{S}_Q = \begin{pmatrix} 1 & & & \\ & w & & \\ & & \ddots & \\ & & & w^{p-1} \end{pmatrix}, \quad w = e^{2\pi i/p} \tag{2.34}$$

Οι τελεστές $\mathbf{S}_Q, \mathbf{S}_P$ είναι οι γεννήτορες των αβελιανών ομάδων

$$\mathbb{Z}_p^Q = \{S_Q^k | k = 0, 1, \dots, p-1\} \tag{2.35}$$

$$\mathbb{Z}_p^P = \{S_P^k | k = 0, 1, \dots, p-1\} \tag{2.36}$$

και μαζί, ορίζουν μια προβολική αναπαράσταση της αβελιανής ομάδας μετατόπισης[6] του $\mathbb{T}_p^2$ [11]

Οι προβολικές αναπαραστάσεις μιας ομάδας G_0 συνήθως κατασκευάζονται ως ανάγωγες αναπαραστάσεις μιας αβελιανής επέκτασης της G_0 από μια υποομάδα H του κέντρου μια μεγαλύτερης ομάδας G, τέτοια ώστε $G_0 = G/H$ [17]. Στην προκειμένη περίπτωση, η μεγαλύτερη αυτή ομάδα είναι η ομάδα HW

$$\mathcal{H}^1(\mathbb{T}_p^2) = (\mathbb{T}_p^2 \times \mathbb{Z}_p, \circ) \tag{2.37}$$

με κέντρο το

$$T_1 = \{(0, 0, n) | n \in \mathbb{Z}_p\} \tag{2.38}$$

Με την κατάλληλη επιλογή της μορφής ω, ο πολλαπλασιαστικός της κανόνας γίνεται

$$(q_1, p_1, t_1) \circ (q_2, p_2, t_2) = (q_1 + q_2, p_1 + p_2, t_1 + t_2 + q_1 p_2 - q_2 p_1) \tag{2.39}$$

Παρατηρούμε ότι

$$e^{ia\mathbf{x}} e^{ib\mathbf{p}} = e^{-iab\hbar} e^{ia\mathbf{p}} e^{ib\mathbf{x}} \tag{2.40}$$

που είναι η εκθετική μορφή των κανονικών σχέσεων μετάθεσης για την θέση και την ορμή και άρα, από τις σχέσεις (2.31) και (2.33), οι κανονικές σχέσεις μετάθεσης Heisenberg, μπορούν να γραφτούν συναρτήσει των $\mathbf{S}_Q$ και $\mathbf{S}_P$ ως

$$\mathbf{S}_Q \mathbf{S}_P = w \mathbf{S}_P \mathbf{S}_Q \tag{2.41}$$

Η τιμή της σταθεράς του Plank τότε θα είναι $\hbar = 2\pi/N$, αφού διαλέξαμε $ab = 1$ στους ορισμούς των τελεστών. Η σχέση (2.41) ορίζει τις λεγόμενες *κανονικές σχέσεις μετάθεσης Heisenberg-Weyl* [12]. Θα χρειαστούμε τώρα το εξής θεώρημα

[6] translation group

Θεώρημα 2.2. (Stone-von Neumann) *Υπάρχει μία μόνο μοναδιαία αναπαράσταση της ομάδας $\mathcal{H}(\mathcal{V}\times F)$ έως ισομορφισμού, για μια συγκεκριμένη επιλογή τιμής του κέντρου της.*

Παρατήρηση 2.2. Από φυσική σκοπιά, η τιμή του κέντρου της ομάδας HW αντιστοιχεί στην τιμή της σταθεράς του Plank $\hbar$.

Άμεση συνέπεια του θεωρήματος Stone-von Neumann είναι το εξής

Πόρισμα 2.3. *Οι γεννήτορες της μοναδιαίας αναπαράστασης της ομάδας $\mathcal{H}(\mathcal{V}\times F)$ ταυτίζονται με τους τελεστές θέσης και ορμής στον χώρο $\mathcal{V}$*

Παρατηρούμε τώρα ότι οι πίνακες $\mathbf{S}_Q$ και $\mathbf{S}_P$ είναι γεννήτορες της άλγεβρας Lie $\mathfrak{su}(p)$ της ομάδας $SU(p)$ [11, 10], η οποία είναι μοναδιαία. Συνδυάζοντας το γεγονός αυτό με το ότι οι τελεστές μετατόπισης θέσης/ορμής είναι ισοδύναμοι με τους συνήθεις αντίστοιχους τελεστές, από το θεώρημα 2.2, το πόρισμα 2.3 και την παρατήρηση 2.2, έχοντας υπ' όψιν ότι έχουμε διαλέξει τιμή για την σταθερά του Plank, καταλήγουμε στο συμπέρασμα ότι η $\mathfrak{su}(p)$ είναι ισόμορφη με την άλγεβρα Lie $\mathfrak{h}_1$ της $\mathcal{H}^1(\mathbb{T}_p^2)$. Εξάλλου, το γινόμενο δύο γεννητόρων μιας άλγεβρας είναι επίσης γεννήτορας και συνεπώς, για την αναπαράσταση που έχει σαν βάση τους πίνακες $\mathbf{S}_Q, \mathbf{S}_P$, το γενικό στοιχείο-πίνακας της $\mathcal{H}^1(\mathbb{T}_p^2)$ θα δίνεται από την σχέση

$$\mathbf{g}_{t,r,s,t} = w^t \mathbf{J}_{r,s} \quad t,r,s = 0,1,2,\ldots,p-1 \tag{2.42}$$

όπου $\mathbf{J}_{r,s} = w^{rs/2}\mathbf{S}_Q^r\mathbf{S}_P^t$ και τα w^t είναι τα εκθετικά των σταθερών δομής f_{trs} της $\mathfrak{h}_1$ [14]. Τέλος, η σχέση (2.41) συνεπάγεται ότι οι γεννήτορες $\mathbf{J}_{r,s}$ είναι κλειστοί για τον πολλαπλασιασμό

$$\mathbf{J}_{r,s}\mathbf{J}_{r',s'} = w^{(r's-rs')/2}\mathbf{J}_{r+r',s+s'} \tag{2.43}$$

2.2.2 Ο DFrFT στην μεταπλεκτική αναπαράσταση

Σε μία διάσημη δημοσίευσή του, ο Weil όρισε την επονομαζόμενη *μεταπλεκτική ομάδα* [30]

Ορισμός 2.7. Μεταπλεκτική ομάδα $Mp(2n)$ ονομάζεται το διπλό κάλυμμα [7] της συμπλεκτικής ομάδας $Sp(2n)$.

Εν γένει, η μεταπλεκτική ομάδα δεν επιδέχεται πιστής αναπαραστάσεως από πεπερασμένους πίνακες. Ο Weil, όμως, απέδειξε ότι στην περίπτωση που η συμπλεκτική ομάδα ορίζεται υπό χώρο που είναι ευθύ άθροισμα χώρων πεπερασμένων σωμάτων, υπάρχει πιστή αναπαράσταση από πεπερασμένους πίνακες στον χώρο αυτό. Τότε, η μεταπλεκτική αναπαράσταση ορίζεται να είναι οι πίνακες ομοιότητας ενός συγκεκριμένου *συμπλεκτικού μετασχηματισμού* - ενός συμπλεκτομορφισμού από και προς τον ίδιο χώρο - των γεννητόρων $\mathbf{J}_{r,s}$ του χώρου HW. Συνεπώς, από την σχέση (2.21) συμπεραίνουμε ότι υπάρχει πιστή μεταπλεκτική αναπαράσταση της ομάδας $\mathcal{H}^1(\mathbb{T}_p^2)$· αυτή ορίζεται από την σχέση [3, 30]

$$\mathbf{U}^{-1}(A)\mathbf{J}_{r,s}\mathbf{U}(A) = \mathbf{J}_{r',s'}, \quad (r',s') = (r,s)A \quad \forall A \in Sp(2,\mathbb{Z}_p) \tag{2.44}$$

[7] double cover

Οι Balian και Itzykson, στην εργασία τους [5] δίνουν μία ρητή μορφή για την αναπαράσταση (2.44) [16, 13, 27]

$$\mathbf{U}(A) = \frac{\sigma(1)\sigma(\delta)}{p} \sum_{r,s=0}^{p-1} w^{[br^2+(d-a)rs-cs^2]/2\delta} \mathbf{J}_{r,s} \tag{2.45}$$

όπου $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\delta = 2-a-d$ και

$$\sigma(a) = \frac{1}{\sqrt{p}} \sum_{p-1}^{r,s=0} w^{ar^2} = (a|p) \begin{cases} 1, & p = 4k+1 \\ i, & p = 4k-1 \end{cases} \tag{2.46}$$

είναι το άθροισμα Gauss [2, 28], ενώ το $(a|p)$ είναι το σύμβολο Jacobi [2] και ισούται με ± 1 ανάλογα με το αν το a είναι ή όχι τετράγωνο ενός ακεραίου modulo p αντίστοιχα.

Η αναπαράσταση (2.45) είναι έγκυρη όταν $\delta \neq 0$, ενώ για $\delta = 0$ έχουμε τις εξής υποπεριπτώσεις

- $b \neq 0$

$$\mathbf{U}(A) = \frac{\sigma(-2b)}{\sqrt{p}} \sum_{r=0}^{p-1} w^{r^2/2b} \mathbf{J}_{r(a-1)/b,r} \tag{2.47}$$

- $b = 0, c \neq 0$

$$\mathbf{U}(A) = \frac{\sigma(-2c)}{\sqrt{p}} \sum_{r=0}^{p-1} w^{-r^2/2c} \mathbf{S}_P^r \tag{2.48}$$

- $A \equiv \mathbf{I}$

$$\mathbf{U}(A) = \mathbf{I}_{p\times p} \tag{2.49}$$

Παρατηρούμε τώρα, ότι υπό την μεταπλεκτική αναπαράσταση, ο γεννήτορας g_3 της $Sp(2,\mathbb{Z}_p)$ (εξ. 2.6) είναι ο μετασχηματισμός Fourier [3]

$$\mathbf{U}(g_3) = \mathbf{U} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (-1)^{k+1} i^n \mathbf{F} \tag{2.50}$$

όπου $n = 0$ ή 1 ανάλογα με το αν $p = 4k \pm 1$ αντίστοιχα. Από την σχέση (2.7) για την κυκλική ομάδα $O(2,\mathbb{Z}_p)$, βλέπουμε ότι το g_3 είναι στοιχείο της ομάδας, άρα θα ισούται με κάποια δύναμη του θεμελιακού στοιχείου της R_0. Με άλλα λόγια, κάποια δύναμη του R_0 θα ισούται με τον μετασχηματισμό Fourier στην μεταπλεκτική αναπαράσταση. Οι Balian και Itzykson έδειξαν ότι η δύναμη αυτή είναι η k-οστή, συνεπώς θέτοντας $\mathbf{G} := \mathbf{U}(R_0)$, θα έχουμε [5]

$$\mathbf{F} = i^n (-\mathbf{G})^k \tag{2.51}$$

όπου πάλι $n = 0$ ή 1 ανάλογα με το αν $p = 4k \pm 1$ αντίστοιχα.

