ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

ΓΕΝΙΚΟ ΤΜΗΜΑ

Τομέας Μαθηματικών

ΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΑΝΑΖΗΤΗΣΗΣ ΣΕ ΜΗ ΔΟΜΗΜΕΝΕΣ ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

Διπλωματική Διατριβή
Μεταπτυχιακού Διπλώματος Ειδίκευσης

Χρήστος Κωνσταντάκης

Επιβλέπων καθηγητής:
Αναπληρωτής Καθηγητής Δημοσθένης Έλληνας

Χανιά 2007

Περίληψη

Το 1996 ο Lov Grover επινόησε τον φερώνυμο Κβαντικό αλγόριθμο ταχείας αναζήτησης ενός στοιχείου μέσα σε μια μη δομημένη βάση δεδομένων με N στοιχεία και απέδειξε ότι το ζητούμενο στοιχείο είναι δυνατόν να βρεθεί με $O(\sqrt{N})$ το πλήθος δοκιμές, ενώ σε έναν κλασικό υπολογιστή οποιασδήποτε τεχνολογίας και αρχιτεκτονικής είναι γνωστό ότι αυτό επιτυγχάνεται με $O(N)$ δοκιμές. Όμως οι καταστάσεις υπέρθεσης, στις οποίες βασίζεται η λειτουργία κάθε Κβαντικού υπολογιστή, είναι εξαιρετικά ασταθείς και η αλληλεπίδραση με το περιβάλλον μπορεί να τις οδηγήσει σε κατάρρευση.
Ο σκοπός μας είναι να μελετήσουμε την ανθεκτικότητα του αλγόριθμου Grover στον κβαντικό θόρυβο. Η παρούσα εργασία χωρίζεται σε τέσσερα Κεφάλαια:

Στο **Κεφάλαιο 0** δίνουμε τα βασικά Μαθηματικά εργαλεία που θα χρησιμοποιήσουμε.
Στο **1ο Κεφάλαιο** παρουσιάζουμε τον κλασικό αλγόριθμο του Grover, και ακολούθως, στο **2ο** και στο **3ο Κεφάλαιο** γίνεται η προαναφερθείσα μελέτη της ανθεκτικότητάς του.
Οι Προτάσεις που αποδεικνύονται στα δυο τελευταία Κεφάλαια έχουν δημοσιευθεί στα [**10**] και [**11**].

Αναλυτικότερα, στο **2ο Κεφάλαιο**, αρχικά μεταφέρουμε ισοδύναμα την αναζήτηση από την αρχική βάση δεδομένων σε μια νέα N-διάστατη βάση δεδομένων της οποίας τα στοιχεία είναι προβολικοί τελεστές, εκφράζουμε την επίδραση του θορύβου x μέσω πλήρως θετικών ιχνοδιατηρητικών απεικονίσεων, και αποδεικνύουμε ότι ο αλγόριθμος παραμένει αποτελεσματικός σε $O(\sqrt{N})$ επαναλήψεις για αριθμησίμως άπειρες τιμές του x («καλές τιμές» του x) τις οποίες και υπολογίζουμε αναλυτικά, ενώ για τις υπόλοιπες τιμές του θορύβου δείχνουμε ότι καταρρέει εκθετικά γρήγορα. Προκύπτουν δυο τέτοιες οικογένειες τιμών του x. Για τα x πρώτου είδους ο αλγόριθμος παίρνει την κλασική του μορφή ενώ για αυτά του δευτέρου είδους παρατηρείται το αξιοσημείωτο φαινόμενο της αναγωγής της αναζήτησης σε αναζήτηση μέσω προβολικού τελεστή χωρίς όμως ο αλγόριθμος να ανάγεται στην κλασική του μορφή.

Στο **3ο Κεφάλαιο** εξετάζουμε την παραπάνω διαδικασία αναζήτησης στοιχείου από τη σκοπιά της Κβαντικής Θεωρίας της Πληροφορίας. Συγκεκριμένα αποδεικνύουμε ότι η εξέλιξη του αρχικού προβολικού τελεστή-πίνακα πυκνότητας πιθανότητας, δίνει σε κάθε βήμα του αλγόριθμου ένα νέο πίνακα πυκνότητας πιθανότητας, του οποίου το διάνυσμα ιδιοτιμών κατισχύεται από το αντίστοιχο διάνυσμα του προηγούμενου βήματος, γεγονός το οποίο σημαίνει ότι η εξέλιξη του αλγόριθμου αυξάνει την κατά von Neumann εντροπία αυτών των πινάκων. Τέλος, δείχνουμε ότι σε κάθε βήμα, η εντροπία ανταλλαγής η οποία χαρακτηρίζει τον κβαντικό θόρυβο που περιγράφεται από μια πλήρως θετική ιχνοδιατηρητική απεικόνιση, εκφράζεται ως γνωστή συνάρτηση του x, είναι σταθερή σε κάθε βήμα για όσες τιμές του x καταρρέει ο αλγόριθμος, και μηδέν για όσες τιμές επιζεί.

Quantum Search Algorithms in Unstructured Data Bases

ABSTRACT

External influences in the form of quantum noise on Grover's search algorithm are investigated. The study shows that the algorithm can be robust under such external noise. The effect of noise is described by a completely positive trace-preserving map (CP), acting on an unsorted N -dimensional database made of projective density matrices. Explicitly we prove that the resulting search positive map depends on *x*, the strength of the coupling to the noisy environment, and that there are infinitely many *x* values, refered to as *good* and *bad x*'s, for which search it is successful after $O\left(\sqrt{N}\right)$ queries, or fails, respectively. There are two kinds of "good *x*'s", and the remarkable fact at this point is that for the "good *x*'s" of the first kind, the algorithm returns to its classic form, and for the "good *x*'s" of the second kind, the search positive map is reduced to a projective operator.

Next we study the information theoretic aspects of the noisy quantum search algorithm. To this end we view the initial state as a pure qubit signal entering through a cascade of quantum channels, each channel described by a completely positive map, and corresponds to the iterations of the algorithm. This map is identical to the search map of the algorithm as mentioned above, for which the parameter *x*, is now characterizing the influence of the noisy channel exercised upon the incoming

quantum signal. The process of searching is now understood as a transmission of the initial signal/item through the composite channel made by $O\left(\sqrt{N}\right)$, elementary channels. The quality of this transmission corresponds to the fidelity of targeting the wanted item in the quantum database, and is studied also in terms of the quantum entropy of the input-output density matrix, and in terms of the entropy exchanged between the qubit signal/item and an external environment.

We prove the following: first, the evolving ρ density matrix in the course of searching has a vector of eigenvalues that is majorized by the corresponding vector of eigenvalues of the initial density matrix. This implies the algorithm is entropy increasing. Second, the entropy exchange, characterizing the amount of quantum noise introduced by the channel, depends naturally on the parameter *x*, in such a way that for *bad x*'s we have the maximal entropy exchange, making the algorithm to fail, while for *good x*'s, the entropy exchange is zero, and the algorithm succeeds. Therefore for such values of *good x*'s, the transmission channel appears noiseless or otherwise the search algorithm appears to be robust under quantum noise.

Ευχαριστίες

Ευχαριστώ θερμά τον Επιβλέποντα Καθηγητή μου κ. Δημοσθένη Έλληνα,

για την επιστημονική του καθοδήγηση στη συγγραφή αυτής της εργασίας,
για την γενικότερη καθοδήγησή του στον τομέα της επιστήμης των Κβαντικών Υπολογιστών,
για τον απεριόριστο χρόνο που διέθεσε για μένα,
και για την αμέριστη ανθρώπινη συμπαράστασή του σε όλη τη διάρκεια των σπουδών μου.

Επίσης ευχαριστώ θερμά τους Καθηγητές μου και το διοικητικό προσωπικό του Γενικού Τμήματος του Πολυτεχνείου Κρήτης.

Στην μνήμη του πατέρα μου Δημήτρη

και στην μητέρα μου Αλεξάνδρα

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 0: Μαθηματικός Φορμαλισμός

Σελ.

ΚΕΦΑΛΑΙΟ 1: Ο αλγόριθμος του Grover

ΚΕΦΑΛΑΙΟ 2: Κβαντικός θόρυβος στον αλγόριθμο του Grover

ΚΕΦΑΛΑΙΟ 3: Εντροπία von Neumann στην αναζήτηση υπό Κβαντικό θόρυβο

Κεφάλαιο 0

Μαθηματικός φορμαλισμός

0.1. Ορισμοί και θεωρήματα

►Εισαγωγή: Τα τέσσερα αξιώματα της Κβαντομηχανικής

Αξίωμα 1ο :

Κάθε απλό και κλειστό (απομονωμένο) σύστημα στην Κβαντομηχανική περιγράφεται από έναν γραμμικό χώρο πάνω στο σώμα των μιγαδικών αριθμών, ο οποίος λέγεται *χώρος καταστάσεων* του συστήματος. Ως χώρο καταστάσεων χρησιμοποιούμε ένα διαχωρίσιμο μιγαδικό χώρο Hilbert, π.χ. τον $\mathbb{C}^2$. Η κατάσταση του συστήματος αυτού σε μια δεδομένη χρονική στιγμή περιγράφεται από ένα διάνυσμα αυτού του χώρου Hilbert το οποίο καλείται *διάνυσμα κατάστασης*.

Παρατήρηση :

I) Θεωρούμε επίσης και έναν αυτοσυζυγή τελεστή ο οποίος είναι πυκνά ορισμένος σε αυτό το χώρο Hilbert. Ο τελεστής αυτός ονομάζεται *Χαμιλτονιανή* του συστήματος.

II) Επειδή ο παραπάνω χώρος Hilbert είναι διαχωρίσιμος θα περιέχει αριθμήσιμο υποσύνολο του οποίου η κλειστότητα είναι ολόκληρος ο χώρος. Από φυσικής άποψης αυτό μας επιτρέπει με αριθμήσιμες το πλήθος παρατηρήσεις να μπορούμε να ορίσουμε μια κατάσταση με μοναδικό τρόπο.

III) *Ακτίνα* σε ένα χώρο Hilbert ονομάζεται το σύνολο των διανυσμάτων αυτού του χώρου τα οποία είναι όλα βαθμωτά μη μηδενικά μιγαδικά πολλαπλάσια του ίδιου μη μηδενικού διανύσματος. Εάν επιπλέον ο μιγαδικός αυτός συντελεστής έχει μέτρο ίσο με τη μονάδα τότε λέμε ότι τα διανύσματα αυτής της ακτίνας περιγράφουν την ίδια κατάσταση. *Συνεπώς μια κατάσταση είναι ακτίνα σε ένα χώρο Hilbert.*

IV) Οι προβολικοί τελεστές του χώρου Hilbert του συστήματος ονομάζονται *καθαρές καταστάσεις* του συστήματος (pure states).

Αξίωμα 2ο :

Όταν λέμε ότι κάνουμε μια *μέτρηση* στο σύστημα κάποια χρονική στιγμή, εννοούμε ότι δρούμε πάνω στο διάνυσμα της κατάστασής του εκείνη τη χρονική στιγμή με ένα προβολικό τελεστή.

Παρατήρηση :

I) Το αποτέλεσμα της μέτρησης εξάγεται με γνωστή πιθανότητα και η μέτρηση αλλάζει την κατάσταση του συστήματος με τρόπο μη αντιστρέψιμο (αφού πρόκειται για δράση προβολικού τελεστή).

II) Ως *παρατηρήσιμα μεγέθη* ενός συστήματος ορίζονται εκείνα για τα οποία μπορεί να γίνει μέτρηση, και είναι οι αυτοσυζυγείς τελεστές του χώρου Hilbert του συστήματος.

Αξίωμα 3^{o} :

Η χρονική εξέλιξη ενός απλού κλειστού Κβαντομηχανικού συστήματος στο οποίο δεν γίνεται κάποια μέτρηση, περιγράφεται από τη δράση μοναδιακών μετασχηματισμών-τελεστών (unitary operators) πάνω στο διάνυσμα κατάστασης. Ο μοναδιακός τελεστής που περιγράφει την εξέλιξη του συστήματος παράγεται από την Χαμιλτονιανή του συστήματος.

Παρατήρηση :

Επειδή ένας μοναδιακός τελεστής είναι προφανώς αντιστρέψιμος, κάθε προηγούμενη κατάσταση ενός κλειστού Κβαντομηχανικού συστήματος, εάν δεν έχει γίνει μέτρηση, μπορεί να περιγραφεί από τη τρέχουσα. Με άλλα λόγια η ιστορία ενός κλειστού Κβαντομηχανικού συστήματος στο οποίο δεν έχουν γίνει μετρήσεις περιγράφεται από μια Μαρκοβιανή διαδικασία.

Αξίωμα 4^{o} :

Ένα σύνθετο Κβαντομηχανικό σύστημα περιγράφεται από το τανυστικό γινόμενο των αντίστοιχων χώρων Hilbert των επιμέρους απλών ανεξάρτητων συστημάτων του.

Παράδειγμα : Ένα διμερές σύστημα μπορεί να περιγραφεί π.χ. από το γινόμενο $\mathbb{C}^2 \otimes \mathbb{C}^2$ και οι καταστάσεις σε αυτό είναι διανύσματα αυτού του χώρου.

Παρατήρηση :

Η Χαμιλτονιανή ενός διμερούς συστήματος το οποίο περιγράφεται από το γινόμενο $H_1 \otimes H_2$ είναι $\hat{H}_1 \otimes \hat{1} + \hat{1} \otimes \hat{H}_2$, όπου $\hat{H}_1$ και $\hat{H}_2$ είναι οι Χαμιλτονιανές των επί μέρους συστημάτων.

0.1.1. Συμβολισμός Dirac ή συμβολισμός «bra-ket»

Κάθε διάνυσμα κατάστασης στο χώρο Hilbert H που περιγράφει το σύστημα ονομάζεται *"ket"*, συμβολίζεται $|\psi\rangle$ και ισχύει $|\psi\rangle = (c_1, c_2, c_3, \ldots)^{\mathrm{T}}$, όπου c_k, $k = 1, 2, 3, \ldots$ είναι οι συντεταγμένες του διανύσματος κατάστασης σε αυτό το χώρο. Για κάθε "ket" $|\psi\rangle$ ορίζεται και ένα *"bra"* το οποίο συμβολίζεται με $\langle\psi|$. Το "bra" είναι ένα συνεχές γραμμικό συναρτησοειδές ορισμένο στο δυϊκό χώρο H^* του H, με τιμές στους μιγαδικούς αριθμούς, και ορίζεται μέσω του εσωτερικού γινομένου του χώρου Hilbert ως εξής:

$$\langle\psi| : H^* \to \mathbb{C} \text{ ώστε για κάθε } |\delta\rangle \in H \text{ να είναι } \langle\psi|\delta\rangle = \left(|\psi\rangle, |\delta\rangle\right).$$

Παρατηρήσεις :

I) Το "bra" είναι το Ερμητιανό συζυγές του "ket», οπότε αν $|\psi\rangle = (c_1, c_2, c_3, \ldots)^{\mathrm{T}}$, τότε $\langle\psi| = \left(c_1^*, c_2^*, c_2^*, \ldots\right)$.

II) Από το θεώρημα αναπαράστασης του Riesz προκύπτει ότι σε κάθε "bra" αντιστοιχεί ένα μοναδικό "ket".

III) Στην περίπτωση που έχουμε τανυστικό γινόμενο χώρων Hilbert $H_1 \otimes H_2$, για κάθε $|\psi_1\rangle \in H_1$ και $|\psi_2\rangle \in H_2$, ορίζουμε ως *σύνθετο* "ket" να είναι το τανυστικό γινόμενο $|\psi_1\rangle \otimes |\psi_2\rangle$ και το συμβολίζουμε $|\psi_1\rangle|\psi_2\rangle$ ή συχνότερα $|\psi_1\psi_2\rangle$.

0.1.2. Ανάκλαση Householder

Ορισμός 0.1.1. :

Έστω τα κάθετα μεταξύ τους διανύσματα $\vec{u}, \vec{v} \in \mathbb{R}^2$. *Ο γεωμετρικός μετασχηματισμός* I_u *στο επίπεδο των* $\vec{u}, \vec{v}$ *για τον οποίο ισχύουν* $\mathrm{I}_u \vec{u} = -\vec{u}$ *και* $\mathrm{I}_v \vec{v} = \vec{v}$ *έχει πίνακα αναπαράστασης*

$$\mathrm{I}_u = I - \frac{2}{\left\|\vec{u}\right\|^2} \vec{u}(\vec{u})^\dagger$$

και ονομάζεται μετασχηματισμός Householder ως προς το διάνυσμα $\vec{u}$.

Παρατηρήσεις:

I) Γεωμετρικά ο παραπάνω μετασχηματισμός είναι ανάκλαση με άξονα συμμετρίας το φορέα του $\vec{v}$ ο οποίος είναι ευθεία κάθετη στο $\vec{u}$. Για το λόγο αυτό ο I_u καλείται και *ανάκλαση Householder.*

II) Αν επιπλέον θεωρήσουμε ότι το $\vec{u}$ είναι μοναδιαίο, τότε $\mathrm{I}_u = I - 2\vec{u}(\vec{u})^\dagger$, και με χρήση του συμβολισμού bra-ket γράφουμε

$$\mathrm{I}_u = I - 2\left|\vec{u}\right\rangle\left\langle\vec{u}\right|.$$

0.1.3. Γενικευμένη Ανάκλαση Householder

Τα παραπάνω γενικεύονται αν αντί για τον προβολικό τελεστή $\left|\vec{u}\right\rangle\left\langle\vec{u}\right|$ που παράγεται από ένα μοναδιαίο διάνυσμα $\vec{u}$, χρησιμοποιηθεί ο προβολικός τελεστής P που κατασκευάζεται από n το πλήθος γραμμικά ανεξάρτητα και μοναδιαία διανύσματα.