Για να υπολογίσουμε την n-οστή δύναμη του πίνακα $\mathbf{G}$, $\mathbf{G}^n = \mathbf{U}(R_0^n)$, πρέπει πρώτα να βρούμε τον 2×2 πίνακα $\mathbf{R}_0^n$ modulo p

$$\mathbf{R}_0^n = \begin{pmatrix} a_0 & b_0 \\ -b_0 & a_0 \end{pmatrix}^n = \begin{pmatrix} a_{n-1} & b_{n-1} \\ -b_{n-1} & a_{n-1} \end{pmatrix}, \quad n = 1, 2, \ldots, 4k-1,$$
$$\mathbf{R}_0^0 = \mathbf{I} = \begin{pmatrix} a_{-1} & b_{-1} \\ -b_{-1} & a_{-1} \end{pmatrix} \tag{2.52}$$

και μετά, εκμεταλλευόμενοι το γεγονός ότι από τον ορισμό των $\mathbf{J}_{r,s}$ ισχύει [3]

$$(J_{r,s})_{k,l} = \delta_{k-r,l} w^{(k+l)s/2} \tag{2.53}$$

να κάνουμε επανειλημμένη χρήση του αθροίσματος Gauss (εξ. 2.46)

$$U_{k,l}(A) = \frac{q}{\sqrt{p}}(-2c|p) \left\{ \begin{array}{c} 1 \\ -i \end{array} \right\} w^{(ak^2+dl^2-2kl)/2c} \tag{2.54}$$

όπου η αγκύλη διαχωρίζει τις περιπτώσεις $p = 4k \pm 1$. Όταν $p = 4k+1$, ο ομομορφισμός βαθμίδας (εξ. 2.45) είναι

$$\mathbf{U}(g_2)_{k,l} = \sigma(1)\sigma(\delta)\delta_{k,gl} \tag{2.55}$$

όπου $\delta = 2 - g - g^{-1}$ και g θεμελιακό στοιχείο της $GF^*[p]$, ενώ για $p = 4k-1$, που είναι η περίπτωση που μας ενδιαφέρει, ο πίνακας $\mathbf{G}$ μπορεί να γραφεί σε κλειστή μορφή η οποία δίνεται από την σχέση [3]

$$G_{k,l} = \frac{1}{\sqrt{p}} i(2b_0|p) w^{(a_0k^2+a_0l^2-2kl)/2b_0} \tag{2.56}$$

όπου τα a_0, b_0 είναι τα στοιχεία του R_0 (εξ. 2.12).

Η διαδικασία που παρουσιάσαμε αναλυτικά στις δύο παραπάνω υποπαραγράφους είναι η επονομαζόμενη κβάντωση Weyl [16] και μέσω αυτής έχουμε κατασκευάσει το κατάλληλο μαθηματικό υπόβαθρο για να υπολογίζουμε όλες τις δυνάμεις του πίνακα $\mathbf{G}$ για ακέραιες τιμές από 0 έως και k. Όμως, αφού όπως είπαμε ο πίνακας $\mathbf{G}^k$ είναι ο μετασχηματισμός Fourier, τότε οι μικρότερες δυνάμεις του πίνακα θα είναι οι n-οστές ρίζες του μετασχηματισμού στο διακριτό διάστημα $[0, k]$, ή αλλιώς, κλασματικές δυνάμεις του μετασχηματισμού Fourier. Αυτός είναι και ο ορισμός που δώσαμε στο Κεφ.1 για τον FrFT. Είμαστε δηλαδή σε θέση να υπολογίσουμε *επακριβώς* τον DFrFT $\mathbf{F}_a$ για ένα συγκεκριμένο εύρος της διακριτής παραμέτρου a, εκμεταλλευόμενοι τον τελεστή στροφής $\mathbf{R_0}$ (εξ. 2.17) της ομάδας SO_2 υπό την μεταπλεκτική αναπαράσταση της ομάδας HW ενός κβαντικού συστήματος με την άλγεβρα του ταλαντωτή BI.

Ο ορισμός του DFrFT μέσω της κβάντωσης Weyl του ταλαντωτή BI φαίνεται αμέσως ότι έχει όλες τις καλές ιδιότητες που θέλαμε, χωρίς να καταφεύγουμε σε διακριτές προσεγγίσεις. Επίσης, δεν πάσχει από τον εκφυλισμό των ιδιοτιμών που κληρονομεί από τον συνήθη μετασχηματισμό Fourier ο ορισμός που παρουσιάσαμε στο πρώτο κεφάλαιο, καθώς όλες οι πράξεις γίνονται modulo p. Αυτό το τελευταίο έχει σαν αποτέλεσμα η δράση του μετασχηματισμού να εμφανίζει μια φαινομενική τυχαιότητα και συνεπώς μοιράζεται αρκετά στοιχεία με άλλους μετασχηματισμούς όπως ο *DRFNT* [32] και ο χαοτικός *Arnold cat map* [16, 18], οι οποίοι βρίσκουν εφαρμογές μεταξύ άλλων στην κρυπτογραφία και την στεγανογραφία.

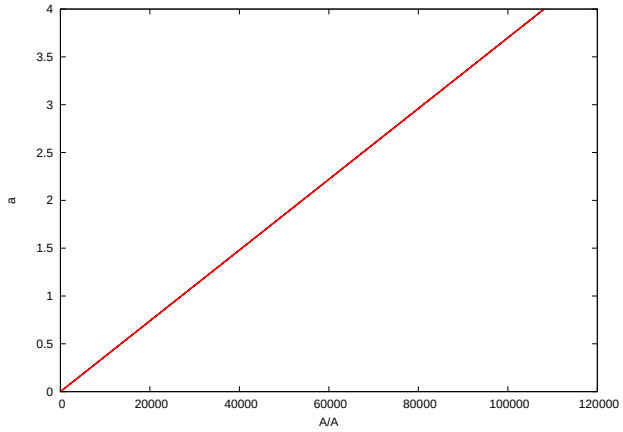
Από την άλλη, ο ορισμός αυτός έχει και ένα μειονέκτημα, το οποίο έγκειται στον περιορισμό των τιμών της παραμέτρου a, λόγω της σχέσης $p = 4k-1$. Για την καλλίτερη μελέτη των δυνατών τιμών της παραμέτρου a, μπορούμε να ορίσουμε το εξής σύνολο

Ορισμός 2.8. Ορίζουμε ως *κλάσματα Fourier* το σύνολο

$$\mathbb{Q}_F = \left\{ (n,k) \middle| \forall k \forall n \left((k \in \mathbb{Z}) \wedge (n \in \mathbb{Z}) \wedge \left(k = \frac{p+1}{4} \right) \wedge (\text{Prime}(p)) \right) \right\} \tag{2.57}$$

Παρατηρούμε ότι το σύνολο $\mathbb{Q}_F$ είναι αναδρομικά απαριθμητό και γνήσιο υποσύνολο των ρητών

$$\mathbb{Q}_F \subsetneq \mathbb{Q} \tag{2.58}$$

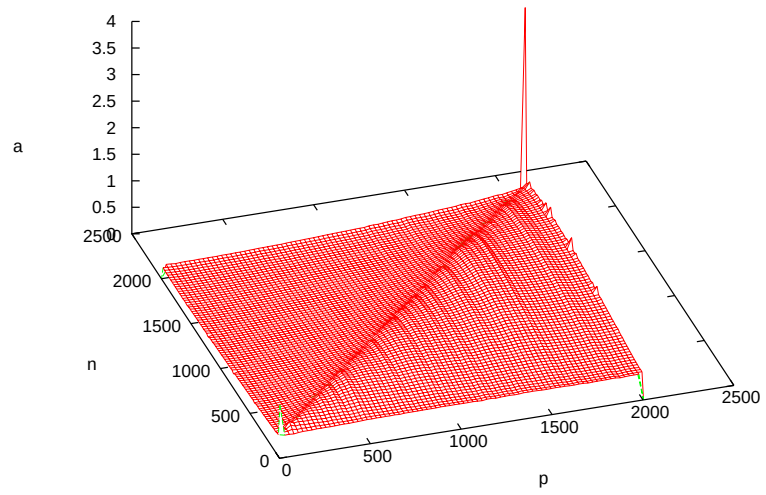


Σχ. 2.3: Κατανομή δυνατών τιμών ανά αύξοντα αριθμό για την παράμετρο a του DFrFT, για τους πρώτους αριθμούς $3 \leq p \leq 2003$, $p = 4k - 1$.

Στο παράρτημα, παραθέτουμε κώδικα `PL/pgSQL` για τον υπολογισμό κλασμάτων Fourier στον περιορισμό[8] $n \in \mathbb{Z}_{4k}$ με την χρήση της βάσης δεδομένων `PostgreSQL`. Στο πνεύμα του πίνακα 1 της αναφοράς [3], των θεμελιακών στοιχείων των ομάδων $GF^*[p]$, $O(2, \mathbb{Z}_p)$ και $GF[p^2]$, για τους πρώτους αριθμούς από το 3 έως το 2003, υπολογίστηκαν τα κλάσματα Fourier για τους πρώτους αυτούς. Είναι 108.104 διακεκριμένοι αριθμοί στο πλήθος, αρχίζοντας από την ελάχιστη τιμή $0,00199601$ μέχρι την μέγιστη $3,998$ σε δεκαδική αναπαράσταση (της προφανούς τιμής 4 εξαιρουμένης). Παρουσιάζουν γραμμική κατανομή όπως φαίνεται στο διάγραμμα του σχ. 2.3. Στο σχ. 2.4 βλέπουμε μια προσαρμογή της κατανομής σε διακριτό πλέγμα για όλα τα ζεύγη (p, n), με το a κανονικοποιημένο στο μηδέν για όσα ζεύγη δεν ορίζεται. Η γραμμική κατανομή του σχ. 2.3 διακρίνεται στην κορυφογραμμή του διαγράμματος, ενώ οι πλαγιές αποτελούν μέτρο της πολλαπλότητας κάθε τιμής του a. Δυστυχώς, η σχέση (2.58) συνεπάγεται ότι το σύνολο $\mathbb{Q}_F$ δεν είναι πυκνό στο $\mathbb{R}$. Πάρα ταύτα, είναι προφανές από τα παραπάνω σχήματα, ότι όσο μεγαλύτερο p διαλέξουμε, τόσο καλλίτερα μπορούμε να προσεγγίσουμε μια τυχαία τιμή του $a \in \mathbb{R}$.

Όσον αφορά τώρα στην πολυπλοκότητα υπολογισμού του μετασχηματισμού από τον ορισμό, παρατηρούμε ότι ο υπολογισμός του αθροίσματος Gauss $\sigma(a)$ ανάγεται ουσιαστικά στον υπολογισμό του συμβόλου Jacobi $(a|p)$, που έχει πολυπλοκότητα χρόνου $O(\log a \log N)$ [9] και χρειάζεται να γίνει άπαξ για συγκεκριμένο $\mathbf{R}_0$. Από την άλλη, ο υπολογισμός της n-οστής δύναμης του πίνακα $\mathbf{R}$ παίρνει $O(8n) = O(1)$ βήματα και για τον πίνακα $\mathbf{G}^n = \mathbf{U}(R_0^n)$ θέλουμε

[8] Η περίοδος του μετασχηματισμού Fourier είναι 4, συνεπώς αριθμοί $\frac{n}{k}$ για $n > 4k$ είναι πλεονάζοντες



Σχ. 2.4: Τρισδιάστατη αναπαράσταση της κατανομής των δυνατών τιμών για την παράμετρο a του DFrFT, για τους πρώτους αριθμούς $3 \leq p \leq 2003$, $p = 4k - 1$.