Ορισμός 0.1.2. :

Έστω τα γραμμικά ανεξάρτητα και μοναδιαία διανύσματα $\vec{q_i} \in \mathbb{R}^m$, *με* m, n *θετικοί ακέραιοι,* $m > n$, $i = 1, 2, \ldots, n$ *και ο πίνακας* $A = \left[q_1, q_2, \ldots, q_n\right]$. *Ο προβολικός τελεστής* P *που κατασκευάζεται από αυτά έχει πίνακα αναπαράστασης*

$$P_A = A\left(A^\dagger A\right)^{-1} A^\dagger.$$

Γενικευμένη ανάκλαση Householder καλείται ο μετασχηματισμός με πίνακα αναπαράστασης

$$\mathrm{I}_A = I_m - 2P_A.$$

Παρατήρηση: Η αντίστοιχη γεωμετρική δράση είναι τώρα ανάκλαση ως προς ένα γραμμικό χώρο κάθετο στο χώρο που παράγουν τα $\vec{q_i}$.

0.1.4. Ανάλυση ιδιαζουσών τιμών ενός πίνακα (ανάλυση SVD)

Θεώρημα 0.1. : *Κάθε πίνακας* $A \in M_{m,n}$ *με τάξη* $rank(A) = k$ *μπορεί να γραφεί στην παραγοντοποιημένη μορφή:*

$$A = V\Sigma W^{\dagger}$$

όπου οι πίνακες $V \in M_m$ *και* $W \in M_n$ *είναι μοναδιακοί και ο* Σ *είναι διαγώνιος με* $\sigma_{11} \geq \sigma_{22} \geq \ldots \geq \sigma_{kk} > \sigma_{k+1,k+1} = \ldots = \sigma_{qq} = 0$ *και* $q = \min\{m,n\}$ *.*

Οι μη αρνητικοί αριθμοί σ_{ii} *είναι οι τετραγωνικές ρίζες των ιδιοτιμών του πίνακα* $AA^{\dagger}$ *, και οι στήλες των* V, W *είναι τα ιδιοδιανύσματα των* $AA^{\dagger}$ *και* $A^{\dagger}A$ *αντίστοιχα.*

Παρατηρήσεις:

I) Η παραγοντοποίηση $A = V\Sigma W^{\dagger}$ ονομάζεται *ανάλυση ιδιαζουσών τιμών του* A (ή αλλιώς ανάλυση SVD του A).

II) Τα ιδιοδιανύσματα των $AA^{\dagger}$ και $A^{\dagger}A$ τοποθετούνται ως στήλες των V, W κατ' αντιστοιχία με τις ιδιοτιμές σ_{ii}^2 αυτών & είναι ορθοκανονικό σύνολο διανυσμάτων.

III) Οι μη αρνητικοί αριθμοί σ_{ii} ονομάζονται *ιδιάζουσες τιμές* του A και τα αντίστοιχα ιδιοδιανύσματα των $AA^{\dagger}$ και $A^{\dagger}A$ λέγονται *ιδιάζοντα διανύσματα* του A .

IV) Ο διαγώνιος πίνακας Σ είναι μοναδικός ενώ οι V, W όχι κατ΄ ανάγκη.

V) Κάθε πίνακας $A \in M_{m,n}$ έχει τουλάχιστον μια και το πολύ $q = \min\{m,n\}$ ιδιάζουσες τιμές.

VI) Αν σε μια ιδιάζουσα τιμή αντιστοιχούν περισσότερα από ένα γραμμικά εξαρτημένα ιδιάζοντα διανύσματα, τότε αυτή καλείται *εκφυλισμένη*, ενώ σε αντίθετη περίπτωση καλείται *μη εκφυλισμένη.*

VII) Αν ένας πίνακας A έχει μόνο μη μηδενικές και μη εκφυλισμένες ιδιάζουσες τιμές, τότε η ανάλυση ιδιαζουσών τιμών είναι μοναδική με επιτρεπόμενη ελευθερία ενός πολλαπλασιαστικού παράγοντα της μορφής $e^{i\varphi}$ σε κάποια στήλη του V και συγχρόνως στην αντίστοιχη στήλη του W . Αν όμως ο A έχει εκφυλισμένη ιδιάζουσα τιμή τότε αν και ο Σ είναι μοναδικός η παραγοντοποίηση δεν είναι μοναδική .

VIII) Η ανάλυση ιδιαζουσών τιμών ενός πίνακα είναι μια από τις γενικεύσεις της φασματικής ανάλυσης ενός πίνακα (μια άλλη είναι η παραγοντοποίηση κατά Schur).

0.1.5. Πολική παραγοντοποίηση πίνακα- Πλησιέστερος μοναδιακός ενός πίνακα

Θεώρημα 0.2. : *Κάθε πίνακας* $A \in M_n$ *μπορεί να γραφεί στη μορφή*

$$A = PU$$

όπου ο P *είναι θετικά ημιορισμένος πίνακας και ο* U *είναι μοναδιακός.*

Παρατηρήσεις :

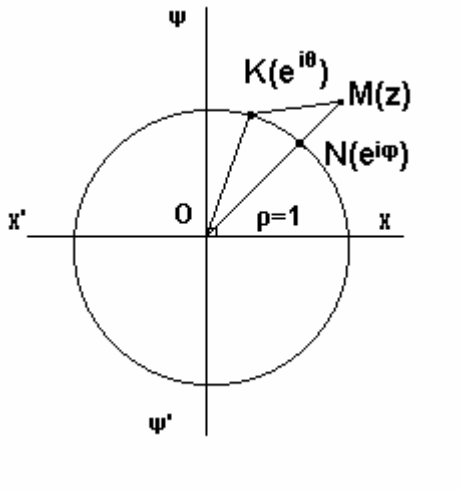
I) Η παραγοντοποίηση $A = PU$ καλείται *πολική παραγοντοποίηση του* A.

II) Ο πίνακας P υπάρχει πάντα και ορίζεται από την ισότητα $P = (AA^{\dagger})^{1/2}$. Αν ο A είναι ομαλός (αντιστρέψιμος), τότε θα αντιστρέφεται και ο P, και συνεπώς ο U θα είναι μοναδικός εξαιτίας της ισότητας $U = P^{-1}A$. Αυτό σημαίνει επίσης ότι η παραγοντοποίηση $A = PU$ θα είναι μοναδική.

III) Γενικά ισχύουν $U = VW^{\dagger}$ και $P = V\Sigma V^{\dagger}$, με V, W να είναι οι μοναδιακοί πίνακες που εμφανίζονται στην SVD ανάλυση του A, και Σ είναι ο αντίστοιχος διαγώνιος πίνακας ιδιαζουσών τιμών.

IV) Αντίστοιχα ισχύουν και οι $A = U'P'$, αλλά τώρα είναι $U' = VW^{\dagger} = U$ και $P' = (A^{\dagger}A)^{1/2}$, $P' = W^{\dagger}\Sigma W$.

V) Η πολική παραγοντοποίηση $A = PU$ είναι το αντίστοιχο της γραφής $z = |z|e^{i\varphi}$ ενός μιγαδικού αριθμού σε πολικές συντεταγμένες. Είναι εύκολο να δειχθεί ότι αν ένας μιγαδικός z απεικονίζεται στο σημείο $M(z)$ στο επίπεδο, τότε από όλους τους μιγαδικούς του μοναδιαίου κύκλου με κέντρο το $O(0,0)$, ο $e^{i\varphi}$ είναι εκείνος με την πλησιέστερη στο $M(z)$ εικόνα.



Ένα αντίστοιχο αποτέλεσμα ισχύει και για ομαλούς πίνακες όπως δείχνουμε στην παρακάτω πρόταση.

Πρόταση 0.1. :

Έστω ομαλός πίνακας $A \in M_n$. Τότε [**14**] *ο πλησιέστερος προς αυτόν μοναδιακός πίνακας είναι αυτός της πολικής παραγοντοποίησης του A.*

Απόδειξη : Επειδή $A \in M_n$ (πεπερασμένης διάστασης) όλες οι norm πινάκων είναι ισοδύναμες. Θα χρησιμοποιήσουμε εκείνη που επάγεται από το ίχνος ενός πίνακα $X \in M_n$, δηλαδή την

$$\|X\| = \sqrt{Tr(XX^\dagger)} \ .$$

Συγκεκριμένα, αρκεί να βρούμε για ποιόν μοναδιακό πίνακα $Q \in M_n$ γίνεται ελάχιστη η μη αρνητική ποσότητα $\|A-Q\|^2$.

Αν ο A είναι μοναδιακός τότε προφανώς ο πλησιέστερος μοναδιακός σε αυτόν είναι ο ίδιος και από την πολική παραγοντοποίησή του έχουμε αμέσως ότι

$$A = (AA^\dagger)^{1/2} U = I^{1/2} U = U \ .$$

Αν ο A δεν είναι μοναδιακός, θα έχουμε ότι:

$$\begin{aligned} \|A-Q\|^2 &= Tr\left\{(A-Q)\left(A^\dagger - Q^\dagger\right)\right\} \\ &= Tr\left(AA^\dagger - QA^\dagger - AQ^\dagger + QQ^\dagger\right) \\ &= Tr\left(AA^\dagger - QA^\dagger - AQ^\dagger + I\right) \\ &= Tr\left(AA^\dagger\right) - Tr\left(QA^\dagger\right) - Tr\left(AQ^\dagger\right) + TrI \end{aligned}$$

ή

$$\boxed{\|A-Q\|^2 = Tr\left(AA^\dagger\right) - 2\Re\mathrm{e}\left[Tr\left(AQ^\dagger\right)\right] + n} \quad (1).$$

Από την ανάλυση ιδιαζουσών τιμών του A έχουμε ότι $A = V\Sigma W^\dagger$ σύμφωνα με τον συμβολισμό του θεωρήματος 0.1, οπότε:

$$\begin{aligned} \Re\mathrm{e}\left[Tr\left(AQ^\dagger\right)\right] &= \Re\mathrm{e}\left[Tr\left(Q^\dagger A\right)\right] \\ &= \Re\mathrm{e}\left[Tr\left(Q^\dagger V\Sigma W^\dagger\right)\right] \\ &= \Re\mathrm{e}\left[Tr\left(W^\dagger Q^\dagger V\Sigma\right)\right] \end{aligned}$$

ή

$$\boxed{\Re\mathrm{e}\left[Tr\left(AQ^\dagger\right)\right] = \Re\mathrm{e}\left[Tr\left(\Psi\Sigma\right)\right]} \ (2), \quad \text{όπου} \ \ \Psi = W^\dagger Q^\dagger V \ .$$

Παρατηρούμε ότι ο πίνακας Ψ είναι μοναδιακός διότι οι V, W, Q είναι μοναδιακοί και

$$\Psi\Psi^\dagger = W^\dagger Q^\dagger V V^\dagger Q W = I \ .$$

Επομένως $Tr\left(\Psi\Psi^\dagger\right) = n$, ή ισοδύναμα $\sum_{i=1}^{n} |\psi|_{ii}^2 = n$ (3). Ακόμα για n τυχαίους μιγαδικούς

$$z_1 = x_1 + y_1 i \ , \ z_2 = x_2 + y_2 i \ , \ \ldots, \ z_n = x_n + y_n i$$

και n τυχαίους μη αρνητικούς $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \geq 0$ ισχύει:

$$\Re\mathrm{e}\left[\sum_{k=1}^{n}\vartheta_k z_k\right]=\sum_{k=1}^{n}\vartheta_k x_k\le\sum_{k=1}^{n}\vartheta_k\left|z\right|_k \quad (4).$$

Η ισότητα θα ισχύει αν και μόνο αν $z_k=x_k\ge 0$ για κάθε $k=1,2,\ldots,n$.

Από τις (2) και (4) έχουμε ότι:

$$\begin{aligned}\Re\mathrm{e}\left[Tr\left(AQ^{\dagger}\right)\right]&=\Re\mathrm{e}\left[Tr\left(\Psi\Sigma\right)\right]\\&=\Re\mathrm{e}\left[\sum_{i=1}^{n}\psi_{ii}\sigma_{ii}\right]\\&\le\sum_{i=1}^{n}\left|\psi_{ii}\right|\sigma_{ii}\quad(5)\qquad(\text{αφού }\sigma_{ii}\ge 0).\end{aligned}$$

Η ισότητα στην (5) ισχύει αν και μόνο αν $\psi_{ii}\ge 0$. Όμως $\Psi\Psi^{\dagger}=I$, οπότε $\psi_{ii}\psi_{ii}^{*}=1$ για κάθε $i=1,2,\ldots,n$, άρα $\psi_{ii}=1$ για κάθε $i=1,2,\ldots,n$. Αυτό σημαίνει ότι αφενός η ελάχιστη τιμή της norm $\left\|A-Q\right\|^2$ είναι :

$$\boxed{\min\left\|A-Q\right\|^2=Tr\left(AA^{\dagger}\right)-2\sum_{i=1}^{n}\sigma_{ii}+n}$$

και αφετέρου ότι αυτό επιτυγχάνεται όταν $\Psi=I$ δηλ. $\Psi=W^{\dagger}Q^{\dagger}V=I$. Από αυτήν και επειδή οι V,W είναι μοναδιακοί έπεται ότι $Q^{\dagger}=WV^{\dagger}$ ή $Q=VW^{\dagger}$ και η ανάλυση ιδιαζουσών τιμών του A θα γίνει:

$$A=V\Sigma W^{\dagger}=\left(V\Sigma V^{\dagger}\right)\left(VW^{\dagger}\right)\quad(6).$$

Σύμφωνα με προηγούμενη παρατήρηση, η (6) είναι πολική παραγοντοποίηση του A και επομένως ο πλησιέστερος προς αυτόν μοναδιακός πίνακας είναι αυτός που προκύπτει από την πολική παραγοντοποίηση του A. Επειδή ακόμα ο A υποτέθηκε ομαλός, η παραπάνω πολική παραγοντοποίηση είναι μοναδική.

0.1.6. Πίνακες Pauli

<u>Ορισμός 0.1.3.</u> :

Πίνακες Pauli ονομάζονται οι παρακάτω τρεις 2x2 πίνακες:

$$\sigma_1=\begin{bmatrix}0&1\\1&0\end{bmatrix},\ \sigma_2=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\ \sigma_3=\begin{bmatrix}1&0\\0&-1\end{bmatrix}.$$

Βασικές ιδιότητες:

1) Είναι Ερμητιανοί και μοναδιακοί.
2) $Tr(\sigma_k)=0$ για $k=1,2,3$.
3) $\det\left(\sigma_k\right)=-1$ για $k=1,2,3$.
4) Είναι οι γεννήτορες της ομάδας $SU\left(2\right)$.
5) $\sigma_k^2=I$ για $k=1,2,3$
6) Σχέσεις μετάθεσης: $\left[\sigma_i,\sigma_j\right]=2i\varepsilon_{ijk}\sigma_k$ με δείκτες $i,j,k\in\left\{1,2,3\right\}$, ενώ ο παράγοντας i στο γινόμενο του δεύτερου μέλους είναι η φανταστική μονάδα. Ο αριθμός ε_{ijk} ονομάζεται σύμβολο Levi-Civita και ισούται με 1 για κάθε άρτια μετάθεση δεικτών, με –1 για κάθε περιττή μετάθεση δεικτών και με μηδέν αν υπάρχουν δυο τουλάχιστον ίσοι δείκτες.

0.1.7. Κατίσχυση (majorization)

Ορισμός 0.1.4. :

Έστω τα διανύσματα $\vec{x}=(x_1,x_2,\ldots,x_n)$ *και* $\vec{y}=(y_1,y_2,\ldots,y_n)$ *του* $\mathbb{R}^n$ *με φθίνουσα διάταξη συντεταγμένων* $x_1\geq x_2\geq\ldots\geq x_n$, $y_1\geq y_2\geq\ldots\geq y_n$. *Θα λέμε ότι το* $\vec{y}$ *κατισχύει του* $\vec{x}$ *(ή ισοδύναμα το* $\vec{x}$ *κατισχύεται από το* $\vec{y}$*) και θα συμβολίζουμε* $\vec{x}\prec\vec{y}$, *αν και μόνο αν ισχύουν οι παρακάτω:*

(α) $\sum_{i=1}^{k}x_i\leq\sum_{i=1}^{k}y_i$, *για κάθε* $k=1,2,\ldots,n-1$

(β) $\sum_{i=1}^{n}x_i=\sum_{i=1}^{n}y_i$.

Παρατηρήσεις και θεωρήματα :

I) Εάν τα $\vec{x}$, $\vec{y}$ δεν έχουν φθίνουσα διάταξη συντεταγμένων τότε αναδιατάσσοντας τις συντεταγμένες τους κατασκευάζουμε τα νέα διανύσματα $x^{\downarrow}=\left(x_1^{\downarrow},x_2^{\downarrow},\ldots,x_n^{\downarrow}\right)$ και $y^{\downarrow}=\left(y_1^{\downarrow},y_2^{\downarrow},\ldots,y_n^{\downarrow}\right)$ ώστε αυτά να έχουν φθίνουσα διάταξη συντεταγμένων. Θα λέμε ότι $\vec{x}\prec\vec{y}$ αν και μόνο αν $x^{\downarrow}\prec y^{\downarrow}$.