$O(N^2)$ βήματα, από την σχέση (2.45). Αυτό σημαίνει, ότι μπορούμε να υπολογίσουμε επακριβώς τον πίνακα του DFrFT $\mathcal{F}_a$, $a \in \{\frac{n}{k} | n = 1, 2, 3, \ldots\}$ σε χρόνο $O(N^2 + \log a \log N) = O(N^2)$. Ο χρόνος αυτός είναι ο ίδιος με αυτόν που χρειάζεται και ο DFT όταν περιοριστούμε στον ορισμό του και δεν χρησιμοποιήσουμε άλλους αλγορίθμους όπως ο FFT. Στο κεφάλαιο που ακολουθεί, θα επιχειρήσουμε να παρουσιάσουμε ένα κβαντικό αλγόριθμο για τον υπολογισμό του DFrFT, με την ελπίδα να επιταχύνουμε την επίλυσή του, με τρόπο παρόμοιο με αυτόν που γίνεται στην περίπτωση του DFT με την χρήση του αλγορίθμου QFT.

3 Ο κβαντικός FrFT

Στο κεφάλαιο αυτό κάνουμε μια σύντομη εισαγωγή στην έννοια της κβαντικής υπολογιστικής και παρουσιάζουμε τα δομικά στοιχεία των κβαντικών υπολογιστών. Θα δούμε τι χρειαζόμαστε για να κάνουμε πράξεις σε έναν τέτοιον υπολογιστή και το τι είδους πράξεις μπορούμε να κάνουμε. Κατόπιν, παρουσιάζουμε τον αλγόριθμο QFT, έναν αλγόριθμο που υπολογίζει τον κβαντικό μετασχηματισμό Fourier τουλάχιστον εκθετικά πιο γρήγορα απ'ότι οποιοσδήποτε γνωστός κλασσικός αλγόριθμος και θα δείξουμε πώς αυτός μπορεί να προσαρμοστεί στην περίπτωση του DFrFT, όπως αυτός ορίστηκε στο κεφ. 2.

3.1 Περί κβαντικών υπολογιστών

Η κβαντική υπολογιστική είναι η επιστήμη που μελετά τις υπολογιστικές διαδικασίες που μπορούν να επιτευχθούν με την χρήση κβαντομηχανικών συστημάτων. Σαν ιδέα ακούγεται απλή, αλλά χρειάστηκαν να περάσουν αρκετές δεκαετίες από την δημιουργία της κβαντομηχανικής περί το 1920, μέχρι να μελετηθεί επιμελώς και να εδραιωθεί ως κλάδος. Ο λόγος είναι ότι η ίδια η κβαντομηχανική, που είναι ένας μαθηματικός φορμαλισμός, ένα «πλαίσιο» για την δημιουργία φυσικών θεωριών, όπως η κβαντική ηλεκτροδυναμική (QED) και η κβαντική χρωμοδυναμική (QCD), έχει ένα μικρό πλήθος από απλούς κανόνες, αλλά η συνέπειες των κανόνων αυτών φαίνονται εγγενώς αντιδιαισθητικές για την ανθρώπινη αντίληψη και οδηγούν στη περιγραφή φυσικών φαινομένων που μοιάζουν «παράδοξα» μεν, αλλά έχουν επιβεβαιωθεί πειραματικά. Από την άλλη, αυτός ο λόγος ήταν και το ίδιο το κίνητρο πίσω από την ανάπτυξη της επιστήμης αυτής· η ελπίδα ότι τα παράδοξα της κβαντομηχανικής μπορεί να μας επιτρέψουν να κάνουμε πράγματα που δεν θα ήταν δυνατά χωρίς τον έλεγχο της φύσης σε αυτό το επίπεδο.

Για να το καταλάβουμε καλλίτερα αυτό, θα πρέπει να το δούμε υπό το φως των αρχών της πληροφορικής, η οποία γεννήθηκε σαν επιστήμη την ίδια περίπου εποχή. Στην περίφημη δημοσίευσή του του 1936 [29], ο Turing ορίζει την λεγόμενη *μηχανή Turing* ως αφηρημένο πρότυπο υπολογιστικό μοντέλο, και αποδεικνύει ότι υπάρχει μια τέτοια μηχανή, η *καθολική μηχανή Turing*, η οποία είναι ικανή να προσομοιώσει οποιαδήποτε άλλη μηχανή Turing. Περαιτέρω, ισχυρίζεται ότι η καθολική μηχανή Turing συλλαμβάνει πλήρως την έννοια του αλγορίθμου, κάτι που έγινε ευρύτερα γνωστό ως θέση *Church-Turing*

> *Οποιαδήποτε αλγοριθμική διαδικασία μπορεί να προσομοιωθεί από μια μηχανή Turing*

Οι βάσεις που έθεσε ο Turing έγιναν η αιτία της παροιμιώδους ανάπτυξης της πληροφορικής και της ανάδυσης κλάδων όπως η *υπολογιστική πολυπλοκότητα*, η οποία μελετά την αποδοτικότητα των αλγορίθμων.

Στα πλαίσια της υπολογιστικής πολυπλοκότητας, λέμε ότι ένας δεδομένος αλγόριθμος είναι *αποδοτικός*, όταν μπορεί να υλοποιηθεί σε χρόνο πολυωνυμικό στο μήκος της εισόδου του. Αντιθέτως, λέμε ότι δεν είναι αποδοτικός όταν χρειάζεται υπέρ του πολυωνυμικού χρόνο, εννοώντας συνήθως εκθετικό. Ο λόγος για την διάκριση αυτή είναι ο *νόμος του Moore*, ο οποίος λέει ότι δεδομένης της παρατηρηθείσας τεχνολογικής ανάπτυξης, η ισχύς των υπολογιστών θα αυξάνεται γραμμικά με τον χρόνο, πράγμα που σημαίνει ότι διαφορές απόδοσης αλγορίθμων μέχρι και σε βαθμό πολυωνυμικής πολυπλοκότητας τείνουν να γίνουν αμελητέες με τον χρόνο.

Εκτός από το μοντέλο των μηχανών Turing, τις επερχόμενες δεκαετίες εφευρέθηκαν και άλλα υπολογιστικά μοντέλα, ακόμα και πιθανοκρατικά, στην προσπάθεια εύρεσης ενός μοντέλου το οποίο θα μπορεί να υπολογίζει αποδοτικά αλγορίθμους που μέχρι στιγμής φαινόταν να μην έχουν πολυωνυμική υλοποίηση. Παρ' όλες της προσπάθειες, όλα τα μοντέλα αυτά αποδείχθηκαν ότι μπορούν να προσομοιωθούν αποδοτικά από την καθολική μηχανή Turing, όταν εφαρμοστούν ρεαλιστικά όρια στην υλοποίησή τους. Παράδειγμα αποτελούν οι αναλογικοί υπολογιστές, οι οποίοι ενώ θεωρητικά υπόσχονταν να ξεπεράσουν την ισχύς των μηχανών Turing, όταν τους επιβληθούν οι ρεαλιστικοί περιορισμοί της διόρθωσης λαθών και του θορύβου, αποτυγχάνουν να αντεπεξέλθουν στην πρόκληση. Αυτό είχε σαν αποτέλεσμα να διατυπωθεί μια παραλλαγή της θέσης Church-Turing, η λεγόμενη *ισχυρή* θέση Churh-Turing

> *Οποιαδήποτε αλγοριθμική διαδικασία μπορεί να προσομοιωθεί αποδοτικά από μια πιθανοκρατική μηχανή Turing*

Επιστρέφοντας στους κβαντικούς υπολογιστές, ο λόγος που μελετούνται ξεχωριστά σαν κλάδος και οποίος έχει επιζήσει εν αντιθέσει με τα υπόλοιπα εναλλακτικά μοντέλα, είναι ότι φαίνεται να είναι το μοναδικό μέχρι στιγμής μοντέλο που παραβιάζει την ισχυρή εκδοχή της θέσης αυτής, ακόμα και με τον περιορισμό των ρεαλιστικών ορίων υλοποίησης. Όπως θα δούμε στην παράγραφο 3.3, έχουν ανακαλυφθεί κβαντικοί αλγόριθμοι που επιλύουν αποδοτικά προβλήματα τα οποία δεν έχουν γνωστή αποδοτική υλοποίηση σε μηχανές Turing και που πιστεύεται πως κατά το μάλλον ούτε έχουν. Το αν πράγματι ισχύει αυτό, το ότι οι κβαντικοί υπολογιστές είναι ένα ισχυρότερο υπολογιστικό μοντέλο από τις μηχανές Turing, είναι ακόμα ένα ανοικτό πρόβλημα, καθώς δεν είναι γνωστό ακόμα ούτε αν μπορούν να υπολογίσουν μια μεγαλύτερη κλάση συναρτήσεων από αυτές που υπολογίζουν οι μηχανές Turing - τις λεγόμενες μερικές αναδρομικές συναρτήσεις [34] - αλλά ούτε και αν η κλάση **BQP**[9] - το κβαντικό αντίστοιχο της **BPP** - περικλείει μέρος από ή όλη την κλάση **NP**.

3.2 Στοιχεία κβαντικής υπολογιστικής

Το *bit* είναι η θεμέλια έννοια της κλασσικής υπολογιστικής· είναι το κβάντο της πληροφορίας, η μικρότερη δυνατή ποσότητα πληροφορίας, το οποίο μπορεί να πάρει μία από τις τιμές μηδέν (0) ή ένα (1). Το ανάλογο του bit στην κβαντική υπολογιστική είναι το λεγόμενο *qubit* ή *q-bit*.