II) Εάν ισχύει μόνο η συνθήκη (α) του ορισμού αλλά για κάθε $k=1,2,\ldots,n$, τότε λέμε ότι *το* $\vec{x}$ *κατισχύεται ασθενώς από το* $\vec{y}$ *(ή ότι υπο-κατισχύεται)* και συμβολίζουμε $\vec{x}\prec_w\vec{y}$.

III) Η κατίσχυση $\vec{x}\prec\vec{y}$ σημαίνει διαισθητικά ότι το «$\vec{x}$ περιέχει κατά κάποια έννοια λιγότερη πληροφορία από το $\vec{y}$». Ακολουθούν δυο παραδείγματα με τέτοια διαισθητική ερμηνεία.

IV) Παραδείγματα : Έστω ότι p_j είναι μια κατανομή πιθανότητας σε ένα πεπερασμένο δειγματικό χώρο με n το πλήθος στοιχεία αλλά όχι η ομοιόμορφη. Τότε ισχύει $\left(\frac{1}{n},\frac{1}{n},\ldots,\frac{1}{n}\right)\prec\left(p_1^{\downarrow},p_2^{\downarrow},\ldots,p_n^{\downarrow}\right)$. Η ερμηνεία εδώ είναι ότι στο αριστερό διάνυσμα όλες οι συντεταγμένες έχουν την ίδια «σημασία», ενώ στο δεξιό η πρώτη συντεταγμένη είναι «σημαντικότερη» από τη δεύτερη η οποία είναι «σημαντικότερη» από την τρίτη κλπ. Άρα για το δεξιό διάνυσμα «γνωρίζουμε» κάτι παραπάνω. Το άλλο παράδειγμα προέρχεται από την Γεωμετρία. Ας υποθέσουμε ότι στον ίδιο κύκλο είναι εγγεγραμμένα ένα τετράγωνο και ένα άλλο τετράπλευρο και ότι συνδέουμε το κέντρο του κύκλου με τις κορυφές των δυο σχημάτων. Τότε οι διαδοχικές ακτίνες στο τετράγωνο έχουν μεταξύ τους γωνία $\pi/2$ ενώ στο τετράπλευρο ορίζονται κάποιες άλλες γωνίες $\vartheta_1,\vartheta_2,\vartheta_3,\vartheta_4$. Προφανώς είναι $\left(\frac{\pi}{2},\frac{\pi}{2},\frac{\pi}{2},\frac{\pi}{2}\right)\prec\left(\vartheta_1^{\downarrow},\vartheta_2^{\downarrow},\vartheta_3^{\downarrow},\vartheta_4^{\downarrow}\right)$. Αυτό σημαίνει ότι αν «σταθεί» κανείς στο κέντρο του κύκλου και θέλει να «πάει» στην κορυφή κάποιου σχήματος, στην περίπτωση του τετραγώνου δεν υπάρχει προτίμηση στην επιλογή της διαδρομής αφού όλες είναι ισοδύναμες, πράγμα που δεν συμβαίνει στο άλλο τετράπλευρο.

V) Αν $\vec{x} \prec \vec{y}$ τότε υπάρχει διπλοστοχαστικός πίνακας A ώστε $\vec{x} = A\vec{y}$.

VI) Θεώρημα του Birkhoff : *Το σύνολο των nxn διπλοστοχαστικών πινάκων είναι κυρτό σύνολο και τα ακρότατά του είναι οι πίνακες μετάθεσης* **[5]**.

VII) Αν ο A είναι Ερμητιανός nxn πίνακας, τότε το διάνυσμα των ιδιοτιμών του κατισχύει του διανύσματος των στοιχείων της κυρίας διαγωνίου του.

VIII) Η κατίσχυση είναι μια μερική διάταξη στο σύνολο $\mathbb{R}^n$.

Ορισμός 0.1.5. : *Μια συνάρτηση $\varphi : \mathbb{R}^n \to \mathbb{R}$ ονομάζεται*

(α) Κυρτή κατά Schur [5] *αν και μόνο αν για κάθε $\vec{x}, \vec{y} \in \mathbb{R}^n$ με $\vec{x} \prec \vec{y}$ είναι*

$$\varphi\left(\vec{x}\right) \le \varphi\left(\vec{y}\right).$$

(β) Κοίλη κατά Schur αν και μόνο αν η $-\varphi$ είναι κυρτή κατά Schur, δηλαδή αν και μόνο αν για κάθε $\vec{x}, \vec{y} \in \mathbb{R}^n$ με $\vec{x} \prec \vec{y}$ είναι

$$\varphi\left(\vec{x}\right) \ge \varphi\left(\vec{y}\right).$$

0.1.8. Qubit

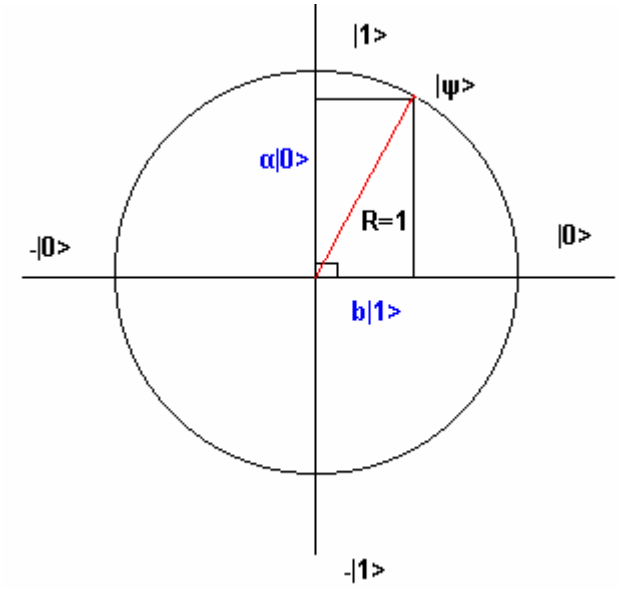
Στην Κλασική Θεωρία της Πληροφορίας, ο βασικός πόρος πληροφορίας είναι το μπιτ (bit από τις λέξεις binary digit) το οποίο μπορεί να βρίσκεται σε μια μόνο από δυο διακριτές καταστάσεις, δηλαδή παίρνει πάντα μια από τις τιμές 0 και 1. Αντίθετα, στην Κβαντική Πληροφορία, η μονάδα πληροφορίας ονομάζεται κβαντικό μπιτ (qubit ή qbit από το quantum bit) και μπορεί να βρίσκεται σε καταστάσεις στις οποίες είναι ταυτόχρονα παρόντα το 0 και 1. Μια τέτοια κατάσταση λέγεται *υπέρθεση (superposition)*. Όταν γίνει μέτρηση το qbit παίρνει μια από τις τιμές 0 και 1 με κάποια γνωστή πιθανότητα αλλά η προηγούμενη κατάσταση υπέρθεσης καταστρέφεται και δεν ανακτάται. Επίσης είναι δυνατόν ομάδες από qbit να έχουν την ιδιότητα του *«συσχετισμού» ή «διαπλοκής» (entanglement)* από την οποία προκύπτουν παράδοξα που αντίκεινται στην ανθρώπινη διαίσθηση (παράδοξο EPR).

Ορισμός 0.1.6. :

Έστω ένας διδιάστατος χώρος Hilbert $H = \langle |0\rangle, |1\rangle \rangle$ με ορθοκανονική βάση $B = \{|0\rangle, |1\rangle\}$. Ονομάζουμε qbit κάθε διάνυσμα $|\psi\rangle \in H$ της μορφής $|\psi\rangle = a|0\rangle + b|1\rangle$, με $a, b \in \mathbb{C}$ ώστε να ισχύει $|a|^2 + |b|^2 = 1$.

Παρατήρηση :

Στο επόμενο σχήμα φαίνεται μια διδιάστατη αναπαράσταση ενός qbit $|\psi\rangle = a|0\rangle + b|1\rangle$ στο επίπεδο που ορίζουν τα ορθοκανονικά διανύσματα $|0\rangle, |1\rangle$.



0.1.9. Πίνακας πυκνότητας

Έχουμε πει ότι η κατάσταση ενός κβαντικού συστήματος είναι μια ακτίνα σε ένα χώρο Hilbert και ότι ένα κβαντικό σύστημα μπορεί να βρίσκεται ταυτόχρονα σε περισσότερες από μια καταστάσεις με κάποια πιθανότητα να βρεθεί σε κάθε μια από αυτές. Ο *πίνακας πυκνότητας* είναι ένα Μαθηματικό εργαλείο το οποίο αφενός μεταφέρει πλήρως την πληροφορία για τις δυνατές καταστάσεις ενός συστήματος, και αφετέρου είναι ιδιαίτερα αποτελεσματικό διότι η μελέτη ανάγεται πλέον σε χώρους τελεστών οι οποίοι έχουν γνωστές ιδιότητες και ιδιαίτερα πλούσια θεωρία.

Ορισμός 0.1.7. :

Έστω ένα διμερές σύστημα το οποίο αποτελείται από δυο qbits A, B *για τα οποία οι αντίστοιχες ορθοκανονικές βάσεις των χώρων Hilbert* H_A, H_B *είναι οι* $\{|0\rangle_A, |1\rangle_A\}$ *και* $\{|0\rangle_B, |1\rangle_B\}$. *Έστω επίσης μια κατάσταση* $|\psi\rangle_{AB} = a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B$ *σε αυτό το σύστημα. Τελεστής πυκνότητας ή πίνακας πυκνότητας για το qbit* A *ορίζεται ο τελεστής*

$$\boxed{\rho_A = |a|^2 |0\rangle_A \langle 0| + |b|^2 |1\rangle_A \langle 1|}$$

Παρατηρήσεις :

i) Ο πιο γενικός πίνακας πυκνότητας που μπορεί να οριστεί σε ένα χώρο Hilbert, άρα σε ένα κβαντικό σύστημα, είναι ο $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$, με $p_j \geq 0$ και $\sum_j p_j = 1$.

ii) Ο πίνακας πυκνότητας αντιπροσωπεύει στατιστικά την ανάμιξη καθαρών καταστάσεων και έχει στην Κβαντομηχανική την αντίστοιχη θέση με αυτήν που έχει η πυκνότητα πιθανότητας στην κλασική Στατιστική Μηχανική. Εάν είναι διαγώνιος πίνακας τότε τα στοιχεία της κυρίας διαγωνίου είναι οι τιμές της κλασικής πυκνότητας πιθανότητας.

iii) Είναι αυτοσυζυγής (Ερμητιανός), θετικός, έχει μη αρνητικές ιδιοτιμές και ίχνος ίσο με 1.

iv) Έστω ότι μια κατάσταση σε ένα χώρο Hilbert γράφεται ως $|\psi_\kappa\rangle = \sum_\kappa a_\kappa |j_\kappa\rangle$, με $\{|j_\kappa\rangle\}_{\kappa\in I}$ να είναι μια ορθοκανονική βάση αυτού του χώρου. Τότε η γενικότερη μορφή του πίνακα πυκνότητας είναι :

$$\rho = \begin{pmatrix} |a_1|^2 & a_1 a_2^* & a_1 a_3^* & \vdots \\ a_2 a_1^* & |a_2|^2 & a_2 a_3^* & \vdots \\ a_3 a_1^* & a_3 a_2^* & |a_3|^2 & \vdots \\ \cdots & \cdots & \cdots & \ddots \end{pmatrix} .$$

v) Μια κατάσταση είναι καθαρή αν και μόνο αν ο πίνακας πυκνότητας είναι προβολικός τελεστής, συνεπώς $\rho = |\psi\rangle\langle\psi|$ και $Tr(\rho^2) = 1$, ενώ θα είναι μικτή αν και μόνο αν είναι κυρτός συνδυασμός καθαρών καταστάσεων, δηλαδή $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$, $p_j \geq 0$, $\sum_j p_j = I$.

0.1.10. Σφαίρα του Bloch

Κάθε 2x2 μιγαδικός Ερμητιανός πίνακας ρ με ίχνος ίσο με 1, έχει τέσσερις ανεξάρτητες πραγματικές παραμέτρους και συνεπώς εκφράζεται από τη βάση $B = \{\sigma_1, \sigma_2, \sigma_3, I\}$ ως

$$\rho(\vec{\lambda}) = \frac{1}{2}\left(I + \sum_{\kappa=1}^{3} \lambda_\kappa \sigma_\kappa\right) \equiv \frac{1}{2}\left(I + \vec{\lambda}\cdot\vec{\sigma}\right)$$
$$= \frac{1}{2}\begin{bmatrix} 1+\lambda_3 & \lambda_1 - i\lambda_2 \\ \lambda_1 + i\lambda_2 & 1-\lambda_3 \end{bmatrix}, \text{ με } \vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)^T \text{ και } \vec{\lambda} = (\lambda_1, \lambda_2, \lambda_3)^T .$$

Ακόμα, επειδή το ίχνος του είναι ίσο με 1, η ικανή και αναγκαία συνθήκη για να έχει μη αρνητικές ιδιοτιμές είναι $|\vec{\lambda}|^2 \leq 1$. Έτσι ορίζεται μια «1-1» και επί απεικόνιση μεταξύ όλων των δυνατών πινάκων πυκνότητας και των σημείων της μοναδιαίας μπάλας.

<u>Ορισμός 0.1.7.</u> ***:***

Σε κάθε σημείο $M(\lambda_1, \lambda_2, \lambda_3)$ της μοναδιαίας μπάλας αντιστοιχίζουμε τον πίνακα πυκνότητας

$$\rho(\vec{\lambda}) = \frac{1}{2}\left(I + \vec{\lambda}\cdot\vec{\sigma}\right).$$

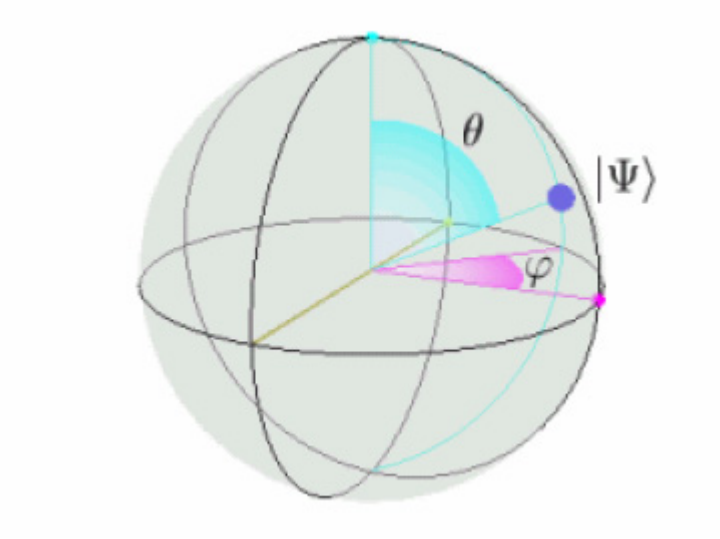
Η αντιστοίχιση αυτή είναι «1-1» και επί, και η μοναδιαία μπάλα εφοδιασμένη με αυτή την αντιστοίχιση ονομάζεται σφαίρα του Bloch.

<u>Παρατηρήσεις</u> :

I) Στην επιφάνεια της μπάλας απεικονίζονται μόνο όσοι πίνακες πυκνότητας έχουν $|\vec{\lambda}| = 1$. Αφού όμως έχουν ίχνος ίσο με 1, οι ιδιοτιμές τους θα είναι το 0 και το 1, άρα θα είναι οι μονοδιάστατοι προβολικοί τελεστές ή αλλιώς οι καθαρές καταστάσεις.

II) Ένα qbit αναπαριστάνεται τρισδιάστατα στη σφαίρα του Bloch [**15**] όπως φαίνεται στο παρακάτω σχήμα διότι μπορεί να γραφεί στην μορφή

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



0.1.11. Μερικό ίχνος (Partial Trace) και CPTP

Η έννοια του μερικού ίχνους ως προς κάποιο χώρο γραμμικών τελεστών είναι μια επέκταση της γνωστής έννοιας του ίχνους πίνακα σε χώρους γραμμικών τελεστών αλλά με μια αξιοσημείωτη ποιοτική διαφορά: ενώ το ίχνος ενός πίνακα είναι ένας μιγαδικός αριθμός(βαθμωτό μέγεθος), το *μερικό ίχνος είναι ένας γραμμικός τελεστής*. Στην σχετική βιβλιογραφία το μερικό ίχνος ορίζεται ξεχωριστά για χώρους γραμμικών τελεστών πεπερασμένης και άπειρης διάστασης. Στην περίπτωση πεπερασμένης διάστασης ακολουθούνται δυο ισοδύναμοι ορισμοί. Ο πρώτος ορίζει το μερικό ίχνος χρησιμοποιώντας βάσεις διανυσματικών χώρων και ο δεύτερος χρησιμοποιώντας μόνο γραμμικούς τελεστές. Θα δώσουμε πρώτα αυτούς τους δυο ορισμούς και κατόπιν τον ορισμό για την περίπτωση άπειρης διάστασης.