Εν αντιθέσει όμως με το κλασσικό bit, το qubit μπορεί να πάρει περισσότερες τιμές· για την ακρίβεια, μπορεί να πάρει οποιαδήποτε τιμή στο συνεχές διάστημα $[0, 1]$. Η ιδιότητα αυτή δεν είναι τελείως ξένη. Το ίδιο συμβαίνει και με τις αποτιμήσεις αληθείας στην *ασαφή λογική*[10]. Αυτό που κάνει δυνατή μια τέτοια θεώρηση του κβάντου της πληροφορίας στα πλαίσια της κβαντικής υπολογιστικής από πλευράς υλοποίησης, είναι μία από τις βασικές αρχές της κβαντομηχανικής, η λεγόμενη *αρχή της επαλληλίας ή υπέρθεσης*. Σύμφωνα με την αρχή αυτή, ένα κβαντομηχανικό σύστημα που χαρακτηρίζεται από n ιδιοκαταστάσεις - καταστάσεις που μπορούν να παρατηρηθούν από ένα πείραμα - μπορεί να υπάρχει σε οποιονδήποτε γραμμικό συνδυασμό των ιδιοκαταστάσεων αυτών. Έτσι, αν

[9] Πιο συγκεκριμένα, **BQP** σημαίνει *Bounded error, Quantum, Polynomial time* και περιλαμβάνει τις γλώσσες που αποφασίζονται σε πολυωνυμικό χρόνο με φραγμένη πιθανότητα λάθους, από κβαντικούς υπολογιστές

[10] fuzzy logic

συμβολίσουμε με $|0\rangle$ μια ιδιοκατάσταση του συστήματος και $|1\rangle$ μία άλλη, τότε το σύστημα την χρονική στιγμή t μπορεί να βρίσκεται σε οποιαδήποτε από τις καταστάσεις υπέρθεσης

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad \text{όπου } |a|^2 + |b|^2 = 1, \quad a, b \in \mathbb{C} \tag{3.1}$$

Στην γενικότερή της μορφή, η αρχή αυτή εκφράζεται από τη σχέση

$$|\psi\rangle = \sum_{i=0}^{n-1} c_i|\psi_i\rangle, \quad \sum_{i=0}^{n-1} |c_i|^2 = 1 \tag{3.2}$$

Αμέσως μπορεί κανείς να κάνει της αντιστοιχία ότι οι ιδιοκαταστάσεις $|0\rangle$ και $|1\rangle$ ενός qubit είναι τα ανάλογα των καταστάσεων 0 και 1 ενός κλασσικού bit. Αυτό που διαφοροποιεί λοιπόν τα qubits από τα bits είναι το συνεχές των υπολοίπων γραμμικών συνδυασμών των «βασικών» καταστάσεων, που είναι επίσης επιτρεπτοί. Από μαθηματική σκοπιά, το qubit μπορεί να ορισθεί ως ένα μοναδιαίο διάνυσμα σε έναν δισδιάστατο διανυσματικό χώρο επί του σώματος των μιγαδικών αριθμών. Εξάλλου, επειδή $|a|^2 + |b|^2 = 1$, η σχέση (3.1) μπορεί να ξαναγραφεί ως

$$|\psi\rangle = e^{i\gamma}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle\right), \quad \theta, \varphi, \gamma \in \mathbb{R} \tag{3.3}$$

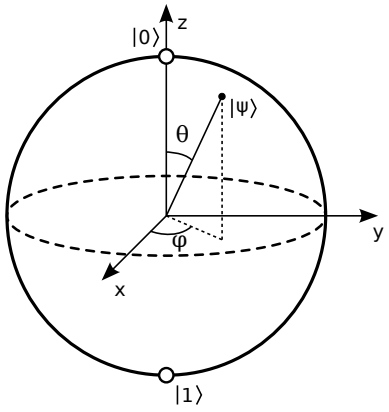
και επειδή ο ολικός παράγοντας φάσης $e^{i\gamma}$ δεν έχει παρατηρήσιμη φυσική σημασία μπορεί να αγνοηθεί και γράψουμε τελικά

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{3.4}$$

Οι αριθμοί θ, φ ορίζουν ένα σημείο στην επιφάνεια της τρισδιάστατης μοναδιαίας σφαίρας, η οποία συχνά καλείται *σφαίρα του Bloch* (σχ. 3.1). Η γεωμετρική αναπαράσταση αυτή, είναι ένα χρήσιμο βοήθημα οπτικοποίησης και κατανόησης του qubit, αλλά θα πρέπει κανείς να θυμάται ότι δεν υπάρχει κάποιο γεωμετρικό αντίστοιχο στις τρεις διαστάσεις για πολλαπλά qubit.

Ένα σημείο κοινής παρανόησης αφορά στην ποσότητα της πληροφορίας που περιέχει ένα qubit. Επειδή υπάρχουν άπειρα σημεία στην επιφάνεια μιας σφαίρας, θα μπορούσε κανείς να πει ότι ένα και μοναδικό qubit περιέχει άπειρη πληροφορία, που μπορεί να αναπαρασταθεί κλασσικά από μια άπειρη δυαδική αναπαράσταση των παραμέτρων θ, φ. Κάτι τέτοιο, όμως, δεν συμβαίνει στην πραγματικότητα· επειδή όπως σε κάθε κβαντομηχανικό σύστημα, μόνο οι ιδιοκαταστάσεις του μπορούν να παρατηρηθούν, όπως επιβάλει η *αρχή της κατάρρευσης της κυματοσυνάρτησης*, οποιαδήποτε «πλεονάζουσα» πληροφορία περιέχει ένα qubit, καταστρέφεται την στιγμή της μέτρησης και καταλήγουμε με μία από τις ιδιοκαταστάσεις $|0\rangle$ ή $|1\rangle$, με πιθανότητα $|a|^2$ ή $|b|^2$ αντίστοιχα. Αυτό, όμως, δεν σημαίνει ότι καταλήγουμε εν τέλει εκεί που θα καταλήγαμε με την χρήση ενός κλασσικού bit. Εφ' όσον δεν πραγματοποιούμε καμμία μέτρηση σε ένα qubit, αυτό παραμένει σε κατάσταση υπέρθεσης και η φύση διατηρεί και χειρίζεται την «κρυμμένη» πληροφορία που αυτό περιέχει· το γεγονός αυτό μπορούμε να το εκμεταλλευτούμε, για να κάνουμε πράξεις με κβαντικές πύλες - όπως κάνουμε με τις κλασσικές πύλες στα bit - οι οποίες γίνονται τρόπο τινά εν παραλλήλω. Επί παραδείγματι, μπορούμε να κάνουμε την πράξη της πρόσθεσης δύο qubit με την κατάλληλη πύλη και για τους τέσσερεις συνδυασμούς των τιμών 0 και 1 σε ένα μόνο βήμα, αντί για τέσσερα που θα χρειαζόμασταν σε έναν κλασσικό υπολογιστή, αν τα qubit

μας είναι προετοιμασμένα σε κατάσταση υπέρθεσης. Την ώρα της μέτρησης, θα πάρουμε μόνο μία από τις τέσσερεις δυνατές τιμές αποτελέσματος, με πιθανότητα αντίστοιχη των συντελεστών πλάτους του τελικού qubit, αλλά σε πολύπλοκα κυκλώματα, αυτή η «συντόμευση» μπορεί να οδηγήσει σε πραγματικό κέρδος. Θα το δούμε αυτό στην πράξη, στην παράγραφο 3.3, με τον αλγόριθμο QFT, που υπολογίζει τον κβαντικό μετασχηματισμό Fourier. Πριν από αυτό όμως, θα δούμε τι είδους πύλες μπορούμε να χρησιμοποιήσουμε στους κβαντικούς υπολογιστές για να κάνουμε πράξεις.



Σχ. 3.1: Αναπαράσταση ενός qubit στην σφαίρα Bloch

3.2.1 Πύλες ενός qubit

Ως γνωστόν, στην περίπτωση των κλασσικών υπολογιστών υπάρχει μόνο μία μη-τετριμμένη πύλη ενός bit· η πύλη NOT, η οποία μετατρέπει το 0 σε 1 και αντίστροφα. Για να κατασκευάσουμε το κβαντικό αντίστοιχο της πύλης αυτής, θα πρέπει να βρούμε έναν μετασχηματισμό που να φέρνει την κατάσταση ενός qubit από το $|0\rangle$ στο $|1\rangle$ και αντίστροφα. Παρατηρούμε ότι αν δράσουμε με τον πρώτο πίνακα του Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ πάνω σε ένα qubit, του οποίου η αναπαράσταση ως διάνυσμα είναι $\begin{pmatrix} a \\ b \end{pmatrix}$, καταλήγουμε με την «ανεστραμμένη» κατάσταση. Αν λοιπόν αρχικά $|a|^2 = 1, |b|^2 = 0$, τότε $|a'|^2 = 0, |b'|^2 = 1$ και έχουμε το επιθυμητό αποτέλεσμα.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} a' \\ b' \end{pmatrix} \tag{3.5}$$

Από την άλλη, το γεγονός ότι ένα qubit μπορεί να πάρει μια απειρία καταστάσεων, αντί για τις δύο ενός bit, μας προϊδεάζει ότι θα υπάρχουν πάνω από μία μη-τετριμμένες πύλες ενός qubit· στην πράξη, υπάρχουν άπειρες. Ο μοναδικός περιορισμός που επιβάλλεται στους τελεστές που μπορούμε να διαλέξουμε, όπως διαλέξαμε πριν τον σ_x, είναι αυτοί να είναι μοναδιαίοι. Αυτό ακολουθεί αναγκαστικά από την συνθήκη κανονικοποίησης $|a|^2 + |b|^2 = 1$. Η μοναδιαιότητα, λοιπόν, είναι ο μοναδικός περιορισμός που πρέπει να επιβάλουμε για να

καταλήξουμε με μία αποδεκτή κατάσταση για το τελικό qubit. Από την απειρία αυτή των δυνατών πυλών ενός qubit, παραθέτουμε μια λίστα με τις πιο χρήσιμες, αν και θα δούμε στην επόμενη παράγραφο ότι υπάρχει τουλάχιστον ένα πεπερασμένο σύνολο από πύλες το οποίο είναι πλήρες, δηλαδή με το οποίο μπορούμε να κάνουμε οποιαδήποτε πράξη.

- Πύλη Pauli-X (NOT)
$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.6}$$
- Πύλη Pauli-Y
$$\mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3.7}$$
- Πύλη Pauli-Z

  Διατηρεί το $|0\rangle$και αλλάζει το πρόσημο του $|1\rangle$ δίνοντας $-|1\rangle$.
$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.8}$$
- Πύλη Φάσης
$$\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \sqrt{\mathbf{Z}} \tag{3.9}$$
- Πύλη $\pi/8$
$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = \sqrt{\mathbf{S}} \because e^{i\pi/4} = \sqrt{i} \tag{3.10}$$
- Πύλη Hadamard

  Μετατρέπει το $|0\rangle$ σε $(|0\rangle + |1\rangle)/\sqrt{2} \equiv |+\rangle$, το οποίο είναι «στα μισά» μεταξύ $|0\rangle$ και $|1\rangle$ και το $|1\rangle$ σε $(|0\rangle - |1\rangle)/\sqrt{2} \equiv |-\rangle$ το οποίο είναι επίσης «στα μισά» μεταξύ $|0\rangle$ και $|1\rangle$, από «την άλλη μεριά». Αυτό φαίνεται καλλίτερα αν γραφεί σαν κανονικοποιημένος γραμμικός συνδυασμός των πυλών X και Z.
$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) \tag{3.11}$$
  Η ιδιότητα αυτή της πύλης Hadamard, της «ισομερούς» κατανομής του qubit στις καταστάσεις βάσης, είναι και ο λόγος που αποκαλείται επίσης *ρίζα της NOT*, παρότι αυτό μπορεί να προκαλέσει σύγχυση, καθώς $\mathbf{H}^2 = \mathbf{I}$, που προφανώς δεν είναι η πύλη NOT.