<u>Ορισμός 0.1.8.</u> (1ος ορισμός του μερικού ίχνους)

Έστω V *και* W *δυο γραμμικοί χώροι πεπερασμένης διάστασης με* $\dim V = m$, $\dim W = n$, *αντίστοιχες βάσεις* $B_V = \{v_1, v_2, \cdots, v_m\}$, $B_W = \{w_1, w_2, \cdots, w_n\}$ *και αντίστοιχους χώρους γραμμικών τελεστών* $L(V)$ *και* $L(W)$. *Έστω επίσης τελεστής* $T \in L(V \otimes W)$ *ο οποίος έχει πίνακα αναπαράστασης* $\{a_{kl,ij}\}$ *με* $1 \le k, i \le m$ *και* $1 \le l, j \le n$ *ως προς τη βάση* $v_k \otimes w_l$ *του* $V \otimes W$. ***Μερικό ίχνος ως προς τον χώρο*** V *ονομάζεται η απεικόνιση*

$$Tr_V : L(V \otimes W) \to L(W)$$

$$L(V \otimes W) \ni T \mapsto Tr_V(T) \in L(W)$$

ώστε ο τελεστής $Tr_V(T)$ *να έχει πίνακα αναπαράστασης* M *του οποίου τα στοιχεία ορίζονται από το άθροισμα*

$$M_{k,i} = \sum_{j=1}^{n} a_{kj,ij} \qquad \text{με } 1 \le k, i \le m.$$

<u>Παρατηρήσεις</u> :

I) Αν και ο πίνακας του γραμμικού τελεστή του χώρου W που προκύπτει από την παραπάνω διαδικασία εξαρτάται από τις βάσεις των αρχικών χώρων, από την Γραμμική Άλγεβρα γνωρίζουμε ότι ο επαγόμενος γραμμικός τελεστής είναι ανεξάρτητος της επιλογής των βάσεων.

II) Αντίστοιχα ορίζεται το μερικό ίχνος ως προς τον χώρο W.

Ορισμός 0.1.9. **(2ος ορισμός του μερικού ίχνους)**

Έστω V *και* W *δυο γραμμικοί χώροι πεπερασμένης διάστασης και* $V \otimes W$ *το τανυστικό τους γινόμενο.* ***Μερικό ίχνος ως προς τον χώρο*** V *ονομάζεται ο μοναδικός γραμμικός τελεστής*

$$Tr_V : L(V \otimes W) \to L(W)$$

για τον οποίο για κάθε $\mathrm{X} \in V$ *και για κάθε* $\Psi \in W$ *ισχύει ότι:*

$$Tr_V(\mathrm{X} \otimes \Psi) = \Psi Tr(\mathrm{X}).$$

Παρατηρήσεις :

i) Αντίστοιχα ορίζεται το μερικό ίχνος ως προς τον χώρο W .

ii) Τα παραπάνω γενικεύονται εύκολα για γινόμενο περισσότερων χώρων: ας υποθέσουμε ότι έχουμε $n \in \mathbb{N}$ το πλήθος γραμμικούς χώρους, τους V_i με $i = 1, 2, \ldots, n$ και το τανυστικό τους γινόμενο

$$\bigotimes_{i=1}^{n} V = V_1 \otimes V_2 \otimes \ldots \otimes V_n .$$

Μερικό ίχνος ως προς τον γραμμικό χώρο V_k ονομάζεται ο μοναδικός γραμμικός τελεστής

$Tr_{V_k} : L\left(\bigotimes_{i=1}^{n} V\right) \to L(V_1 \otimes V_2 \otimes \ldots \otimes V_{k-1} \otimes V_{k+1} \otimes \ldots \otimes V_n)$ για τον οποίο για κάθε $X_i \in V_i$ ισχύει ότι:

$$Tr_{V_k}\left(\bigotimes_{i=1}^{n} X_i\right) = Tr(X_k)(X_1 \otimes X_2 \otimes \ldots \otimes X_{k-1} \otimes X_{k+1} \otimes \ldots \otimes X_n).$$

iii) Κατ' αντιστοιχία με την γνωστή κυκλική ιδιότητα του ίχνους $Tr(AB) = Tr(BA)$, έχουμε την ισότητα:

$Tr_V(T(I_V \otimes X)) = Tr_V((I_V \otimes X)T)$, με $X \in W$, $T \in L(V \otimes W)$.

iv) Σύμφωνα με τον ορισμό, σε ένα διμερές σύστημα που περιγράφεται από το τανυστικό γινόμενο χώρων Hilbert $H_A \otimes H_B$, θα ισχύει ότι:

$$Tr_A(|x_1\rangle\langle x_2| \otimes |y_1\rangle\langle y_2|) = |y_1\rangle\langle y_2| Tr(|x_1\rangle\langle x_2|).$$

v) Αν σε ένα διμερές σύστημα $H_A \otimes H_B$, είναι $|\psi\rangle_{AB} = \sum_{i,m} a_{im} |i\rangle \otimes |m\rangle$, $\sum_{i,m} |a_{im}|^2 = 1$, και $\{|i\rangle_A\}, \{|i\rangle_B\}$ $i = 0, 1$, είναι ορθοκανονικές βάσεις των H_A, H_B αντίστοιχα, τότε από την προηγούμενη παρατήρηση προκύπτει ότι:

$$\boxed{Tr_B(|\psi\rangle_{AB\,AB}\langle\psi|) = \sum_{i,j,m} a_{im} a^*_{jm} |i\rangle_{A\,A}\langle j|}.$$

► **Μερικό ίχνος σε τανυστικό γινόμενο απειροδιάστατων χώρων Hilbert**

Έστω ότι V και W είναι δυο χώροι Hilbert άπειρης διάστασης, $V \otimes W$ το τανυστικό τους γινόμενο, και $\{w_i\}$ μια βάση του W . Από την Συναρτησιακή Ανάλυση γνωρίζουμε ότι κάθε

γραμμικός τελεστής $T \in L(V \otimes W)$ μπορεί να αναπαρασταθεί με έναν απειροδιάστατο πίνακα γραμμικών τελεστών με στοιχεία $T_{ij} \in W$, της μορφής

$$\begin{bmatrix} T_{11} & T_{12} & \cdots \\ T_{21} & T_{22} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}.$$

Σύμφωνα με τον παραπάνω συμβολισμό έχουμε τον ορισμό:

Ορισμός 0.1.10.

Α) Αν ο T είναι μη αρνητικός γραμμικός τελεστής του $L(V \otimes W)$ και $\sum T_{kk}$ συγκλίνει στον $L(W)$ κατά την ισχυρή τελεστική τοπολογία S.O.T. (Strong Operator Topology) σε κάποιον $R \in L(W)$, τότε ορίζουμε

$$Tr_V(T) = \sum T_{kk} = R.$$

Με ανάλογο τρόπο ορίζεται το μερικό ίχνος μη θετικού γραμμικού τελεστή του $L(V \otimes W)$.

Β) Αν ο T είναι αυτοσυζυγής τελεστής, με T^+, T^- θετικό και αρνητικό μέρος αντίστοιχα, τότε το μερικό ίχνος ορίζεται αν και μόνο αν ορίζονται τα $Tr_V(T^+), Tr_V(T^-)$, και $Tr_V(T)$ ορίζεται να είναι ο τελεστής του $L(W)$ που έχει τα $Tr_V(T^+), Tr_V(T^-)$ ως θετικό και αρνητικό μέρος αντίστοιχα.

Παρατήρηση :

Επειδή το άθροισμα $\sum T_{kk}$ συγκλίνει στον $L(W)$ κατά την S.O.T., έπεται ότι ο R είναι ανεξάρτητος της βάσης του W.

► **Μια θεμελιώδης εφαρμογή του μερικού ίχνους στην Κβαντομηχανική**

Έστω ότι σε ένα απλό σύστημα έχουμε ένα qbit $|\psi\rangle = a|0\rangle + b|1\rangle$ με πίνακα πυκνότητας $\rho = |a|^2 |0\rangle\langle 0| + |b|^2 |1\rangle\langle 1|$, και ένα παρατηρήσιμο μέγεθος M. Στην Κβαντομηχανική, η αναμενόμενη τιμή του M είναι εξ' ορισμού ίση με :

$$\begin{aligned} \langle M \rangle &= \langle \psi | M | \psi \rangle \\ &= \left(a^* \langle 0| + b^* \langle 1|\right) M \left(a|0\rangle + b|1\rangle\right) \\ &= |a|^2 \langle 0|M|0\rangle + |b|^2 \langle 1|M|1\rangle \\ &= \sum_{i=1,2} a_{ii} \langle i|M|i\rangle \qquad \text{με } a_{11} = |a|^2 \text{ και } a_{22} = |b|^2 \end{aligned}$$

ή

$$\langle M \rangle = Tr(M \cdot \rho) \quad (1) \qquad \text{αφού } \rho = |a|^2 |0\rangle\langle 0| + |b|^2 |1\rangle\langle 1|.$$

Ας υποθέσουμε τώρα ότι έχουμε ένα διμερές σύστημα που περιγράφεται από το τανυστικό γινόμενο χώρων Hilbert $H_A \otimes H_B$ με $\{|i\rangle_A\}, \{|i\rangle_B\}$, $i = 0,1$ να είναι ορθοκανονικές βάσεις των H_A, H_B αντίστοιχα, και μια κατάσταση

$$\left|\psi\right\rangle_{AB} = \sum_{i,m} a_{im} \left|i\right\rangle \otimes \left|m\right\rangle, \text{ με } \sum_{i,m} \left|a_{im}\right|^2 = 1 \ .$$

Ένα παρατηρήσιμο μέγεθος M_A μόνο στο πρώτο υποσύστημα θα είναι το παρατηρήσιμο $M_A \otimes I$ στο διμερές. Αφού το μέγεθος M_A εμπλέκει μόνο το πρώτο υποσύστημα είναι λογικό να περιμένουμε ότι η αναμενόμενη τιμή του θα ικανοποιεί μια ισότητα όπως η (1) στην οποία το εμφανιζόμενο ρ να είναι ο πίνακας πυκνότητας μόνο του πρώτου qbit.

Περιμένουμε δηλαδή να ισχύει μια ισότητα της μορφής:

$$\left\langle M_A \right\rangle = Tr\left(M_A \cdot \rho_A\right) \text{ (2).}$$

Υπολογίζουμε τη αναμενόμενη τιμή του M_A κατά τα γνωστά:

$$\begin{aligned}
\left\langle M_A \right\rangle &= {}_{AB}\left\langle \psi \right| \left(M_A \otimes I\right) \left|\psi\right\rangle_{AB} \\
&= \left(\sum_{j,n} a^*_{jnA} \left\langle j\right| \otimes {}_B \left\langle n\right|\right)\left(M_A \otimes I\right)\left(\sum_{i,m} a_{im} \left|i\right\rangle_A \otimes \left|m\right\rangle_B\right) \\
&= \sum_{i,j,m} a^*_{jm} a_{imA} \left\langle j\right| M_A \left|i\right\rangle_A \\
&= Tr\left(M_A \cdot \rho_A\right), \text{ όπου} \\
\rho_A &= \sum_{i,j,m} a_{im} a^*_{jm} \left|i\right\rangle_{AA} \left\langle j\right|.
\end{aligned}$$

Σύμφωνα με προηγούμενη παρατήρηση θα είναι:

$$\boxed{\rho_A = Tr_B\left(\left|\psi\right\rangle_{AB\,AB} \left\langle\psi\right|\right)}.$$

Αξίζει να σημειωθεί επίσης ότι από τις ιδιότητες του μερικού ίχνους έπεται ότι ο παραπάνω πίνακας πυκνότητας είναι μοναδικός.

► Υπερτελεστές-πλήρως θετικές ιχνοδιατηρητικές απεικονίσεις

Έστω τώρα ότι στο προηγούμενο διμερές σύστημα $H_A \otimes H_B$ δεν γίνεται κάποια μέτρηση. Τότε όπως γνωρίζουμε, η χρονική του εξέλιξη θα περιγράφεται από τη δράση κάποιου μοναδιακού τελεστή πάνω στο διάνυσμα κατάστασης. Ένα σημαντικό ερώτημα που μπορεί να τεθεί εδώ είναι το πώς θα μπορούσαμε να περιγράψουμε αυτόνομα την εξέλιξη ενός υποσυστήματος, π.χ. του A. Για το σκοπό αυτό αρκεί να εξετάσουμε το πώς θα εξελιχθεί ένας πίνακας πυκνότητας του πρώτου συστήματος. Ας υποθέσουμε ότι αρχικά ο πίνακας πυκνότητας του A είναι ρ_A και ότι το δεύτερο υποσύστημα βρίσκεται σε καθαρή κατάσταση η οποία προκύπτει από το $\left|0\right\rangle_B$. Τότε το διμερές σύστημα περιγράφεται από τον πίνακα πυκνότητας $\rho_A \otimes \left|0\right\rangle_{BB}\left\langle 0\right|$ και η εξέλιξη του συστήματος ύστερα από πεπερασμένο χρόνο θα περιγράφεται από τον τελεστή $U_{AB}\left(\rho_A \otimes \left|0\right\rangle_{BB}\left\langle 0\right|\right)U^\dagger_{AB}$, με U_{AB} μοναδιακός. Άρα ο τελικός πίνακας πυκνότητας του A θα είναι:

$$\begin{aligned}
\rho'_A &= Tr_B\left(U_{AB}\left(\rho_A \otimes \left|0\right\rangle_{BB}\left\langle 0\right|\right)U^\dagger_{AB}\right) \\
&= \sum_m \left({}_B\left\langle m\right| U_{AB} \left|0\right\rangle_B\right) \rho_A \left({}_B\left\langle 0\right| U^\dagger_{AB} \left|m\right\rangle_B\right)
\end{aligned}$$

ή

$$\boxed{\rho'_A = \sum_m M_m \rho_A M^\dagger_m}, \quad \text{με } M_m = {}_B\left\langle m\right| U_{AB} \left|0\right\rangle_B.$$

Αφού ο U_{AB} είναι μοναδιακός και οι βάσεις των χώρων ορθοκανονικές, για τους τελεστές $M_m = {}_B\left\langle m\right| U_{AB} \left|0\right\rangle_B$ του δεύτερου χώρου θα ισχύει:

$$\sum_m M^\dagger_m M_m = \sum_m {}_B\left\langle 0\right| U^\dagger_{AB} \left|m\right\rangle_{BB} \left\langle m\right| U_{AB} \left|0\right\rangle_B$$

$$= {}_B\left\langle 0 \middle| U_{AB}^{\dagger} U_{AB} \middle| 0 \right\rangle_B$$

ή

$$\sum_m M_m^{\dagger} M_m = 1 \quad (3).$$

Παρατηρούμε ότι και ο ρ'_A είναι πίνακας πυκνότητας διότι:

- είναι Ερμητιανός αφού ο ρ_A είναι Ερμητιανός:

$$\begin{aligned}\left(\rho'_A\right)^{\dagger} &= \left(\sum_m M_m \rho_A M_m^{\dagger}\right)^{\dagger} \\ &= \sum_m \left(M_m^{\dagger}\right)^{\dagger} \rho_A^{\dagger} M_m^{\dagger} \\ &= \sum_m M_m \rho_A M_m^{\dagger} \\ &= \rho_A .\end{aligned}$$

- είναι μη αρνητικός διότι και ο ρ_A είναι μη αρνητικός:

$${}_A\left\langle \psi \middle| \rho'_A \middle| \psi \right\rangle_A = \sum_m \left({}_A\left\langle \psi \middle| M_m \right) \rho_A \left(M_m^{\dagger} \middle| \psi \right\rangle_A \right) \geq 0$$

- έχει ίχνος ίσο με ένα αφού ο ρ_A έχει ίχνος ίσο με ένα, ισχύει η (3) και η κυκλική ιδιότητα του ίχνους:

$$\begin{aligned}Tr\rho'_A &= Tr\left(\sum_m M_m \rho_A M_m^{\dagger}\right) \\ &= \sum_m Tr\left(M_m \rho_A M_m^{\dagger}\right) \\ &= \sum_m Tr\left(\rho_A M_m^{\dagger} M_m\right) \\ &= Tr\left(\sum_m \rho_A M_m^{\dagger} M_m\right) \\ &= Tr\left(\rho_A \sum_m M_m^{\dagger} M_m\right) \\ &= Tr\rho_A \\ &= 1\end{aligned}$$

Ορισμός 0.1.11.

Έστω H_A, H_B δυο χώροι Hilbert. Μια θετική γραμμική απεικόνιση $S : L\left(H_A\right) \to L\left(H_A\right)$ ονομάζεται πλήρως θετική στον H_A αν και μόνο αν η απεικόνιση

$$S \otimes I_B : L\left(H_A \otimes H_B\right) \to L\left(H_A \otimes H_B\right)$$

είναι θετική για κάθε χώρο Hilbert H_B, δηλαδή για κάθε επέκταση του H_A σε $H_A \otimes H_B$.

Ορισμός 0.1.12.

Αν H_A είναι χώρος Hilbert και $M_m \in L\left(H_A\right)$ ώστε να ισχύει $\sum_m M_m^{\dagger} M_m = 1$, η απεικόνιση

$$E\left(\rho_A\right) : L\left(H_A\right) \to L\left(H_A\right)$$

$$L\left(H_A\right) \ni \rho_A \mapsto E\left(\rho_A\right) = \rho'_A = \sum_m M_m \rho_A M_m^{\dagger} \in L\left(H_A\right)$$

καλείται:

I) αθροιστική τελεστική αναπαράσταση

II) υπερτελεστής ή πλήρως θετική ιχνοδιατηρική απεικόνιση (Completely Positive Trace Preserving linear map ή CPTP) εάν επιπλέον είναι και πλήρως θετική στον χώρο H_A.

Παρατηρήσεις :

I) Οι τελεστές $M_m \in L(H_A)$ με $M_m = {}_B\langle m|U_{AB}|0\rangle_B$ ονομάζονται *τελεστές του Kraus*, ή *γεννήτορες* του CPTP $E(\rho_A)$ και η ισότητα $\sum_m M_m^\dagger M_m = 1$ καλείται *συνθήκη Kraus* [**13**].