Αν περιοριστούμε προς στιγμήν μόνο στις πύλες ενός qubit, τότε από την αναπαράσταση της σφαίρας του Bloch (σχ. 3.1) καθίσταται προφανές ότι οποιαδήποτε πύλη θα πρέπει να μπορεί να αναλυθεί σε γινόμενο στροφών στις τρεις διαστάσεις. Άρα, οποιοδήποτε σύνολο γεννητόρων της ομάδας SO_3 θα είναι ένα πλήρες σύνολο μετασχηματισμών ενός qubit και καθώς η ομάδα SU_2 είναι ισόμορφη με την SO_3, συνεπάγεται ότι κάθε σύνολο γεννητόρων της SU_2 που αναπαρίστανται από 2×2 πίνακες θα είναι ένα πλήρες σύνολο πυλών ενός qubit.

3.2.2 Πύλες πολλαπλών qubit

Στα κλασσικά υπολογιστικά κυκλώματα, συνήθεις πύλες πολλαπλών bit είναι οι AND, OR, XOR, NAND και NOR. Από αυτές, η πύλη NAND αποτελεί από μόνη της ένα πλήρες σύνολο πυλών για οποιονδήποτε υπολογισμό, ακριβώς όπως ο σύνδεσμος NAND αποτελεί πλήρες σύνολο συνδέσμων στην μαθηματική λογική [33]. Στην περίπτωση των κβαντικών υπολογιστών, η πρότυπη πύλη πολλαπλών qubit είναι η πύλη *ελεγχόμενου NOT*.

- Πύλη Ελεγχόμενου NOT (Controlled NOT, C-NOT)

  Η πύλη αυτή έχει δύο qubit εισόδου, το qubit *ελέγχου* και το qubit *στόχου* και η δράση της πάνω σε ιδιοκαταστάσεις μπορεί να περιγραφεί ως εξής: αν το qubit ελέγχου είναι στην κατάσταση $|0\rangle$, τότε το qubit στόχου παραμένει αμετάβλητο, ενώ αν το qubit ελέγχου είναι στην κατάσταση $|1\rangle$, τότε το qubit ελέγχου παίρνει την τιμή που θα είχε αν πέρναγε μέσα από μια πύλη NOT (σχ. 3.2).[11]

$$\mathbf{U}_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \mathbf{I}_2 \oplus \mathbf{X} \tag{3.12}$$

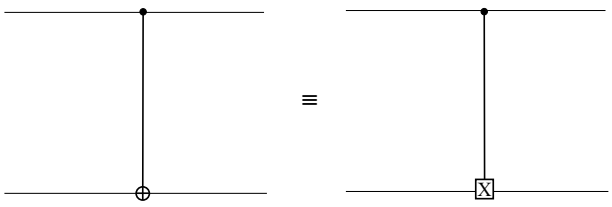
  Η αναπαράσταση της C-NOT ως πίνακα φαίνεται στην σχέση (3.12), απ' όπου ορίζεται και η δράση της σε καταστάσεις επαλληλίας. Βλέπουμε επίσης ότι ο πίνακας της πύλης μπορεί να αναλυθεί σε ευθύ άθροισμα πινάκων· ο πρώτος πίνακας είναι ο μοναδιαίος και ο δεύτερος ο πίνακας της πύλης NOT. Αυτό σημαίνει ότι στον πρώτο από τους δύο αναλλοίωτους υποχώρους του ταυστικού χώρου των δύο qubit δρα μόνον ο τελεστής $\mathbf{I}$, οπότε το πρώτο qubit παραμένει αμετάβλητο, ενώ στον δεύτερο δρα μόνον ο τελεστής $\mathbf{X}$ της πύλης NOT και άρα αυτός ορίζει το φάσμα των καταστάσεων που μπορεί να πάρει το δεύτερο qubit. Συνεπώς, μπορούμε να δούμε την πύλη C-NOT σαν μια γενίκευση της πύλης XOR· δρούμε με XOR στα qubit ελέγχου και στόχου και το αποτέλεσμα το φυλάττουμε στο qubit στόχου[12]

$$|a, b\rangle \rightarrow |a, b \oplus a\rangle \tag{3.13}$$

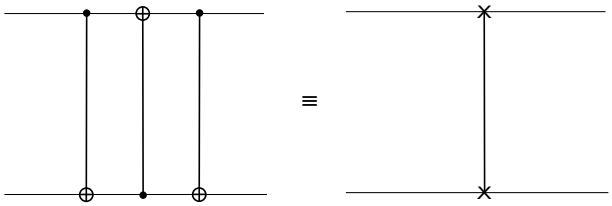
  Είναι προφανές ότι μπορούμε να ορίσουμε με παρόμοιο τρόπο μια απειρία πυλών πολλαπλών qubit· στην πράξη, κάθε πύλη U ενός qubit μπορεί να μετατραπεί σε ελεγχόμενη πύλη C-U με το ευθύ άθροισμα $\mathbf{I} \oplus \mathbf{U}$. Αυτό που πρέπει να σημειωθεί, όμως, είναι ότι δεν έχουν όλες οι κλασσικές πύλες το κβαντικό τους ανάλογο, όπως συμβαίνει με την πύλη NOT. Ο λόγος είναι ότι αφού κάθε κβαντική πύλη αναπαρίσταται από μοναδιαίους πίνακες, θα πρέπει να είναι και αντιστρέψιμη, αφού πάντα ορίζεται ο αντίστροφος ενός τέτοιου πίνακα. Πύλες, όμως, όπως η XOR και η NAND δεν είναι αντιστρέψιμες. Αυτό μπορεί να φαίνεται, αρχικά, ότι περιορίζει σημαντικά τις

[11] Το σύμβολο $\oplus$ όταν δρα σε πίνακες συμβολίζει ευθύ άθροισμα

[12] Το σύμβολο $\oplus$ όταν δρα σε αριθμούς συμβολίζει πρόσθεση modulo 2



Σχ. 3.2: Οι δύο ισοδύναμες αναπαραστάσεις της πύλης C-NOT.



Σχ. 3.3: Κύκλωμα ανταλλαγής δύο qubit και η ισοδύναμη συμβολική αναπαράστασή του ως πύλη.

λογικές πράξεις που μπορούμε να κάνουμε στους κβαντικούς υπολογιστές, αλλά όπως αποδεικνύεται [22], το πλήρες σύνολο πυλών ενός qubit, μαζί με την πύλη C-NOT, αποτελεί με την σειρά του πλήρες σύνολο πυλών πολλαπλών qubit. Άρα λοιπόν, μπορούμε να κάνουμε όλες τις συνήθεις λογικές πράξεις, κατασκευάζοντας *σύνθετες* πύλες. Ένα πολύ χρήσιμο παράδειγμα τέτοιας σύνθετης πύλης, είναι αυτό της ανταλλαγής qubit.

- Κύκλωμα ανταλλαγής qubit (swap gate)

  Η πύλη αυτή αποτελείται από τρεις πύλες C-NOT στην σειρά, με την μεσαία ανεστραμμένη όσον αφορά στον ρόλο των qubit ελέγχου και στόχου (σχ. 3.3). Το αποτέλεσμα της δράσης της είναι η ανταλλαγή των καταστάσεων των δύο qubit εισόδου, όπως φαίνεται παρακάτω

$$\begin{aligned} |a,b\rangle &\rightarrow |a, a\oplus b\rangle \\ &\rightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\rightarrow |b, (a\oplus b)\oplus b\rangle = |b,a\rangle \end{aligned} \tag{3.14}$$

  Από το σχ. 3.3 καθίσταται προφανής και η αναπαράσταση της πύλης ως πίνακα

$$\mathbf{U}_{SG} = (\mathbf{I}_2 \oplus \mathbf{U}_{CN})(\mathbf{U}_{CN} \oplus \mathbf{I}_2)(\mathbf{I}_2 \oplus \mathbf{U}_{CN}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.15}$$

Στο σημείο αυτό, έχουμε αναπτύξει τις βασικές έννοιες που χρειαζόμαστε για να κατασκευάζουμε κβαντικά υπολογιστικά κυκλώματα. Στην επόμενη παράγραφο, θα παρουσιάσουμε ένα τέτοιο, το οποίο επιλύει τον κβαντικό μετασχηματισμό Fourier και που θα αποτελέσει και την βάση για την κατασκευή ενός ανάλογου που θα επιλύει τον DFrFT.

3.3 Ο αλγόριθμος QFT

Ίσως η πιο θεαματική ανακάλυψη της κβαντικής υπολογιστικής έως τώρα είναι το ότι οι κβαντικοί υπολογιστές είναι ικανοί να εκτελέσουν αποδοτικά διαδικασίες που φαίνονται εικάζεται ότι δεν είναι εφικτές σε κλασσικούς υπολογιστές. Επί παραδείγματι, ο υπολογισμός της παραγοντοποίησης ενός ακεραίου n-bit χρειάζεται $\exp(\Theta(n^{1/3}\log^{2/3} n))$ βήματα με τον καλλίτερο γνωστό κλασσικός αλγόριθμος, τον επονομαζόμενο *κόσκινο αριθμητικού σώματος*. Από την άλλη, ο αλγόριθμος του Shor, ένας από τους πιο διάσημους κβαντικούς αλγόριθμους, κάνει τον ίδιο υπολογισμό σε $O(n^2 \log n \log\log n)$ βήματα, δηλαδή είναι εκθετικά πιο γρήγορος [22]. Στην καρδιά του αλγορίθμου αυτού, βρίσκεται ο κβαντικός μετασχηματισμός Fourier (QFT). Ο QFT είναι ένας αποδοτικός κβαντικός αλγόριθμος για την εκτέλεση του διακριτού μετασχηματισμού Fourier σε κβαντομηχανικά πλάτη πιθανότητας.

Ένας από τους συνηθισμένους τρόπους γραφής του DFT είναι

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \tag{3.16}$$

όπου $(x_0, \ldots, x_{N-1})$ είναι το διάνυσμα προς μετασχηματισμό και $(y_0, \ldots, y_{N-1})$ είναι το μετασχηματισμένο διάνυσμα.

Ο κβαντικός μετασχηματισμός Fourier από άποψη ορισμού είναι ακριβώς ο ίδιος, μόνο που συνηθίζεται να γράφεται με διαφορετικό συμβολισμό.

Ορισμός 3.1. Ως κβαντικός μετασχηματισμός Fourier μιας ορθοκανονικής βάσης $|0\rangle, \ldots, |N-1\rangle$ ορίζεται ο γραμμικός τελεστής $\mathbf{F}$ που η δράση του πάνω σε κάποια κατάσταση $|j\rangle$ της βάσης είναι

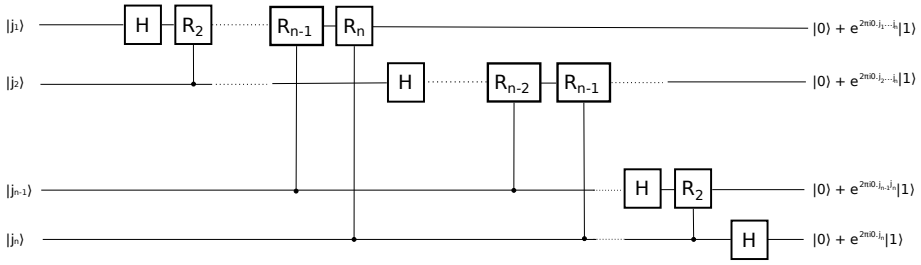
$$\mathbf{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle \tag{3.17}$$

Ισοδύναμα, η δράση του τελεστή πάνω σε μια τυχαία κατάσταση $\sum_{j=0}^{N-1} x_j|j\rangle$ μπορεί να γραφεί

$$\mathbf{F} \sum_{j=0}^{N-1} x_j |j\rangle = \sum_{k=0}^{N-1} y_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} x_l e^{2\pi i jk/N} |k\rangle \tag{3.18}$$

όπου τα πλάτη y_k είναι ο DFT των πλατών x_j. Παρότι δεν είναι προφανές από τον ορισμό αυτό, ο τελεστής $\mathbf{F}$ είναι μοναδιαίος και συνεπώς μπορεί να υλοποιηθεί σε κβαντικό υπολογιστή. Το ίδιο το κύκλωμα που τον υπολογίζει θα αποτελέσει έμμεση απόδειξη της μοναδιαιότητάς του.

Για την κατασκευή του κυκλώματος, θέτουμε $N = 2^n$ και διαλέγουμε την βάση $|0\rangle, \ldots, |2^n - 1\rangle$ για την υπολογιστική μας βάση. Θα δούμε ότι είναι βολικότερο να γράφουμε την κατάσταση $|j\rangle$ χρησιμοποιώντας την δυαδική αναπαράσταση



Σχ. 3.4: Αποδοτικό κύκλωμα για τον υπολογισμό του κβαντικού μετασχηματισμού Fourier. Το κύκλωμα αυτό βγαίνει άμεσα από την σχέση (3.23). Έχουν παραληφθεί οι πύλες ανταλλαγής στο τέλος του κυκλώματος, οι οποίες αντιστρέφουν την σειρά των qubit, όπως επίσης και οι παράγοντες κανονικοποίησης $1/\sqrt{2}$ στην έξοδο.

$j = j_1 j_2 \dots j_n$ που στην δεκαδική αναπαράσταση είναι $j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$. Ακόμα, θα γράφουμε $0.j_l j_{l+1} \dots j_m$ για να αναπαραστήσουμε το δυαδικό κλάσμα $j_l/2 + j_{l+1}/4 + \dots + j_m/2^{m-l+1}$. Με την χρήση του συμβολισμού αυτού θα φέρουμε την μορφή του μετασχηματισμού Fourier του ορισμού 3.1 σε μορφή γινομένου, γνωστή και ως *ανάπτυγμα Cooley-Tukey* [28].

$$\mathbf{F}|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \tag{3.19}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} |k_1 \dots k_n\rangle \tag{3.20}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \tag{3.21}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \tag{3.22}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \tag{3.23}$$

$$= \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \dots (|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle)}{2^{n/2}} \tag{3.24}$$

όπου τα κλασματικά εκθετικά στην τελευταία σχέση εμφανίζονται γιατί κάθε διαίρεση με 2^{-l} δημιουργεί l κλασματικά δυαδικά ψηφία, ενώ το ακέραιο κομμάτι μπορεί να παραληφθεί λόγω της περιοδικότητας της συνάρτησης $e^{2\pi i}$. Η μορφή γινομένου (3.23) κάνει σχεδόν προφανή τη μορφή που πρέπει να έχει το κύκλωμα που θα υπολογίζει τον μετασχηματισμό, το οποίο φαίνεται στο σχήμα 3.4 . Η πύλη περιστροφής $\mathbf{R}_k$ αντιστοιχεί στον μοναδιαίο μετασχηματισμό

$$\mathbf{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \tag{3.25}$$

Για να βεβαιωθούμε ότι όντως το κύκλωμα αυτό υπολογίζει τον κβαντικό μετασχηματισμό Fourier, θα το περπατήσουμε βήμα-βήμα αρχίζοντας με την κατάσταση $|j_1 j_2 \dots j_n\rangle$ ως είσοδο.

Η εφαρμογή της πύλης Hadamard στο πρώτο bit δημιουργεί την κατάσταση

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2 \ldots j_n\rangle \tag{3.26}$$

αφού $e^{2\pi i 0.j_1} = -1$ όταν j_1=1 και +1 ειδάλλως. Η εφαρμογή της πύλης C-R_2 παράγει την κατάσταση

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2 \ldots j_n\rangle \tag{3.27}$$

Συνεχίζουμε εφαρμόζοντας τις πύλες C-R_3 έως C-R_n, κάθε μία από τις οποίες προσθέτει ένα περισσότερο bit στην φάση του παράγοντα του πρώτου $|1\rangle$. Στο τέλος της διαδικασίας αυτής, έχουμε την κατάσταση

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)|j_2 \ldots j_n\rangle \tag{3.28}$$

Εν συνεχεία, πραγματοποιούμε μια παρόμοια διαδικασία στο δεύτερο qubit. Η πύλη Hadamard μας βάζει στην κατάσταση

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2}|1\rangle\right)|j_3 \ldots j_n\rangle \tag{3.29}$$

και οι πύλες C-R_2 έως C-R_{n-1} μας δίδουν

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i 0.j_1 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right)|j_3 \ldots j_n\rangle \tag{3.30}$$

Προχωρώντας κατά αυτόν τον τρόπο για κάθε qubit, παίρνουμε την τελική κατάσταση

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_1 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) \tag{3.31}$$

Με την βοήθεια πυλών ανταλλαγής (οι οποίες παραλείπονται από το σχ. 3.4 χάριν σαφήνειας), αντιστρέφουμε την σειρά των qubit και τελικά έχουμε

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right) \tag{3.32}$$

που είναι ακριβώς η σχέση (3.23). Εξάλλου, έχουμε και την έμμεση απόδειξη ότι ο κβαντικός μετασχηματισμός Fourier είναι μοναδιαίος, αφού κάθε πύλη που χρησιμοποιήσαμε στο κύκλωμα είναι μοναδιαία.

Όσον αφορά στην πολυπλοκότητα του κυκλώματος που χρησιμοποιήσαμε, βλέπουμε ότι η εφαρμογή της πύλης Hadamard και των $n-1$ ελεγχόμενων περιστροφών στο πρώτο qubit αναλογεί σε n πύλες. Ομοίως για το δεύτερο qubit, έχουμε άλλες $n-1$ πύλες, δηλαδή $n+(n-1)$ πύλες για τα δύο πρώτα qubit. Κατά αυτόν τον τρόπο, εν τέλει έχουμε $n+(n-1)+\ldots+1 = n(n+1)/2$ πύλες εν τω συνόλω, και άλλες $n/2$ πύλες ανταλλαγής. Συνεπώς, το κύκλωμα έχει πολυπλοκότητα χρόνου $O(n^2) = O(log^2 N)$, αφού $N = 2^n$ και άρα ο QFT είναι *εκθετικά* πιο γρήγορος από τον FFT.

3.4 Κβαντικός υπολογισμός του DFrFT

Για να υπολογίσουμε τον DFrFT με παράμετρο a, όταν $a \in \mathbb{Q}_F$, αρκεί να κατασκευάσουμε ένα κύκλωμα που υλοποιεί τον πίνακα $\mathbf{G}$ της σχέσης (2.56), αφού από το (i) του πορίσματος 1.1

$$\mathbf{F}_{m/k} = \prod_{j=1}^{m} \mathbf{F}_{1/k} = \prod_{j=1}^{m} \mathbf{G} \tag{3.33}$$

Συνεπώς, αν έχουμε ένα τέτοιο κύκλωμα, τότε μπορούμε να το χρησιμοποιήσουμε $O(m)$ φορές για να υπολογίσουμε τον μετασχηματισμό $\mathbf{F}_{m/k}$. Ακολουθώντας τον συμβολισμό της παραγράφου 3.3, μπορούμε να γράψουμε τον DFrFT παραμέτρου $1/K$, όπου $N = 4K - 1$, N πρώτος, ως

$$y_k = \sum_{j=0}^{N-1} G_{k,j} x_j \tag{3.34}$$

$$= \frac{1}{\sqrt{N}} i(2b_0|N) \sum_{j=0}^{N-1} x_j e^{\pi i(a_0 j^2 + a_0 l^2 - 2jk)/Nb_0} \tag{3.35}$$

ή με την συνήθη γραφή για μια ορθοκανονική βάση $|0\rangle, \ldots, |N-1\rangle$

$$\mathbf{G}|j\rangle = \frac{1}{\sqrt{N}} i(2b_0|N) \sum_{k=0}^{N-1} e^{\pi i(a_0 k^2 + a_0 j^2 - 2kj)/Nb_0} |k\rangle \tag{3.36}$$

Στόχος μας είναι να φέρουμε την εξίσωση (3.36) σε μορφή τανυστικού γινομένου, ανάλογη με αυτή της σχέσης (3.23). Έχουμε λοιπόν

$$\mathbf{G}|j\rangle = \frac{1}{\sqrt{N}} i(2b_0|N) \sum_{k=0}^{N-1} e^{\pi i a_0 k^2/Nb_0} e^{\pi i a_0 j^2/Nb_0} e^{-2\pi i jk/Nb_0} |k\rangle \tag{3.37}$$

$$= \frac{e^{\pi i a_0 j^2/Nb_0}}{\sqrt{N}} i(2b_0|N) \sum_{k=0}^{N-1} e^{\pi i a_0 k^2/Nb_0} e^{-2\pi i jk/Nb_0} |k\rangle \tag{3.38}$$

$$= \frac{e^{\pi i a_0 j^2/Nb_0}}{\sqrt{N}} i(2b_0|N) \sum_{k=0}^{2^n-1} e^{\pi i a_0 k^2/2^n b_0} e^{-2\pi i jk/2^n b_0} |k\rangle \tag{3.39}$$

Στην σχέση (3.39) έχουμε κάτι την αλλαγή από N σε $2^n - 1$ στο όριο της άθροισης. Αν ο πρώτος αριθμός N είναι και πρώτος Mersenne[13], όπως π.χ. συμβαίνει για την περίπτωση του $N = 127 = 4 \cdot 32 - 1 = 2^7 - 1$, τότε η αλλαγή συνεισφέρει μόνον δύο πλεονάζοντες προσθετικούς όρους, οι οποίοι ανάλογα με την απαιτούμενη ακρίβεια μπορούν εύκολα να αγνοηθούν ή να υπολογιστούν και να αφαιρεθούν. Στην αντίθετη περίπτωση, διαλέγουμε $2^n > N$ ως την πρώτη δύναμη του 2 μετά το N και επεκτείνουμε την υπολογιστική βάση με $2^n - N + 1$ ancilla qubits σε $|0\rangle \otimes \ldots \otimes |N-1\rangle \otimes |0\rangle^{2^n - N + 1}$ αν υποθέσουμε ότι το υπολογιστικό μας μοντέλο είναι big-endian· στο τέλος του υπολογισμού απορρίπτουμε τα πλεονάζοντα ancilla qubits. Συνεχίζοντας, θέτουμε $A_j = ie^{\pi i a_0 j^2/Nb_0}(2b_0|N)$

[13] Πρώτοι αριθμοί Mersenne είναι οι πρώτοι αριθμοί που μπορούν να γραφούν με την μορφή $2^n - 1$ για κάποιο n. Αν $N = 4K - 1$, τότε προφανώς, θα πρέπει $K = 2^m$ για κάποιο m.