II) Όπως είδαμε παραπάνω, η διατήρηση του ίχνους οφείλεται στην συνθήκη Kraus.

► Αναπαράσταση τυχαίου CPTP

Από την προηγούμενη συζήτηση για τους υπερτελεστές και τις πλήρως θετικές ιχνοδιατηρητικές απεικονίσεις προκύπτει ότι αν θέλουμε να αναπαραστήσουμε ένα τυχαίο CPTP, έστω το $E(\rho_A)$, υπάρχουν δυο επιλογές:

I) Είτε να χρησιμοποιήσουμε τελεστές μόνο από τον πρώτο χώρο A, οπότε χρησιμοποιούμε τους τελεστές Kraus και την:
$$E(\rho_A) = \sum_m M_m \rho_A M_m^\dagger .$$

II) Είτε να κάνουμε μια επέκταση σε ένα βοηθητικό χώρο-περιβάλλον B (ancilla), οπότε πάντα θα υπάρχει κάποιος μοναδιακός τελεστής U_{AB} του διμερούς χώρου για τον οποίο θα είναι
$$E(\rho_A) = Tr_B\left(U_{AB}\left(\rho_A \otimes |0\rangle_{BB}\langle 0|\right)U_{AB}^\dagger\right).$$
Η ύπαρξη αυτού του μοναδιακού τελεστή εξασφαλίζεται από το θεώρημα του Stinespring [**12**] σύμφωνα με το οποίο αν
$$E : L(H_A) \to L(H_A)$$
είναι ένα CPTP σε έναν πεπερασμένης διάστασης χώρο Hilbert H_A, τότε υπάρχουν χώρος Hilbert H_B με $\dim(H_B) \le \dim^2(H_A)$ και μοναδιακός τελεστής U_{AB} του $H_A \otimes H_B$, ώστε για κάθε πίνακα πυκνότητας $\rho_A \in L(H_A)$ να ισχύει
$$E(\rho_A) = Tr_B\left(U_{AB}\left(\rho_A \otimes |0\rangle_{BB}\langle 0|\right)U_{AB}^\dagger\right).$$

► Αλγεβρική κλειστότητα στο σύνολο των CPTP

Μια άλλη αξιοσημείωτη ιδιότητα των πλήρως θετικών ιχνοδιατηρητικών απεικονίσεων είναι ότι αν το σύνολο των CPTP του ίδιου χώρου $L(H)$ εφοδιαστεί με την πράξη της σύνθεσης συναρτήσεων είναι αλγεβρικά κλειστό όπως θα δείξουμε ευθύς αμέσως.

Πράγματι, έστω δυο CPTP του χώρου $L(H)$, τα E, F με γεννήτορες Kraus $\{M_m\}$, $m \in \mathrm{I}_1$ και $\{N_l\}$, $l \in \mathrm{I}_2$ αντίστοιχα. Γνωρίζουμε ότι για κάθε πίνακα πυκνότητας ρ_A του $L(H)$ ο $\rho'_A = E(\rho_A)$ είναι επίσης ένας πίνακας πυκνότητας, άρα ορίζεται $F(\rho'_A) = F(E(\rho_A))$ και επομένως η σύνθεση $F \circ E$ ορίζεται στον $L(H)$. Θα είναι:
$$\begin{aligned}(F \circ E)(\rho_A) &= F(E(\rho_A)) \\ &= \sum_l N_l\left(E(\rho_A)\right)N_l^\dagger \\ &= \sum_l N_l\left(\sum_m M_m \rho_A M_m^\dagger\right)N_l^\dagger\end{aligned}$$

$$= \sum_{l,m} \left(N_l M_m \right) \rho_A \left(N_l M_m \right)^\dagger$$
$$= \sum_k R_k \rho_A R_k^\dagger \qquad \text{με } R_k = N_l M_m \ , \ k \in \mathrm{I}_1 \bigcup \mathrm{I}_2 \, ,$$

και επίσης

$$\sum_k R_k^\dagger R_k = \sum_{l,m} \left(N_l M_m \right)^\dagger N_l M_m$$
$$= \sum_{l,m} M_m{}^\dagger N_l{}^\dagger N_l M_m$$
$$= \sum_m M_m{}^\dagger \left(\sum_l N_l{}^\dagger N_l \right) M_m$$
$$= \sum_m M_m{}^\dagger M_m$$
$$= I \, .$$

Άρα η σύνθεση $F \circ E$ είναι επίσης CPTP στον ίδιο χώρο, το οποίο είναι και το ζητούμενο.

0.1.12. Η εντροπία στην Κλασική και στην Κβαντική Θεωρία Πληροφορίας

Ιστορικά, η γέννηση της Κλασικής Θεωρίας της Πληροφορίας τοποθετείται στα 1847 όταν ο G. Boole επινόησε την φερώνυμη Άλγεβρα αλλά η σύγχρονη μορφή της δόθηκε το 1948 από τον Claude Shannon ο οποίος εισήγαγε την έννοια του bit, απέδειξε ότι η Άλγεβρα Boole μπορεί να υλοποιηθεί μέσω απλών ηλεκτρικών κυκλωμάτων και όρισε την έννοια της εντροπίας της πληροφορίας η οποία έκτοτε έγινε γνωστή ως «εντροπία κατά Shannon».

Ο Shannon έθεσε και απάντησε δυο θεμελιώδη ερωτήματα:
1^{ο}) Πόσο μπορεί να συμπιεστεί ένα μήνυμα ώστε να μην χαθεί η πληροφορία την οποία μεταφέρει; (the noiseless coding theorem)
2^{ο}) Μέχρι ποίου σημείου μπορεί να μεταφερθεί αξιόπιστα κάποια πληροφορία μέσω ενός καναλιού το οποίο υπόκειται σε θόρυβο; (the noisy channel coding theorem)

Ένα μήνυμα είναι η μετάδοση μιας ακολουθίας γραμμάτων (και συμβόλων) από ένα αλφάβητο. Έστω ένα αλφάβητο $\{a_1, a_2, \ldots, a_k\}$ το οποίο αποτελείται από k το πλήθος γράμματα τα οποία είναι στατιστικά ανεξάρτητα και το κάθε ένα a_m από αυτά μπορεί να μεταδοθεί με μια εκ των προτέρων γνωστή πιθανότητα p_m με $0 \le p_m \le 1$ και $\sum_m p_m = 1$.
Η απάντηση που έδωσε ο Shannon στο πρώτο ερώτημα είναι ότι το ελάχιστο απαιτούμενο μήκος l που πρέπει να έχει ένα μήνυμα ώστε να μην χαθεί η ουσιαστική πληροφορία που μεταφέρει, ικανοποιεί την ανισότητα:

$$H \le l \le H + 1 \, , \qquad \text{με}$$
$$H = -\sum_k p_k \log_2 p_k \, .$$

Η συνάρτηση H που ορίζεται από την παραπάνω ισότητα ονομάζεται *«εντροπία κατά Shannon»* και ουσιαστικά μας λέει σε πόσα κλασικά bits αποθηκεύεται η ουσιώδης πληροφορία ενός μηνύματος.

Παρατήρηση :

Η συνάρτηση H είναι κοίλη κατά Schur και αυτό σημαίνει ότι όσο περισσότερο πλησιάζει προς την ομοιόμορφη η κατανομή που περιγράφει την ακριβή αναμετάδοση των γραμμάτων του αλφαβήτου, απαιτείται ολοένα & μεγαλύτερο πλήθος κλασικών bits.

Ένα εξαιρετικά ενδιαφέρον και κρίσιμο ερώτημα είναι αν υπάρχει κάποια διαφορά όταν χρησιμοποιούμε κβαντικές καταστάσεις για την μετάδοση μιας πληροφορίας. Η απάντηση είναι καταφατική εφόσον χρησιμοποιηθεί υπέρθεση και δόθηκε από τον Schumacher [**18**].

Ένα κβαντικό αλφάβητο είναι τώρα ένα σύνολο καθαρών καταστάσεων $\{|\psi_k\rangle, p_k\}$, όπου p_k είναι κάποια κατανομή πιθανότητας, κάθε γράμμα περιγράφεται από ένα πίνακα πυκνότητας

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$$

και ένα κβαντικό μήνυμα μήκους n περιγράφεται από τον πίνακα πυκνότητας

$\rho^{\otimes n} = \rho \otimes \cdots \otimes \rho$ (διότι τα γράμματα στέλνονται ανεξάρτητα).

<u>Θεώρημα του Schumacher</u> :

Αν ένα κβαντικό μήνυμα έχει μήκος $n \to +\infty$, τότε η καλύτερη δυνατή συμπίεση που μπορεί να επιτευχθεί, είναι συμπίεση σε ένα χώρο Hilbert H για τον οποίο ισχύει

$$\log(\dim H) = nS(\rho).$$

Η συνάρτηση $S(\rho)$ ονομάζεται εντροπία κατά von Neumann, είναι το Κβαντομηχανικό αντίστοιχο της εντροπίας κατά Shannon και ορίζεται ως εξής:

<u>Ορισμός 0.1.13.</u>

Για κάθε πίνακα πυκνότητας ρ_Q που παριστάνει μια μικτή κατάσταση ενός συστήματος Q ορίζουμε να είναι:

$$S(\rho_Q) = -Tr(\rho_Q \log \rho_Q).$$

► Βασικές ιδιότητες της εντροπίας von Neumann

1) Κάθε προβολικός τελεστής(δηλαδή κάθε καθαρή κατάσταση) έχει εντροπία von Neumann ίση με μηδέν.
2) Αν $\{|a_m\rangle\}, m \in \mathrm{I}$ είναι μια ορθοκανονική βάση στην οποία ο πίνακας πυκνότητας ρ είναι διαγώνιος με ιδιοτιμές λ_i, τότε από το φασματικό θεώρημα έχουμε ότι

$$\rho = \sum_i \lambda_i |a_i\rangle\langle a_i|, \text{ άρα}$$

$$S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i = H(A)$$

όπου $H(A)$ είναι η κατά Shannon εντροπία του αλφαβήτου $\{a_m\}$, $m \in \mathrm{I}$, του οποίου η ακριβής μετάδοση περιγράφεται από την κατανομή λ_i.

3) Η εντροπία von Neumann εξαρτάται μόνο από τις ιδιοτιμές του πίνακα πυκνότητας άρα παραμένει αναλλοίωτη σε μοναδιακή αλλαγή βάσης, δηλαδή

$$S(U\rho U^\dagger) = S(\rho), \text{ με } U \text{ μοναδιακός.}$$

4) Γίνεται μέγιστη όταν οι καταστάσεις είναι ισοπίθανες, δηλαδή όταν:

$$\lambda_i = \frac{1}{n}.$$

5) Είναι κοίλη συνάρτηση. Αυτό έπεται από την αντίστοιχη ιδιότητα της λογαριθμικής συνάρτησης και η φυσική του ερμηνεία είναι ότι όσο περισσότερο αγνοούμε το πώς είναι προετοιμασμένη η αρχική κατάσταση, η εντροπία von Neumann θα αυξάνει και μεγιστοποιείται(προηγούμενη παρατήρηση)όταν δεν έχουμε καμία πληροφορία για αυτήν.
6) Σε ένα διμερές σύστημα AB με πίνακα πυκνότητας ρ_{AB} ισχύει

$$S(\rho_{AB}) \le S(\rho_A) + S(\rho_B) \quad (1) \qquad \text{(υποπροσθετικότητα)}$$

Αν επιπλέον τα υποσυστήματα είναι ασυσχέτιστα δηλαδή είναι

$$\rho_{AB} = \rho_A \otimes \rho_B$$

τότε η (1) ισχύει ως ισότητα. Η (1) δηλώνει ότι η «προβλεψιμότητα» και η «τάξη» στην «ολότητα» είναι ανώτερη σε σύγκριση με το άθροισμα των αντίστοιχων μεγεθών στους «επιμέρους κόσμους», ή αλλιώς, αν ένα σύνθετο σύστημα το οποίο αποτελείται από δυο επιμέρους συσχετισμένα υποσυστήματα αναλυθεί σε αυτά τα υποσυστήματα, θα χαθεί η γνώση του τρόπου συσχέτισης και η συνολική εντροπία των επιμέρους υποσυστημάτων θα είναι μεγαλύτερη από την αρχική.
Όμως η ισότητα ισχύει όταν οι «επιμέρους κόσμοι» δεν επικοινωνούν μεταξύ τους (δεν έχουν καμία επιρροή ο ένας στον άλλο).

7) Σε ένα διμερές σύστημα AB ισχύει η παρακάτω τριγωνική ανισότητα (Araki-Lieb)

$$\left|S\left(\rho_A\right)-S\left(\rho_B\right)\right| \le S\left(\rho_{AB}\right) \le S\left(\rho_A\right)+S\left(\rho_B\right).$$

8) Σε ένα τριμερές σύστημα ABC με πίνακα πυκνότητας ρ_{ABC} ισχύει

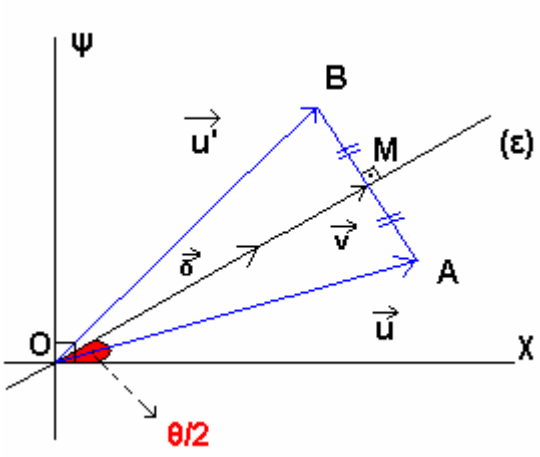
$$S\left(\rho_{ABC}\right)+S\left(\rho_B\right) \le S\left(\rho_{AB}\right)+S\left(\rho_{BC}\right)$$ (ισχυρή υποπροσθετικότητα).

0.2. Λήμματα

Λήμμα 0.1. : *Έστω επίπεδο* (Π) *εφοδιασμένο με ορθοκανονικό σύστημα αξόνων* Oxy *, και ευθεία* (ε) *που διέρχεται από το* O *και σχηματίζει γωνία* $\vartheta/2$ *με τον άξονα* xx' *. Η ανάκλαση ως προς την ευθεία* (ε) *είναι ένας γεωμετρικός μετασχηματισμός στο* (Π) *ο οποίος έχει πίνακα:*

$$I_\vartheta = \begin{bmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{bmatrix}.$$

Απόδειξη :



Θα δείξουμε πρώτα ότι αν $\vec{\delta}$ είναι ένα μοναδιαίο διάνυσμα του (Π) με φορέα την ευθεία (ε), τότε το συμμετρικό ενός διανύσματος $\vec{u}$ του επιπέδου ως προς την ευθεία (ε) είναι το $\vec{u'}$ με

$$\vec{u'} = 2\left(\vec{u}\vec{\delta}\right)\vec{\delta} - \vec{u} \qquad (1).$$

Αφού το $\vec{\delta}$ είναι μοναδιαίο διάνυσμα με φορέα την (ε), θα ισχύει

$$\vec{\delta} = \left(\cos\frac{\vartheta}{2}, \sin\frac{\vartheta}{2}\right)^{\mathrm{T}} \quad (2).$$

Έστω $\vec{v}$ η προβολή του $\vec{u}$ πάνω στην (ε). Τότε θα έχουμε ότι

$$\vec{v} = \left(\frac{\vec{u}\vec{\delta}}{\left\|\vec{\delta}\right\|^2}\right)\vec{\delta} \qquad \text{ή}$$

$$\vec{v} = \left(\vec{u}\vec{\delta}\right)\vec{\delta}.$$

Στο τρίγωνο OAB είναι $\vec{u} + \vec{u'} = 2\vec{v}$, οπότε προκύπτει αμέσως η (1). Έστω ακόμα ότι $\vec{u} = (x, y)^{\mathrm{T}}$ και $\vec{u'} = (x', y')^{\mathrm{T}}$. Από αυτές και τις (1), (2), μετά τις πράξεις προκύπτει ότι

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x\cos\vartheta + y\sin\vartheta \\ x\sin\vartheta - y\cos\vartheta \end{pmatrix}$$

$$= \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

άρα ο πίνακας της ανάκλασης ως προς την ευθεία (ε) είναι ο

$$I_\vartheta = \begin{bmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{bmatrix}.$$

Λήμμα 0.2. : *Έστω ένα επίπεδο (Π) εφοδιασμένο με ορθοκανονικό σύστημα αξόνων Oxy. Αν ο πίνακας ανάκλασης κατά γωνία ϑ ως προς κάποια ευθεία ανάκλασης (ε) είναι I_ϑ, και ο πίνακας στροφής κατά γωνία φ είναι R_φ, τότε ο πίνακας $R_\varphi I_\vartheta R_\varphi^\dagger$ είναι ο πίνακας ανάκλασης κατά γωνία $\vartheta - 2\varphi$ ως προς (ε).*

Απόδειξη :

Είναι $R_\varphi = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}$ και $I_\vartheta = \begin{bmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{bmatrix}$, άρα

$$R_\varphi I_\vartheta R_\varphi^\dagger = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{bmatrix} \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\vartheta-\varphi) & \sin(\vartheta-\varphi) \\ \sin(\vartheta-\varphi) & -\cos(\vartheta-\varphi) \end{bmatrix} \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\vartheta-2\varphi) & \sin(\vartheta-2\varphi) \\ \sin(\vartheta-2\varphi) & -\cos(\vartheta-2\varphi) \end{bmatrix}, \text{ που είναι το ζητούμενο.}$$

Λήμμα 0.3. *: Σε ένα επίπεδο (Π) εφοδιασμένο με ορθοκανονικό σύστημα αξόνων Oxy, η διαδοχική δράση δυο ανακλάσεων κατά γωνίες a και b, με αυτή τη σειρά, είναι στροφή κατά γωνία $a-b$.*

Απόδειξη :

Αρκεί να δείξουμε ότι $I_b I_a = R_{a-b}$.

Είναι: $I_b I_a = \begin{bmatrix} \cos b & \sin b \\ \sin b & -\cos b \end{bmatrix} \begin{bmatrix} \cos a & \sin a \\ \sin a & -\cos a \end{bmatrix}$

$$= \begin{bmatrix} \cos(a-b) & \sin(a-b) \\ -\sin(a-b) & \cos(a-b) \end{bmatrix}$$

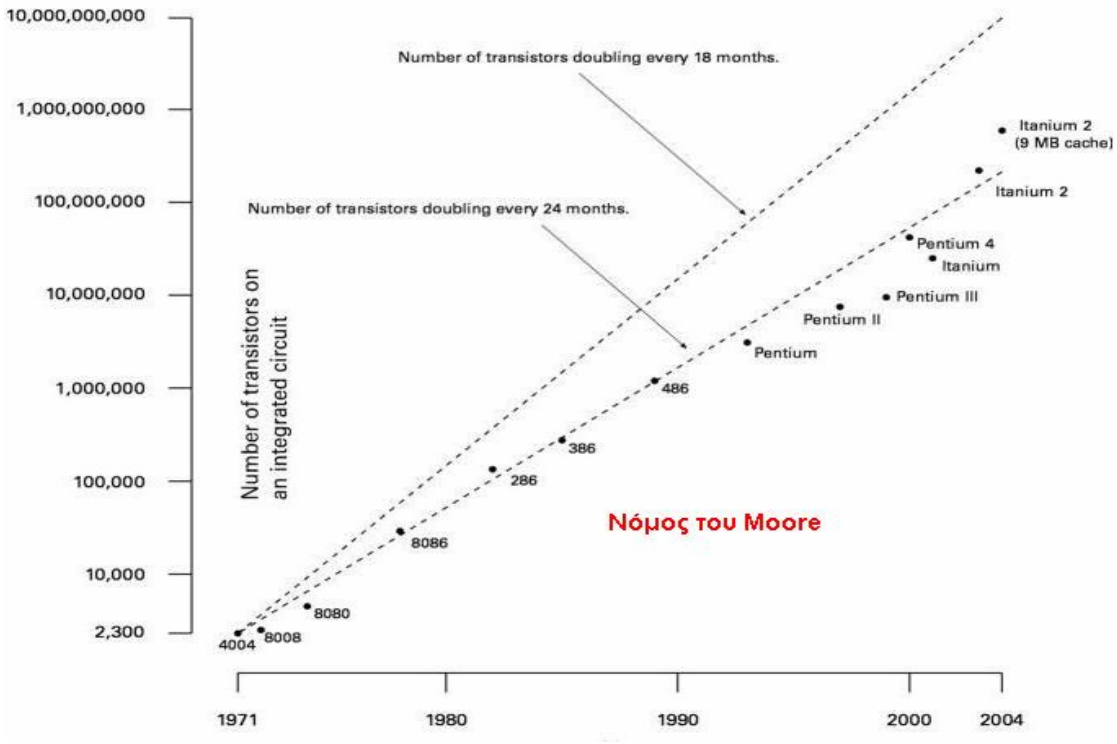
$$= R_{a-b}.$$

Κεφάλαιο 1

Ο αλγόριθμος του Grover

Εισαγωγή – Ιστορικά στοιχεία

Το 1943 κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, κατασκευάστηκε στην Μεγάλη Βρετανία ο Colossus, ο πρώτος υπολογιστής με ηλεκτρικά κυκλώματα. Είχε σχεδιαστεί για να αποκρυπτογραφεί τα κωδικοποιημένα μηνύματα της μηχανής «Αίνιγμα» των Γερμανών και λειτουργούσε με λυχνίες κενού. Όμως ήταν περιορισμένων δυνατοτήτων και δεν μπορούσε να εκτελέσει καμία άλλη εργασία εκτός από την επίλυση προβλημάτων αποκωδικοποίησης. Το 1944 η I.B.M. παρουσίασε τον πρώτο υπολογιστή σε πλήρη ανάπτυξη, τον Harvard Mark I, ο οποίος χρησιμοποιούσε ασφαλοδιακόπτες που ήταν πιο αξιόπιστοι από τις λυχνίες κενού. Ο πρώτος ηλεκτρονικός αριθμητικός υπολογιστής, ο ENIAC, κατασκευάστηκε το 1945 στην Αμερική και χρησιμοποιούσε λυχνίες για την υλοποίηση των λογικών κυκλωμάτων του. Μπορούσε να εκτελεί 5.000 πράξεις το δευτερόλεπτο με πενταψήφιους αριθμούς, να λύνει κάποια απλά προβλήματα και ήταν 1.000 φορές ταχύτερος από τον προηγούμενο (ηλεκτρομηχανικό) Harvard Mark I, αλλά είχε πολύ μικρή μνήμη για να είναι δυνατόν να αποθηκεύσει προγράμματα. Ακολούθησαν, πρώτα το 1948 ο Manchester Mark I, ο πρώτος υπολογιστής ο οποίος μπορούσε πλέον να «τρέξει» κανονικά ένα πρόγραμμα (Μεγάλη Βρετανία) και κατόπιν ο UNIVAC I που παρουσιάσθηκε το 1951. Αυτός ήταν 10 φορές ταχύτερος από τον ENIAC και είχε 100 φορές μεγαλύτερη μνήμη. Όμως όλοι αυτοί οι υπολογιστές πρώτης γενιάς, εξ' αιτίας των λυχνιών κενού, ήταν τεραστίων διαστάσεων, μικρής υπολογιστικής ισχύος, είχαν προβλήματα υπερθέρμανσης και ήταν πολύ ακριβοί. Η κρίσιμη εφεύρεση που έδωσε την λύση στα προβλήματα της υπολογιστικής ισχύος, χώρου, κόστους και υπερθέρμανσης ήταν το τρανζίστορ(1948). Από το 1956 που εμφανίστηκε ο πρώτος υπολογιστής με τρανζίστορ και μετά, το μέγεθος των υπολογιστών άρχισε να μειώνεται ραγδαία και παράλληλα αυξήθηκε αντίστοιχα η υπολογιστική ισχύς. Το 1965 ο Gordon Moore, ένας από τους ιδρυτές της εταιρείας Intel, έκανε μια εμπειρική παρατήρηση η οποία έκτοτε έγινε γνωστή ως «Νόμος του Moore».
Παρατήρησε ότι η πυκνότητα των τρανζίστορ σε ολοκληρωμένα κυκλώματα, άρα και η ισχύς των υπολογιστών, διπλασιάζεται κάθε 18-24 μήνες. Μέχρι σήμερα η πρόβλεψη αυτή αποδείχθηκε ακριβής όπως φαίνεται από το παρακάτω διάγραμμα της Intel.



Εξαιτίας της αλματώδους ανάπτυξης της νανοτεχνολογίας, ο Νόμος του Moore μάλλον θα εξακολουθήσει να ισχύει τουλάχιστον και για τη δεκαετία του 2000, ήδη έχουν κατασκευαστεί και μοριακοί διακόπτες πολλαπλής χρήσης. Αυτό σημαίνει ότι αν στο εγγύς μέλλον οι διαστάσεις των λογικών πυλών είναι πλέον της τάξεως υποατομικών σωματιδίων, τα κβαντικά φαινόμενα όχι μόνο δεν θα είναι αμελητέα αλλά αντίθετα θα είναι ιδιαίτερα κρίσιμα. Συνεπώς είναι απαραίτητο να έχουμε μια Θεωρία Πληροφορίας η οποία να λαμβάνει υπόψη τους νόμους της Κβαντομηχανικής .

Η ανάγκη αυτή έγινε γρήγορα κατανοητή και ήδη από την δεκαετία του 1970 εμφανίστηκαν οι πρώτες μελέτες και τα πρώτα σημαντικά αποτελέσματα στην Κβαντική Θεωρία της Πληροφορίας(Holevo, Bennett). Το 1981 ο Feynman παρατήρησε ότι είναι αδύνατο να περιγραφεί η εξέλιξη ενός Κβαντομηχανικού συστήματος μέσω ενός κλασικού υπολογιστή, άρα θα πρέπει να κατασκευαστεί μια καινούρια συσκευή στη οποία αυτό θα είναι εφικτό.

Η συσκευή αυτή η οποία θα εκτελεί υπολογισμούς και λογικές πράξεις λαμβάνοντας υπόψη τα Κβαντομηχανικά φαινόμενα ονομάστηκε *Κβαντικός Υπολογιστής*. Η βασική αρχή λειτουργίας αυτής της συσκευής θα είναι η χρήση των κβαντικών ιδιοτήτων των σωματιδίων για την αναπαράσταση, την αποθήκευση και τη διαχείριση δεδομένων. Φυσικά η επεξεργασία των δεδομένων αυτών θα πρέπει να γίνεται βάσει κανόνων οι οποίοι θα υπακούουν στους νόμους της Κβαντομηχανικής. Τη δεκαετία του 1980 και συγκεκριμένα το 1985, περιγράφθηκε θεωρητικά από τον Deutsch ο *καθολικός Κβαντικός Υπολογιστής*, μια θεωρητική μηχανή ανάλογη της καθολικής μηχανής Turing, η οποία συνδυάζει τις αρχές Turing-Church που διέπουν την κλασική Πληροφορική με τις αρχές της Κβαντομηχανικής. Για παράδειγμα, αν έχουμε έναν Κβαντικό Υπολογιστή ο οποίος χρησιμοποιεί δυο qbits, ο καταχωρητής (register) περιγράφεται από μια κατάσταση

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

όπου οι μιγαδικοί αριθμοί a,b,c,d περιγράφουν την πιθανότητα εμφάνισης των qbits μετά από κάποια μέτρηση. Ακριβέστερα, η πιθανότητα να εμφανιστεί $|00\rangle$ είναι $|a|^2$, η πιθανότητα να εμφανιστεί $|01\rangle$ είναι $|b|^2$ κλπ, με $|a|^2+|b|^2+|c|^2+|d|^2=1$. Επίσης, η πιθανότητα να εμφανιστεί 0 στο πρώτο qbit είναι $|a|^2+|b|^2$, αντίστοιχα $|a|^2+|c|^2$ στο δεύτερο qbit. Όπως έχουμε πει, «μέτρηση» στην Κβαντομηχανική είναι η δράση ενός προβολικού τελεστή πάνω στο διάνυσμα κατάστασης. Στην συγκεκριμένη περίπτωση, αν θέλουμε να κάνουμε μέτρηση στον πρώτο χώρο για να δούμε αν θα εμφανιστεί 0 και δεν θέλουμε να μετρήσουμε κάτι στον δεύτερο, θα δράσουμε πάνω στο $|\psi\rangle$ με τον τελεστή T, όπου

$$T = |0\rangle\langle 0| \otimes I_B .$$

Εάν εμφανιστεί 0 στον πρώτο χώρο, η κατάσταση μετά τη μέτρηση θα είναι

$$|0\rangle \otimes \left(\frac{a}{\sqrt{|a|^2+|b|^2}}|0\rangle + \frac{b}{\sqrt{|a|^2+|b|^2}}|1\rangle \right)$$

και αυτό θα συμβεί με πιθανότητα $|a|^2+|b|^2$.

Αντίστοιχα, αν θέλουμε να κάνουμε μέτρηση στον δεύτερο χώρο για να δούμε αν θα εμφανιστεί 1 και δεν θέλουμε να μετρήσουμε κάτι στον πρώτο, θα δράσουμε στο $|\psi\rangle$ με τον τελεστή T, αλλά τώρα θα είναι

$$T = I_A \otimes |1\rangle\langle 1|$$

Αν εμφανιστεί 1 στο δεύτερο χώρο, η μεταμετρητική κατάσταση θα είναι

$$\left(\frac{b}{\sqrt{|b|^2+|d|^2}}|0\rangle + \frac{d}{\sqrt{|b|^2+|d|^2}}|1\rangle \right) \otimes |1\rangle$$

και αυτό θα συμβεί με πιθανότητα $|b|^2+|d|^2$.

Γενικά, εάν υποθέσουμε ότι έχουμε έναν Κβαντικό Υπολογιστή με n qbits, ο καταχωρητής θα περιγράφεται από μια κατάσταση

$$|\psi\rangle = a_0|00\ldots0\rangle + a_1|00\ldots1\rangle + \ldots + a_{2^{n-1}}|11\ldots1\rangle$$

όπου οι μιγαδικοί a_k με $k = 0,1,\ldots,2^{n-1}$ περιγράφουν με αντίστοιχο με πριν τρόπο την πιθανότητα εμφάνισης των $|00\ldots0\rangle, |00\ldots1\rangle$ κλπ . Αντίστοιχα γίνονται και οι μετρήσεις.

Είναι προφανές ότι σε ένα Κβαντικό Υπολογιστή πρέπει πλέον να εξετάζουμε υπό αυτό το πρίσμα την επιλυσιμότητα τουλάχιστον των γνωστών προβλημάτων της κλασικής Πληροφορικής. Μπορεί όμως να γίνει μια τέτοια επίλυση; Κι αν ναι, με ποιόν τρόπο, πόσο γρήγορα και πόσο αξιόπιστα; Για να απαντηθούν αυτά τα ερωτήματα θα πρέπει αρχικά να έχουμε κατασκευάσει το θεωρητικό μοντέλο επίλυσης σ' αυτά τα προβλήματα, θα πρέπει δηλαδή να έχουμε *Κβαντικούς αλγόριθμους* .

Ο Deutsch το 1985, έγραψε επίσης και τον πρώτο Κβαντικό αλγόριθμο με τον οποίο είναι δυνατόν να ελεγχθεί αν μια δίτιμη συνάρτηση

$$f : \{0,1\} \to \{0,1\}$$

είναι σταθερή ή όχι (constant or balanced). Αργότερα γράφτηκαν και άλλοι Κβαντικοί αλγόριθμοι με γνωστότερους αυτούς των Deutsch και Josca, Shor και Grover.

Στην παρούσα εργασία θα ασχοληθούμε στο εξής με την μελέτη του αλγόριθμου του Grover.

► Περιγραφή του αλγόριθμου Grover

1.1. Γενικά στοιχεία

Ο Lov Grover εξέτασε και έλυσε (**[1], [2], [3]**) το 1996, το πρόβλημα της αναζήτησης στοιχείου μέσα σε μια μη δομημένη βάση δεδομένων. Όπως και στην κλασική Θεωρία Πληροφορίας, *βάση δεδομένων* θεωρείται κάθε σύνολο του οποίου τα στοιχεία μπορούν να χρησιμοποιηθούν για την εξαγωγή ή τη διαχείριση (αποθήκευση, μετάδοση, επεξεργασία) πληροφορίας. Είναι φανερό ότι το πρώτο κρίσιμο ερώτημα που τίθεται για μια βάση δεδομένων είναι η ύπαρξη ή όχι κάποιου λογικού συσχετισμού μεταξύ των στοιχείων της, και το χειρότερο που μπορεί να συμβεί είναι η πλήρης απουσία μιας τέτοιας σύνδεσης. Τότε λέμε ότι η βάση δεδομένων *είναι μη δομημένη* (unsorted data base). Για παράδειγμα μπορούμε να θεωρήσουμε έναν τηλεφωνικό κατάλογο ο οποίος περιέχει, σε δυο στήλες, τα ονόματα και τα τηλέφωνα N το πλήθος συνδρομητών. Αν εξετάζουμε τον κατάλογο ως προς τα ονόματα, τότε είναι μια δομημένη βάση δεδομένων αφού τα ονόματα αναγράφονται με αλφαβητική σειρά, ενώ αν τον εξετάζουμε ως προς τα τηλέφωνα τότε είναι μη δομημένη βάση δεδομένων. Το ερώτημα που απάντησε ο Grover είναι ισοδύναμο με το «πώς θα βρούμε μέσα στο σύνολο όλων των αριθμών τηλεφώνων του καταλόγου έναν δεδομένο αριθμό και πόσο υπολογιστικό χρόνο θα χρειαστούμε γι' αυτό;». Απέδειξε επίσης ότι αυτό μπορεί να επιτευχθεί σε υπολογιστικό χρόνο $O\left(\sqrt{N}\right)$, και πιο συγκεκριμένα χρειάζονται περίπου $\pi/4\sqrt{N}$ δοκιμές-επαναλήψεις. Η διαφορά υπολογιστικής ταχύτητας μεταξύ του αλγόριθμου Grover και ενός κλασικού αλγόριθμου είναι τεράστια και γίνεται ολοένα μεγαλύτερη καθώς αυξάνει το μέγεθος της βάσης δεδομένων, διότι κάθε κλασικός αλγόριθμος επιλύει το πρόβλημα σε υπολογιστικό χρόνο $O(N)$ με $N/2$ κατά μέσο όρο δοκιμές. Αν υποθέσουμε ότι ο τηλεφωνικός κατάλογος του παραδείγματος είναι παγκόσμιος και έχει π.χ. 5.000.000.000 αριθμούς τηλεφώνων, τότε ένας κλασικός υπολογιστής θα βρει τον ζητούμενο αριθμό τηλεφώνου σε 2.500.000.000 περίπου δοκιμές, ενώ ο Κβαντικός Υπολογιστής που χρησιμοποιεί τον αλγόριθμο του Grover θα χρειαστεί περίπου 55-56.000 δοκιμές. Ακόμα ο αλγόριθμος Grover μπορεί να χρησιμοποιηθεί και για την εύρεση k αντικειμένων από τα N και αυτό επιτυγχάνεται με $\pi/4\sqrt{N/k}$ δοκιμές.