για συντομία και έχουμε

$$\mathbf{G}|j\rangle = \frac{A_j}{\sqrt{N}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{\frac{\pi i a_0 2^n (\sum_{l=1}^{n} k_l 2^{-l})^2}{b_0}} e^{\frac{-2\pi i j \sum_{l=1}^{n} k_l 2^{-l}}{b_0}} |k_1 \dots k_n\rangle \tag{3.40}$$

Το τετράγωνο του αθροίσματος στο πρώτο εκθετικό της τελευταίας σχέσης μπορεί εν γένει να αναπτυχθεί με την βοήθεια του πολυωνυμικού αναπτύγματος του De Moivre, την γενίκευση του διωνυμικού αναπτύγματος του Newton.

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{k_1,k_2,\dots k_m} \binom{n}{k_1, k_2, \dots k_m} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m} \tag{3.41}$$

όπου η άθροιση γίνεται επί όλων των ακολουθιών (k_m) με την ιδιότητα $\sum_m k_m = n$. Για $n = 2$, η σχέση αυτή γίνεται πιο απλά

$$\left(\sum_{i=1}^{m} x_i \right)^2 = \sum_{i=1}^{m} \sum_{j=1}^{m} x_i x_j \tag{3.42}$$

οπότε

$$\begin{aligned}
\mathbf{G}|j\rangle &= \frac{A_j}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{\frac{\pi i a_0 2^n \sum_{l=1}^{n} \sum_{m=1}^{n} k_l k_m 2^{-l-m}}{b_0}} e^{\frac{-2\pi i j \sum_{l=1}^{n} k_l 2^{-l}}{b_0}} |k_1 \dots k_n\rangle \\
&= \frac{A_j}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \prod_{m=1}^{n} \bigotimes_{l=1}^{n} e^{\frac{\pi i a_0 2^n k_l k_m 2^{-l-m}}{b_0}} e^{\frac{-2\pi i j k_l 2^{-l}}{b_0}} |k_l\rangle \qquad (3.43) \\
&= \frac{A_j}{2^{n/2}} \prod_{m=1}^{n} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{\frac{\pi i a_0 2^n k_l k_m 2^{-l-m}}{b_0}} e^{\frac{-2\pi i j k_l 2^{-l}}{b_0}} |k_l\rangle \right] \qquad (3.44)
\end{aligned}$$

Η σχέση (3.44) έχει την επιθυμητή μορφή τανυστικού γινομένου και είναι το ανάλογο της σχέσης (3.23) για τον κβαντικό μετασχηματισμό Fourier. Παρατηρούμε ότι η εν λόγω μορφή είναι επίσης μοναδιαία, αφού $|A_j| = \pm 1$. Αυτό σημαίνει ότι μπορεί να αποτελέσει την βάση για την κατασκευή ενός κυκλώματος που υπολογίζει τον κβαντικό κλασματικό μετασχηματισμό Fourier για παράμετρο $1/K$ και κατ' επέκτασιν, χρησιμοποιώντας το m φορές, για οποιαδήποτε παράμετρο $a \in \mathbb{Q}_F$.

Ένα τέτοιο κύκλωμα, αν και διαισθητικά περιμένει κανείς να είναι παρόμοιο με αυτό του QFT, θα είναι προφανώς πιο περίπλοκο· σε πρώτη προσέγγιση, όμως, εκτιμάται ότι η αύξηση θα είναι της τάξεως του n εξ αιτίας του πλεονάζοντος γινομένου και άρα θα έχουμε πολυπλοκότητα $O(n^3) = O(log^3 N)$. Συνεπώς, εφαρμόζοντας το κύκλωμα m φορές, τόσες όσες χρειάζεται για τυχόν $a = m/k \in \mathbb{Q}_F$, καταλήγουμε σε $O(mlog^3 N)$ βήματα. Επειδή, όμως $m \leq 4k$ και $N = 4k + 1$, θα ισχύει $O(m) = O(N)$, άρα το ανώτατο όριο πολυπλοκότητας θα είναι $O(Nlog^3 N)$. Διαφαίνεται, λοιπόν, ότι μπορούμε με την χρήση κβαντικών κυκλωμάτων να επιτύχουμε έναν αλγόριθμο για τον DFrFT συγκρίσιμης αποδοτικότητας με του FFT για τον κλασσικό μετασχηματισμό Fourier.

4 Επίλογος

Στην εργασία αυτή, παρουσιάσαμε την έννοια του κλασματικού μετασχηματισμού Fourier και επιχειρήσαμε να αξιολογήσουμε κάποιους από τους ορισμούς που έχουν προταθεί μέχρι σήμερα στην βιβλιογραφία για τον διακριτό μετασχηματισμό (DFrFT). Τα βασικά κριτήρια για την αξιολόγηση ήταν κάποιες ιδιότητες που θέλουμε να έχει ο μετασχηματισμός, όπως η προσθετική ιδιότητα της παραμέτρου του, η μοναδιαιότητα, η ακρίβεια και η υπολογιστική πολυπλοκότητα. Από τους ορισμούς αυτούς, ιδιαίτερη έμφαση δώσαμε στον ορισμό των Candan, Kutay και Ozaktas [8], ο οποίος έχει όλες τις ιδιότητες που θέλουμε, πλην όμως είναι εγγενώς προσεγγιστικός και υπολογιστικά ακριβός.

Εν συνεχεία, δώσαμε έναν νέο ορισμό για τον DFrFT, ο οποίος έχει επίσης τις εν λόγω ιδιότητες, αλλά είναι και ακριβής, καθώς βασίζεται εξ αρχής σε θεωρία ομάδων. Ο ορισμός αυτός στηρίζεται στην λεγόμενη κβάντωση Weyl, μια διαδικασία μέσω της οποίας μπορεί να ορισθεί και ο καλά γνωστός DFT, όταν εφαρμοστεί στο φυσικό σύστημα του κβαντικού αρμονικού ταλαντωτή. Στην περίπτωση του DFrFT, το κατάλληλο φυσικό σύστημα είναι ο κβαντικός ταλαντωτής Balian-Itzykson, του οποίου ο φασικός χώρος έχει την μορφή $GF[p]$, όπου ο p είναι πρώτος αριθμός της μορφής $4k-1$.

Τέλος, εξετάσαμε το ενδεχόμενο ύπαρξης ενός κβαντικού αλγορίθμου για την επιτάχυνση του υπολογισμού του μετασχηματισμού, βασιμένοι στην ιδέα πίσω από τον κβαντικό αλγόριθμο για τον συνήθη μετασχηματισμό Fourier.

Σημειώνουμε ότι τα αποτελέσματα που βγάλαμε μπορούν να γενικευτούν για την περίπτωση όπου ο φασικός χώρος του ταλαντωτή BI έχει την μορφή $GF[p^n]$. Η άλγεβρα των ομάδων που περιγράφουν την διαδικασία της κβάντωσης παραμένει ουσιαστικά η ίδια, αλλά στην περίπτωση αυτή, το τυχόν κβαντικό κύκλωμα μπορεί να περιγραφεί πιο φυσικά με αρχιτεκτονική n-qudit, δηλαδή qubit n καταστάσεων, κάτι που μένει να μελετηθεί ενδελεχώς.

5 Παράρτημα

Ακολουθεί ο PL/pgSQL κώδικας δημιουργίας μιας βάσης δεδομένων PostgreSQL ονόματι qdfrft για την ανάλυση των δυνατών τιμών της παραμέτρου a του DFrFT.

```
/* Δημιουργία και χρήση της βάσης δεδομένων */
CREATE DATABASE qdfrft;
USE qdfrft;
CREATE TABLE primes(p int PRIMARY KEY, k int DEFAULT NULL);
CREATE TABLE alphas(p int, n int, a float(24));
CREATE VIEW nu AS SELECT DISTINCT alphas.n FROM alphas ORDER BY alphas.n;
CREATE VIEW pn AS SELECT primes.p, nu.n FROM primes, nu ORDER BY primes.p, nu.n;

/* Αποθηκευμένη συνάρτηση σκανδαλισμού για την εισαγωγή πρώτου αριθμού.
Αν ο αριθμός είναι της μορφής 4k-1, υπολογίζει και ενημερώνει την τιμή k,
ειδάλλως της θέτει την τιμή NULL */
CREATE OR REPLACE FUNCTION fnInsPrimeTrigger() RETURNS trigger AS $$
BEGIN
        IF CAST((NEW.p+1)/4 AS int)=CAST((NEW.p+1)/4.0 AS float(24)) THEN
                NEW.k:=(NEW.p+1)/4;
        ELSE
                NEW.k:=NULL;
        END IF;
        RETURN NEW;
END;
$$ LANGUAGE plpgsql;

/* Σκανδάλη εισαγωγής πρώτου αριθμού */
DROP TRIGGER IF EXISTS trInsPrimeTrigger ON primes;
CREATE TRIGGER trInsPrimeTrigger
BEFORE INSERT OR UPDATE
ON primes FOR EACH ROW
EXECUTE PROCEDURE fnInsPrimeTrigger();

/* Αποθηκευμένη συνάρτηση για τον υπολογισμό των δυνατών τιμών της παραμέτρου a
για δεδομένο πρώτο αριθμό p. Υπολογίζονται οι τιμές n/k για n=1,2,...k
CREATE OR REPLACE FUNCTION calcAlpha(prime int) RETURNS int AS $$
DECLARE
        kappa float(1);
        alpha float(1);
BEGIN
        SELECT k INTO kappa FROM primes WHERE p = prime;
        FOR i in 1..4*kappa LOOP
                alpha:=i/kappa;
                INSERT INTO alphas (p,n,a) VALUES (prime, i, alpha);
        END LOOP;
        RETURN 0;
END;
$$ LANGUAGE plpgsql;
```

```
/* Αποθηκευμένη συνάρτηση για τον υπολογισμό των δυνατών τιμών της παραμέτρου a
για όλους τους πρώτους αριθμούς στην βάση.
CREATE OR REPLACE FUNCTION calcAllAlphas() RETURNS int AS $$
DECLARE
        prime record;
BEGIN
        FOR prime IN SELECT p FROM primes WHERE k IS NOT NULL LOOP
                PERFORM calcAlpha(prime.p);
        END LOOP;
        RETURN 0;
END;
$$ LANGUAGE plpgsql;
```

Για να γεμίσουμε τον πίνακα **primes** με τους πρώτους αριθμούς, εκτελούμε την παρακάτω εντολή από το κέλυφος του UNIX. Υποθέτουμε ότι η λίστα με τους πρώτους βρίσκεται υπό μορφή γραμμών στο αρχείο **primes.lst**

```
cat primes.lst| sed -e \
's/\(.\+\)/INSERT INTO primes (p) VALUES (\1);/'|psql qdfrft -f -
```

ενώ για να γεμίσουμε τον πίνακα με τις τιμές του a, εκτελούμε

```
pqsl qdfrft -c "SELECT calcAllAlphas();"
```

Ακολουθούν μερικά παραδειγματικά ερωτήματα SQL

```
/* Πλήθος πρώτων αριθμών της μορφής p=4k-1 */
SELECT COUNT(p) FROM primes WHERE k IS NOT NULL;
/* Συνολικό πλήθος τιμών της παραμέτρου a*/
SELECT COUNT(a) FROM alphas;
/* Πλήθος διακεκριμένων τιμών της παραμέτρου a*/
SELECT COUNT(*) FROM (SELECT DISTINCT a FROM alphas) AS dalphas;
/* Πλειάδες (p,n,a) με το a κανονικοποιημένο στο μηδέν όπου
δεν ορίζεται */
SELECT pn.p,pn.n,COALESCE(a,0) AS a FROM pn LEFT OUTER JOIN alphas
ON pn.n=alphas.n AND pn.p=alphas.p ORDER BY p,n,a;
```

Βιβλιογραφία

[1] L. B. Almeida. The fractional Fourier transform and time-frequency representation. *IEEE Trans. Sig. Proc.*, 42:3084–3091, 1994.