Εδώ αξίζει να σημειωθεί ότι το πρόβλημα της αναζήτησης στοιχείου μέσα σε μια μη δομημένη βάση δεδομένων έχει ως ισοδύναμη Μαθηματική διατύπωση τον προσδιορισμό των τιμών της αντίστροφης κάποιας συνάρτησης. Αν π.χ. είναι δυνατόν να βρίσκουμε μέσω ενός Κβαντικού Υπολογιστή τις τιμές μιας συνάρτησης φ με πεδίο ορισμού κάποιο σύνολο με N το πλήθος στοιχεία, τότε το να βρούμε την αντίστροφη εικόνα κάποιου στοιχείου είναι στην ουσία ένα πρόβλημα αναζήτησης μέσα στην βάση δεδομένων που ορίζεται από το πεδίο ορισμού της φ. Αν η φ είναι «1-1» τότε ζητάμε ένα μόνο στοιχείο, ειδάλλως περισσότερα.

1.2. Περιγραφή και διατύπωση του προβλήματος

Ας υποθέσουμε ότι έχουμε μια μη δομημένη βάση δεδομένων με N στοιχεία, έστω $N = 2^n$, εκ των οποίων ζητάμε κάποιο συγκεκριμένο. Το πρόβλημα μπορεί ισοδύναμα να διατυπωθεί ως εξής: για να «μαρκάρουμε» το ζητούμενο στοιχείο θεωρούμε την συνάρτηση

$$f : \{0,1\}^n \to \{0,1\}$$

με τύπο $f(x) = 0$ για όλα τα $x \in \{0,1\}^n$ εκτός από ένα μοναδικό x_0 για το οποίο είναι $f(x_0) = 1$.

Αν αντιστοιχίσουμε το ζητούμενο αντικείμενο της βάσης δεδομένων στο x_0 και όλα τα υπόλοιπα αντικείμενα στα υπόλοιπα $x \in \{0,1\}^n$ με κάποιο «1-1 και επί» τρόπο, είναι φανερό ότι αρκεί ισοδύναμα να κατασκευάσουμε έναν αλγόριθμο που θα βρίσκει το x_0.

Υποθέτουμε τώρα ότι διαθέτουμε έναν Κβαντικό Υπολογιστή ο οποίος έχει $n+1$ qbits, άρα απαιτείται ένας χώρος Hilbert διάστασης $1+\log_2 N$. Συμβολίζουμε με $|x\rangle$ τον καταχωρητή στον οποίο θα εμφανίζονται όλα τα

$$|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$$

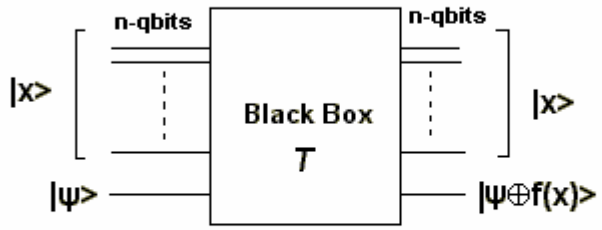
δηλαδή όλα τα $x \in \{0,1\}^n$, άρα όλα τα αντικείμενα της βάσης δεδομένων, και ορίζουμε $|\psi\rangle$ να είναι $|0\rangle$ ή $|1\rangle$, ή γενικά κάποιος γραμμικός συνδυασμός τους.

Τα διανύσματα $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$ τα συμβολίζουμε επίσης με $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ και θα χρησιμοποιήσουμε αργότερα αυτό το συμβολισμό.

Η f περιγράφεται από τη δράση ενός μοναδιακού τελεστή T πάνω στο διάνυσμα $|x\rangle|\psi\rangle$ από την ισότητα

$$T|x\rangle|\psi\rangle = |x\rangle|\psi \oplus f(x)\rangle$$

στην οποία με $\oplus$ συμβολίζεται η πρόσθεση mod2. Το γεγονός ότι η αρχική βάση δεδομένων είναι μη δομημένη, σημαίνει ότι ο τελεστής T δρα πάνω στο διάνυσμα $|x\rangle|\psi\rangle$ με κάποιο τρόπο στον οποίο δεν μπορούμε να επέμβουμε, π.χ. μέσα σε ένα «μαύρο κουτί».



Παρατηρούμε ότι αν επιλέξουμε ως

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

τότε η δράση του T πάνω στο διάνυσμα $|x\rangle|\psi\rangle$ δίνεται από τις παρακάτω ισότητες

$$T|x\rangle|\psi\rangle = T|x\rangle\left(\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right)$$
$$= \frac{1}{\sqrt{2}}\left(T|x\rangle|0\rangle - T|x\rangle|1\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|x\rangle\left(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\right).$$

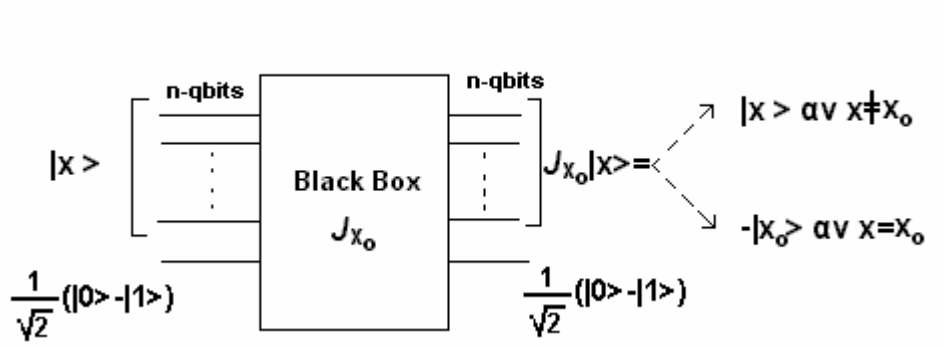
Από τον ορισμό της f και την παραπάνω ισότητα συμπεραίνουμε ότι

$$T|x\rangle|\psi\rangle = \begin{cases} \frac{1}{\sqrt{2}}|x\rangle\left(|0\rangle-|1\rangle\right) = |x\rangle|\psi\rangle, x \neq x_0 \\ -\frac{1}{\sqrt{2}}|x_0\rangle\left(|0\rangle-|1\rangle\right) = -|x_0\rangle|\psi\rangle, x = x_0 \end{cases}.$$

Το αποτέλεσμα αυτό μας οδηγεί στο να θεωρήσουμε ισοδύναμα αντί για τον T, τον τελεστή J_{x_0} η δράση του οποίου ορίζεται από τις

$$J_{x_0}|x\rangle = \begin{cases} |x\rangle, x \neq x_0 \\ -|x_0\rangle, x = x_0 \end{cases} = (-1)^{f(x)}|x\rangle.$$

Έτσι το προηγούμενο «μαύρο κουτί» περιγράφεται ισοδύναμα από το παρακάτω σχήμα:



Σκεπτόμενοι γεωμετρικά, μπορούμε να «μαρκάρουμε» το $|x_0\rangle$ τοποθετώντας το κάθετα σε όλα τα υπόλοιπα $|x\rangle$ στον χώρο $\mathbb{R}^n$. Μάλιστα μπορούμε ακόμα περισσότερο να θεωρήσουμε ότι κάθε ένα από τα $|x\rangle$ θα είναι κάποιο από τα μοναδιαία διανύσματα της φυσικής βάσης του χώρου $\mathbb{R}^n$. Παρατηρούμε ότι τότε ο τελεστής J_{x_0} είναι μια *ανάκλαση Householder*, ακριβέστερα είναι μια ανάκλαση στο υπερεπίπεδο που είναι ορθογώνιο στο $|x_0\rangle$ και ισχύει:

$$J_{x_0} = I - 2|x_0\rangle\langle x_0|.$$

Επομένως το αρχικό πρόβλημα αναζήτησης μέσα στη βάση δεδομένων έχει αναχθεί πλέον στον προσδιορισμό του x_0 δοθέντος ενός «μαύρου κουτιού» το οποίο υπολογίζει τη δράση του συγκεκριμένου τελεστή ανάκλασης J_{x_0} (ή ισοδύναμα «μαρκάρει» το x_0 μέσω μιας ανάκλασης).

Για τις ανακλάσεις Householder είναι γνωστά τα παρακάτω δυο λήμματα:

Λήμμα 1.1. : *Αν $|x\rangle$ και $|\psi\rangle$ είναι δυο τυχαία διανύσματα (τυχαίες καταστάσεις) σ' ένα χώρο Hilbert, τότε η ανάκλαση J_x διατηρεί τον χώρο S που παράγεται από τα διανύσματα $|x\rangle$ και $|\psi\rangle$.*

Απόδειξη :

Έστω $|v\rangle \in S$. Τότε υπάρχουν $c_1, c_2 \in \mathbb{C}$ ώστε $|v\rangle = c_1|x\rangle + c_2|\psi\rangle$ και

$$\begin{aligned} J_x|v\rangle &= J_x\left(c_1|x\rangle + c_2|\psi\rangle\right) \\ &= \left(I - 2|x\rangle\langle x|\right)\left(c_1|x\rangle + c_2|\psi\rangle\right) \\ &= c_1|x\rangle - 2c_1|x\rangle\langle x||x\rangle + c_2|\psi\rangle - 2c_2|x\rangle\langle x|\psi\rangle \\ &= \left(c_1 - 2c_1\|x\|^2 - 2c_2\langle x|\psi\rangle\right)|x\rangle + c_2|\psi\rangle \end{aligned}$$

και αυτό δείχνει αμέσως το ζητούμενο.

Λήμμα 1.2. : *Για κάθε μοναδιακό τελεστή U ισχύει*

$$UJ_{|x\rangle}U^{-1} = J_{U|x\rangle}$$

Απόδειξη :

Είναι

$$\begin{aligned} UJ_{|x\rangle}U^{-1} &= U\left(I - 2|x\rangle\langle x|\right)U^{-1} \\ &= UU^{-1} - 2U|x\rangle\langle x|U^{-1} \\ &= I - 2U|x\rangle\left(U|x\rangle\right)^{\dagger} \qquad \text{(αφού } U^{\dagger} = U^{-1}\text{)} \\ &= J_{U|x\rangle}. \end{aligned}$$

1.3. Ο τελεστής αναζήτησης του Grover

Είναι φανερό ότι για να λειτουργήσει το «μαύρο κουτί» θα πρέπει να εισαχθεί κάποια αρχική κατάσταση. Από τη στιγμή που η βάση δεδομένων είναι μη δομημένη δεν υπάρχει καμία ιδιαίτερη προτίμηση, άρα η αρχική κατάσταση μπορεί να επιλεχθεί τυχαία, και η πιο λογική επιλογή είναι να εμφανιστούν σε ισοπίθανη υπέρθεση όλα τα στοιχεία της βάσης δεδομένων. Επομένως η πρώτη μας ενέργεια θα είναι να προετοιμάσουμε το σύστημα στην κατάσταση

$$|s\rangle \equiv |x\rangle = \frac{1}{\sqrt{N}}\sum_{\lambda=0}^{N-1}|\lambda\rangle$$

(για τα διανύσματα $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$ θα χρησιμοποιούμε στο εξής τον συμβολισμό $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ που αναφέραμε στην αρχή αυτής της ενότητας).

Αυτό τεχνικά μπορεί να γίνει αν εφαρμόσουμε στα $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ τον μετασχηματισμό Walsh-Hadamard $H^{\otimes n}$, όπου

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

είναι ο μετασχηματισμός Walsh-Hadamard (ή Hadamard gate) ο οποίος απεικονίζει τα $|0\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix}^{\mathrm{T}}$ και $|1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}^{\mathrm{T}}$ στην ισοπίθανη υπέρθεσή τους

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\langle 0|+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\langle 1|=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.$$

Επίσης η ισοπίθανη υπέρθεση όλων των άλλων στοιχείων της βάσης δεδομένων εκτός από το x_0 είναι

$$|r\rangle=\frac{1}{\sqrt{N-1}}\sum_{\lambda\neq x_0}|\lambda\rangle.$$

Παρατηρούμε ότι αφενός τα $|r\rangle$ και $|x_0\rangle$ είναι μοναδιαίου μήκους και κάθετα μεταξύ τους και αφετέρου για την αρχική κατάσταση $|s\rangle$ του καταχωρητή ισχύει

$$|s\rangle=\frac{1}{\sqrt{N}}|x_0\rangle+\sqrt{\frac{N-1}{N}}|r\rangle \quad (1)$$

άρα αυτή θα ανήκει στον διδιάστατο υπόχωρο $S=\langle|r\rangle,|x_0\rangle\rangle$. Στο εξής θα εργαστούμε μέσα στον S και θα θεωρούμε ότι

$$|x_0\rangle=\begin{pmatrix}1 & 0\end{pmatrix}^{\mathrm{T}} \text{ και } |r\rangle=\begin{pmatrix}0 & 1\end{pmatrix}^{\mathrm{T}}.$$

Ακόμα από την (1) είναι αμέσως φανερό ότι

$$|s\rangle=\left(\frac{1}{\sqrt{N}} \quad \sqrt{\frac{N-1}{N}}\right)^{\mathrm{T}}.$$

<u>Ορισμός 1.1.</u> :

Ορίζουμε ως τελεστή αναζήτησης του Grover τον τελεστή που ορίζεται από την ισότητα

$$\boxed{U_G=-J_sJ_{x_0}}$$

όπου J_S και J_{x_0} είναι οι ανακλάσεις Householder

$$J_{x_0}=I-2|x_0\rangle\langle x_0| \text{ και } J_s=I-2|s\rangle\langle s|.$$

1.4. Διατύπωση του αλγόριθμου Grover

Στη συνέχεια θα διατυπώσουμε τον αλγόριθμο του Grover με δυο προτάσεις τις οποίες και θα αποδείξουμε. Στην πρώτη πρόταση θα δείξουμε ότι ο υπόχωρος $S=\langle|r\rangle,|x_0\rangle\rangle$ είναι κλειστός ως προς τη δράση του τελεστή αναζήτησης U_G, και στη δεύτερη θα δείξουμε ότι μπορούμε να βρούμε το ζητούμενο x_0, αν ο U_G εφαρμοστεί $O\left(\sqrt{N}\right)$ φορές στο $|s\rangle$.

<u>Πρόταση 1.1.</u> : *Ο υπόχωρος $S=\langle|r\rangle,|x_0\rangle\rangle$ είναι κλειστός ως προς τη δράση του τελεστή αναζήτησης του Grover.*

<u>Απόδειξη</u> :

Τα διανύσματα $|s\rangle$ και $|r\rangle$ είναι γραμμικά ανεξάρτητα μεταξύ τους διότι αν $\lambda,\mu\in\mathbb{C}$ ώστε

$$\lambda|s\rangle+\mu|r\rangle=0$$

τότε θα ισχύει

$$\lambda\left(\frac{1}{\sqrt{N}}|x_0\rangle+\sqrt{\frac{N-1}{N}}|r\rangle\right)+\mu|r\rangle=0 \text{ ή}$$

$$\frac{\lambda}{\sqrt{N}}|x_0\rangle+\left(\lambda\sqrt{\frac{N-1}{N}}+\mu\right)|r\rangle=0 \qquad (2).$$

Όμως τα $|r\rangle$ και $|x_0\rangle$ είναι κάθετα, άρα γραμμικά ανεξάρτητα, και από την (2) προκύπτει αμέσως ότι $\lambda=\mu=0$.

Παρατηρούμε ακόμα ότι από την (1) έχουμε

$$|x_0\rangle=\sqrt{N}|s\rangle-\sqrt{N-1}|r\rangle \qquad (3)$$

άρα τα $|r\rangle$ και $|s\rangle$ παράγουν τον S διότι αν $|v\rangle\in S$, τότε

$$\begin{aligned}|v\rangle&=c_1|x_0\rangle+c_2|r\rangle && \text{με } c_1,c_2\in\mathbb{C}\\ &=c_1\left(\sqrt{N}|s\rangle-\sqrt{N-1}|r\rangle\right)+c_2|r\rangle && \text{λόγω της (3)}\\ &=c_1\sqrt{N}|s\rangle+\left(c_2-c_1\sqrt{N-1}\right)|r\rangle.\end{aligned}$$

Συνεπώς τα $|r\rangle$ και $|s\rangle$ είναι μια βάση του S και προφανώς ισχύει ότι:

$$S=\langle|r\rangle,|x_0\rangle\rangle=\langle|r\rangle,|s\rangle\rangle.$$

Ας υποθέσουμε τώρα ότι ο J_{x_0} δρα πάνω σε κάποιο $|v\rangle=c_1|x_0\rangle+c_2|r\rangle\in S$. Τότε, σύμφωνα με το Λήμμα 1.1 η ανάκλαση αυτή διατηρεί τον χώρο $\langle|v\rangle,|x_0\rangle\rangle$ και επίσης ισχύει ότι:

$$S=\langle|v\rangle,|x_0\rangle\rangle=\langle|r\rangle,|x_0\rangle\rangle=\langle|r\rangle,|s\rangle\rangle.$$

Στη συνέχεια δρα ο J_S πάνω σε κάποιο άλλο στοιχείο του S (ο οποίος έχει διατηρηθεί μετά την πρώτη δράση), το $|w\rangle=c_2|s\rangle+c_3|r\rangle\in S$ και σύμφωνα πάλι με το ίδιο Λήμμα, η ανάκλαση J_S θα διατηρεί τον χώρο $\langle|w\rangle,|s\rangle\rangle=\langle|r\rangle,|s\rangle\rangle=S$.