[2] T. M. Apostol. *Introduction to analytic number theory.* Springer, New York, 1984.

[3] G. G. Athanasiu and E. G. Floratos. Coherent states in finite quantum mechanics. *Nuclear Physics*, B425:343–364, 1994.

[4] D. H. Bailey and P. N. Swarztrauber. The fractional Fourier transform and applications. *SIAM Review*, 33(3):389–404, 1991.

[5] R. Balian and C. Itzykson. Observations sur la mécanique quantique finie. *C.R. Acad. Sci. Paris*, Sér. I Math. 303:773–778, 1986.

[6] A. Bultheel and H. Martínez Sulbaran. Computation of the fractional Fourier transform. *Applied and Computational Harmonic Analysis*, 16(3):182–202, 2004.

[7] Ç. Candan. The discrete fractional Fourier transform. Master's thesis, Bilkent University, Ankara, 1998.

[8] Ç. Candan, M. A. Kutay, and H. M. Ozaktas. The discrete fractional Fourier transform. *IEEE Trans. Sig. Proc.*, 48:1329–1337, 2000.

[9] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, Berlin, 1993.

[10] D. Fairlie, P. Fletcher, and C. Zachos. Trigonometric structure constants for new infinite-dimensional algebras. *Physics Letters B.*, 218(2):203–206, 1989.

[11] E. G. Floratos. The Heisenberg-Weyl group on the $Z_n \times Z_n$ discretized torus membrane. *Physics Letters B*, 228(3):335–340, 1989.

[12] E. G. Floratos and G. K. Leontaris. *World-volume supermembrane instantons in the light-cone frame*, volume 163/2000 of *Springer Tracts in Modern Physics*, pages 285–299. Springer Berlin / Heidelberg, 2007.

[13] M. Gel'fand, M. I. Graev, and I. I. Piatetskii-Shapiro. *Representation theory and automorphic functions.* Saunders, London, 1966, 1990.

[14] H. Georgie. *Lie algebras in particle physics: from isospin to unified theories.* Perseus Group, Massachusetts, second edition, 1999.

[15] B. C. Hall. *Lie groups, Lie algebras, and representations.* Springer, Berlin, 2003.

[16] J. H. Hannay and M. V. Berry. Quantization of linear maps on the torus-Fresnel diffraction by a periodic grating. *Physica D*, 1:267–291, 1980.

[17] A. Kirillov. *Eléments de la théorie des represéntations.* MIR, Moscow, 1974.

[18] P. Lebœuf and A. Voros. Quantum nodal points as fingerprints of classical chaos. In G. Casati and B.V. Chirikov, editors, *Quantum Chaos, Between order and disorder*, pages 507–533. Cambridge U.P., Cambridge, 1993.

[19] B. Lidl and H. Niederreiter. Finite fields. In *Encyclopedia of mathematics and its applications*, volume 20. Cambridge U.P., Cambridge, 1984.

[20] G. Matrin. A Darboux theorem for multi-symplectic manifolds. *Letters in Mathematical Physics*, 16(2):133–138, 1988.

[21] V. Namias. The fractional order Fourier transform and its applications in quantum mechanics. *J. Inst. Math. Appl.*, 25:241–265, 1980.

[22] M. A. Nilsen and Chuang I. L. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[23] J. O'Neil. DiscreteTFDs: a collection of Matlab files for computing time-frequency distributions or time-frequency representations. online, 1999. `http://tfd.sourceforge.net`.

[24] H. M. Ozaktas, O. Arıkan, M. A. Kutay, and G. Bozdağı. Digital computation of the fractional Fourier transform. *IEEE Trans. Sig. Proc.*, 44:2141–2150, 1996.

[25] S. C. Pei and M. H. Yeh. Improved discrete fractional Fourier-transform. *Opt. Letters*, 22:1047–1049, 1997.

[26] E. Stein and G. Weiss. *Introduction to Fourier Analysis on Euclidean Spaces.* Princeton University Press, Princeton, N.J., 1971.

[27] S. Tanaka. Construction and classification of irreducible representations of special linear group of the second order over a finite field. *Osaka J. Math*, 4:65–84, 1967.

[28] R. Tolimieri, M. An, and C. Lu. *Mathematics of Multidimensional Fourier Transform Algorithms.* Springer, New York, second edition, 1997.

[29] A. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42(2), 1936.

[30] A. Weil. Sur certains groupes d'opérateurs unitaires. *Acta Mathematica*, 111(1):143–211, 1964.

[31] N. Wiener. Hermitian polynomials and Fourier analysis. *J. Math. Phys.*, 8:70–73, 1929.

[32] L. Zhengjun, Z. Haifa, and L. Shutian. A discrete fractional random transform. *Optics Communications*, 225(4-6):357–365, 2005.

[33] Δημητρακόπουλος, Κ. *Σημειώσεις μαθηματικής λογικής.* Ελληνικό Ανοικτό Πανεπιστήμιο, Αθήνα, 1999.

[34] Μοσχοβάκης, Γ. *Υπολογισιμότητα.* , Αθήνα, 1999.

[35] Τραχανάς, Σ. *Κβαντομηχανική Ι.* Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο, 1999.

Ευρετήριο

DFrFT, *βλ.* μετασχηματισμός,Fourier

FFT, 3
FrFT, *βλ.* μετασχηματισμός,Fourier

q-bit, *βλ.* qubit
qubit, 24

άλγεβρα
  $\mathfrak{h}$, 18
  $\mathfrak{su}_2$, 18
  Heisenberg-Weyl, 14
  Lie, 15, 18

αλγόριθμος
  DFrFT, 7
  FrFT, 3
  QFT, 30
  Shor, 30
  αποδοτικός, 23
ανάλυση
  Gram-Schmidt, 15
  ιδιοτιμών, 3, 5
ανάπτυγμα
  Cooley-Tukey, 31
αναπαράσταση
  SL_2, 12
  έγκυρη, 19
  διανυσματικού χώρου, 14
  δυαδική, 30
  μεταπλεκτική, 18, 19
  μοναδιαία, 18
  ομάδας μετατόπισης, 17
  πιστή, 18
  προβολική, 17
αρχή
  επαλληλίας, 24
  κατάρρευσης κυματοσυνάρτησης, 25
  υπέρθεσης, 24

βάση
  Darboux, 15
  εφαπτομενικού χώρου, 11
  ορθοκανονική, 15, 30
  υπολογιστική, 30

γεννήτορες
  O_2, 14
  SL_2, 12
  $\mathbb{Z}_p^Q, \mathbb{Z}_p^P$, 17
  $\mathfrak{su}_2$, 18
  Heisenberg-Weyl, 18

διαφορομορφισμός, 10

εξίσωση
  Darboux, 15
  Shrödinger, 1
  Χαμιλτονιανή, 11
  χαρακτηριστική, 13

θέση
  Church-Turing, 23
    ισχυρή, 24
θεώρημα
  Lagrange, 13
  Liouville, 11
  Stone-von Neumann, 17

ιδιοδιάνυσμα, 5
ιδιοκατάσταση, 24
ιδιοσυνάρτηση, 5
ιδιοτιμή, 5

κέντρο, 17, 18
κβάντωση
  Weyl, 9, 20
κλάση
  BPP, 24
  BQP, 24
  NP, 24

μετασχηματισμός
  Fourier, 1
    πίνακας, 5
    περίοδος, 4
  Fourier,κβαντικός, 30
    κύκλωμα, 31
    ορισμός, 30
  Fourier,κλασματικός
    ιδιότητες, 2
    ορισμός, 1
    ορισμός,διακριτός, 3
  Weyl, 9
  z-transform, 4
  γραμμικός κανονικός, 2

κανονικός, 11
κανονικός γραμμικός, 11
συμπλεκτικός, 18
μηχανή
Turing, 23
καθολική, 23
μορφή
2-μορφή, 10
Χαμιλτονιανών εξισώσεων, 11
γινομένου (Fourier), 31
διγραμμική, 14
συμπλεκτική, 10
τελεστική, 14

νόμος
Moore, 23

ομάδα
O_2, 12
SL_2, 3, 12
SO_2, 3, 13
SU_2, 18
Heisenberg-Weyl, 14
Lie, 15
αβελιανή, 12, 17
κυκλική, 13, 19
μεταπλεκτική, 18
μετατόπισης, 17
πολλαπλασιαστική, 12
στροφών, 13
συμπλεκτική, 12, 15, 18

πίνακας
Fourier, *βλ.* μετασχηματισμός
Vandermonde, 5
πολλαπλότητα, 10
διαφορίσιμη, 15
συμπλεκτική, 11
υποκείμενη, 15
πολυπλοκότητα, 3, 7
πολυώνυμο
Hermite, 6
πυρήνας, 2
πύλη
C-NOT, 28
Hadamard, 27
NOT, 27
Pauli
Y, 27
Z, 27
Pauli-X, 27
swap, 29
ανταλλαγής, 29
π/8, 27
περιστροφής, 31
φάσης, 27

σταθερά
Plank, 18
δομής, 18
συμπλεκτομορφισμός, 11
Χαμιλτονιανός, 11
συνάρτηση
chirp, 2
Hermite, 5
αναδρομική, 24
τάσης μεταβολής, 2
συνέλιξη, 2
σχέση
κανονική μετάθεσης, 15
Heisenberg, 16, 17
Heisenberg-Weyl, 17
εκθετική, 17

τάξη
ομάδας, 13
προσέγγισης, 6
ταλαντωτής
Balian-Itzykson, 13, 14
αρμονικός, 9, 14
τελεστής
διαφορικός, 6
θέσης, 16
μετατόπισης, 6, 16, 18
ορμής, 16
στροφής, 3, 14

υποομάδα, *βλ.* ομάδα
υποχώρος, *βλ.* χώρος

χώρος
Hilbert, 15
διανυσματικός, 14
Heisenberg-Weyl, 15, 18
συμπλεκτικός, 14
ευθύ άθροισμα, 18
εφαπτομενικός, 11
θέσης, 17
καταστατικός, 16
ορμής, 16

παραμετρικός, 10
φασικός, 2, 10, 11, 15