<u>Πρόταση 1.2.</u> : *Αν $N\gg 1$ και $|s^{(m)}\rangle:=U_G^m|s\rangle$, τότε είναι $|\langle x_0|s^{(m)}\rangle|^2\approx 1$ για $m=O\left(\sqrt{N}\right)$ το πλήθος δράσεις του τελεστή αναζήτησης.*

<u>Απόδειξη</u> :

Όπως έχουμε αναφέρει προηγουμένως είναι $|s\rangle=\left(\frac{1}{\sqrt{N}}\quad\sqrt{\frac{N-1}{N}}\right)^{\mathrm{T}}$, $|x_0\rangle=\begin{pmatrix}1&0\end{pmatrix}^{\mathrm{T}}$ και

$$J_{x_0}=I-2|x_0\rangle\langle x_0|,\ J_s=I-2|s\rangle\langle s|,$$

άρα οι ανακλάσεις αυτές θα παριστάνονται από τους πίνακες

$$J_{x_0}=\begin{pmatrix}-1&0\\0&1\end{pmatrix} \text{ και } J_s=\begin{pmatrix}\frac{N-2}{N}&-\frac{2\sqrt{N-1}}{N}\\-\frac{2\sqrt{N-1}}{N}&-\frac{N-2}{N}\end{pmatrix}.$$

Αυτό σημαίνει ότι ο τελεστής αναζήτησης έχει πίνακα

$$U_G = -J_s J_{x_0} = \begin{pmatrix} \dfrac{N-2}{N} & \dfrac{2\sqrt{N-1}}{N} \\ -\dfrac{2\sqrt{N-1}}{N} & \dfrac{N-2}{N} \end{pmatrix}.$$

Αμέσως βλέπουμε ότι ισχύει η ισότητα

$$\left(\frac{N-2}{N}\right)^2 + \left(\frac{2\sqrt{N-1}}{N}\right)^2 = 1.$$

Επομένως υπάρχει $\vartheta \in \mathbb{R}$ ώστε $\vartheta = \arcsin\left(\dfrac{2\sqrt{N-1}}{N}\right)$, άρα

$$U_G = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix},$$

το οποίο είναι βεβαίως αναμενόμενο διότι στο Λήμμα 0.3. έχουμε δείξει ότι το γινόμενο δυο ανακλάσεων είναι στροφή. Για τυχαίο θετικό ακέραιο m ισχύει ότι

$$U_G^m = \begin{pmatrix} \cos(m\vartheta) & \sin(m\vartheta) \\ -\sin(m\vartheta) & \cos(m\vartheta) \end{pmatrix}.$$

Συνεπώς θα είναι

$$\left|s^{(m)}\right\rangle = U_G^m \left|s\right\rangle = \begin{pmatrix} \cos(m\vartheta) & \sin(m\vartheta) \\ -\sin(m\vartheta) & \cos(m\vartheta) \end{pmatrix} \begin{bmatrix} \dfrac{1}{\sqrt{N}} \\ \sqrt{\dfrac{N-1}{N}} \end{bmatrix} \text{ ή}$$

$$\left|s^{(m)}\right\rangle = \begin{bmatrix} \dfrac{1}{\sqrt{N}}\cos(m\vartheta) + \sqrt{\dfrac{N-1}{N}}\sin(m\vartheta) \\ -\dfrac{1}{\sqrt{N}}\sin(m\vartheta) + \sqrt{\dfrac{N-1}{N}}\cos(m\vartheta) \end{bmatrix}.$$

Ισχύει επίσης

$$\left(\frac{1}{\sqrt{N}}\right)^2 + \left(\sqrt{\frac{N-1}{N}}\right)^2 = 1,$$

άρα υπάρχει $a \in \mathbb{R}$ ώστε $a = \arccos\left(\dfrac{1}{\sqrt{N}}\right)$ και τότε

$$\left|s^{(m)}\right\rangle = \begin{bmatrix} \cos a\cos(m\vartheta) + \sin a\sin(m\vartheta) \\ -\sin a\sin(m\vartheta) + \cos a\cos(m\vartheta) \end{bmatrix} = \begin{bmatrix} \cos(m\vartheta - a) \\ \sin(m\vartheta - a) \end{bmatrix}.$$

Η τελευταία ισότητα μας δείχνει την εξέλιξη της αρχικής κατάστασης αν εφαρμόσουμε σε αυτήν τον αλγόριθμο αναζήτησης m φορές. Η γωνιακή απόσταση των $\left|s^{(m)}\right\rangle$ και $\left|x_0\right\rangle$ μπορεί να προσδιοριστεί από το εσωτερικό τους γινόμενο το οποίο είναι

$$\boxed{\left\langle x_0 \middle| s^{(m)} \right\rangle = \cos(m\vartheta - a)}.$$

Ο αλγόριθμος θα είναι επιτυχής αν έχει βρει είτε το ζητούμενο x_0, είτε το $-x_0$, δηλαδή όταν

$$\left|\left\langle x_0 \middle| s^{(m)} \right\rangle\right|^2 = \cos^2\left(m\vartheta - a\right) = 1,$$

το οποίο συμβαίνει για $m = a/\vartheta$ (4).

Από υπόθεση είναι $N \gg 1$, άρα $\sin\vartheta = 2\sqrt{N-1}/N \approx 0$, οπότε $\vartheta \approx 2/\sqrt{N}$. Επίσης είναι $\cos a = 1/\sqrt{N} \to 0$, άρα $a \approx \pi/2$. Από αυτά και την (4) προκύπτει ότι

$$\boxed{m = \frac{\pi}{4}\sqrt{N} = O\left(\sqrt{N}\right)}.$$

Παρατηρήσεις :

I) Σύμφωνα με το Λήμμα 1.2., για κάθε μοναδιακό τελεστή U είναι $UJ_{|s\rangle}U^{-1} = J_{U|s\rangle}$, άρα και ο $U_G = -UJ_{|s\rangle}U^{-1}J_{x_0} = -J_{U|s\rangle}J_{x_0}$ είναι επίσης τελεστής αναζήτησης. Η αλγεβρική σημασία αυτού του γεγονότος είναι ότι *ο αλγόριθμος επιτρέπει ελευθερία ως προς την ομάδα* $SU(2)$.

II) Έχει αποδειχθεί (Bennett 1997) ότι ο αλγόριθμος είναι *βέλτιστος*, δηλαδή ότι αν ένας αλγόριθμος αναζήτησης χρησιμοποιεί ως «μαύρο κουτί» μόνο μια διαδικασία ανάκλασης, τότε για να είναι επιτυχής πρέπει να εφαρμοστεί τουλάχιστον όσες φορές και ο αλγόριθμος του Grover.

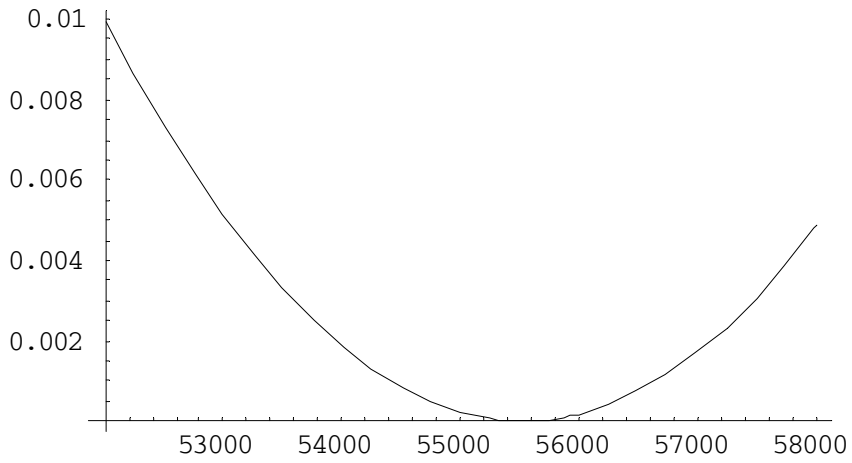
III) Με εντελώς ανάλογο τρόπο γίνεται η αναζήτηση περισσότερων στοιχείων.

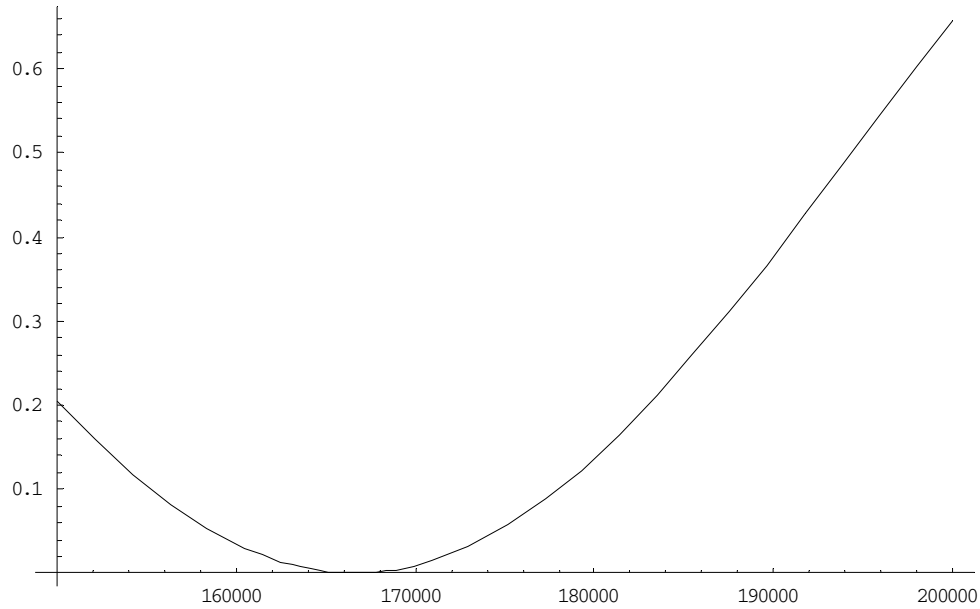
Αριθμητική επαλήθευση

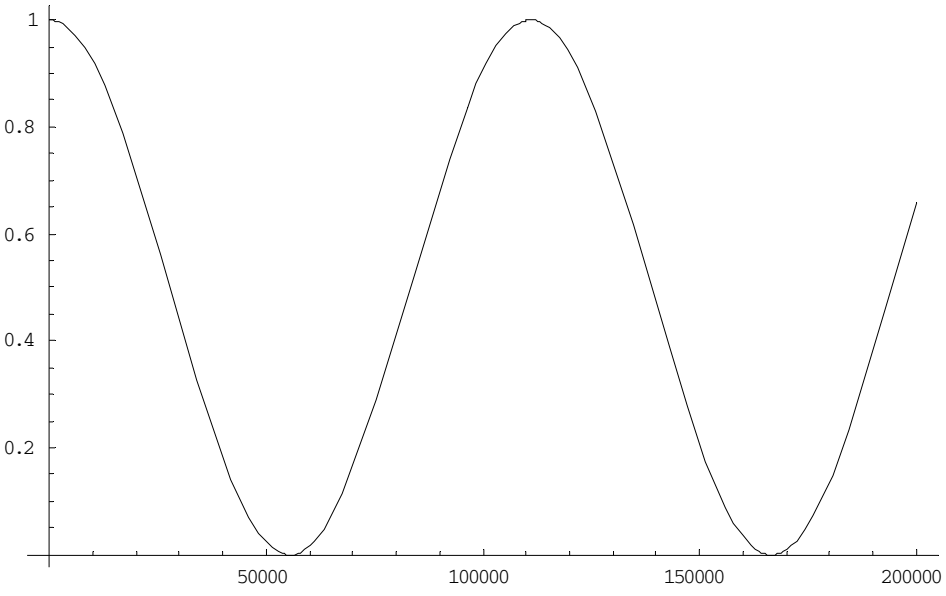
Στα παρακάτω διαγράμματα (με Mathematica 5) φαίνεται η γραφική παράσταση της συνάρτησης

$$y(m) = 1 - \cos^2\left(m\vartheta - a\right)$$

για τη βάση δεδομένων του τηλεφωνικού καταλόγου που είχαμε αναφέρει στην αρχή με $N = 5\cdot 10^9$ αριθμούς τηλεφώνων, με ανεξάρτητη μεταβλητή τον αριθμό επαναλήψεων. Όπως διαπιστώνουμε από το πρώτο και το δεύτερο σχήμα, η πρώτη επιτυχία του αλγόριθμου συμβαίνει μεταξύ 55-56.000 επαναλήψεων και η δεύτερη μεταξύ 160-170.000 επαναλήψεων. Στο τρίτο σχήμα φαίνεται μια πιο γενική εικόνα αυτής της γραφικής παράστασης.




0.6
0.5
0.4
0.3
0.2
0.1
160000
170000
180000
190000
200000


1
0.8
0.6
0.4
0.2
50000
100000
150000
200000

Κεφάλαιο 2

Κβαντικός θόρυβος στον αλγόριθμο του Grover

2.1. Εισαγωγή

Στα προηγούμενα είδαμε ότι η θεμελιώδης διαφορά μεταξύ Κβαντικού και κλασικού υπολογιστή έγκειται στο τι χρησιμοποιεί ο καθένας ως βασικό πόρο πληροφορίας. Ενώ ο μεν κλασικός υπολογιστής χρησιμοποιεί το bit το οποίο μπορεί να λάβει μόνο δυο διακριτές τιμές, ο Κβαντικός χρησιμοποιεί αντίστοιχα το qbit το οποίο μπορεί λόγω υπέρθεσης να παίρνει άπειρες τιμές. Σ' αυτό ακριβώς το γεγονός οφείλεται και η μεταξύ τους τεράστια διαφορά υπολογιστικής ισχύος που είναι και το ισχυρό πλεονέκτημα του Κβαντικού υπολογιστή απέναντι στον κλασικό. Όμως ο Κβαντικός υπολογιστής έχει ως αδύνατο σημείο το ότι είναι εξαιρετικά ασταθής. Είναι γνωστό ότι κάθε φυσικό σύστημα αλληλεπιδρά με το περιβάλλον του και δεν υπάρχει τίποτα που να είναι απολύτως απομονωμένο. Αυτό σημαίνει ότι τα qbits θα μεταβάλλονται λόγω εξωτερικών, γενικά τυχαίων, επιδράσεων (κβαντικός θόρυβος) οπότε η λειτουργία και η αποτελεσματικότητα ενός Κβαντικού υπολογιστή θα εξαρτώνται άμεσα από την επίδραση του περιβάλλοντος. Τα αξιώματα της Κβαντομηχανικής σύμφωνα με τα οποία η χρονική εξέλιξη ενός συστήματος δίνεται από μοναδιακούς τελεστές και οι μετρήσεις γίνονται με προβολικούς τελεστές, περιγράφουν ιδανικές καταστάσεις, συνεπώς και οι αντίστοιχοι αλγόριθμοι θα είναι «ιδανικοί αλγόριθμοι». Άρα αν θέλουμε να εφαρμόσουμε ρεαλιστικά Κβαντικούς αλγόριθμους θα πρέπει να ξέρουμε επίσης πώς και πόσο επηρεάζονται τα qbits από τις εξωτερικές συνθήκες. Στα επόμενα ο σκοπός μας θα είναι να μελετήσουμε την επίδραση του εξωτερικού περιβάλλοντος στον αλγόριθμο του Grover. Πιο συγκεκριμένα θα καθορίσουμε πρώτα ποια θα είναι η καινούρια Χαμιλτονιανή μέσω της οποίας περιγράφεται η επίδραση του περιβάλλοντος, θα βρούμε τον αντίστοιχο μοναδιακό τελεστή εξέλιξης και θα κατασκευάσουμε τρεις νέους τελεστές αναζήτησης. Ο πρώτος και γενικότερος, θα προκύψει απ' ευθείας από την νέα Χαμιλτονιανή και θα δείχνει το πώς λαμβάνεται υπόψη η επίδραση του περιβάλλοντος, ενώ ο δεύτερος και ο τρίτος θα κατασκευαστούν από μοναδιακούς γεννήτορες. Στη συνέχεια θα υπολογίσουμε την αξιοπιστία του αλγόριθμου και για τις τρεις περιπτώσεις των παραπάνω τελεστών αναζήτησης και θα δείξουμε ότι αν και ο αλγόριθμος καταρρέει εκθετικά γρήγορα υπό την επίδραση κβαντικού θορύβου, εντούτοις υπάρχουν άπειρες αριθμητικές τιμές αυτού του μεγέθους για τις οποίες επιζεί και είναι αποτελεσματικός σε $O\left(\sqrt{N}\right)$ επαναλήψεις.

2.2. Η επίδραση του περιβάλλοντος

2.2.1. Ο μοναδιακός τελεστής εξέλιξης υπό την επίδραση Κβαντικού θορύβου

Έχουμε δει ότι ο αλγόριθμος του Grover επιτρέπει ελευθερία ως προς την ομάδα $SU(2)$, οπότε αντί για τον τελεστή αναζήτησης $U_G = -J_s J_{x_0}$ μπορούμε να θεωρούμε τον

$$U_G = -UJ_{|s\rangle}U^{\dagger}J_{x_0} = -J_{U|s\rangle}J_{x_0}$$

όπου U είναι τυχαίο στοιχείο της ομάδας $SU(2)$. Αυτό σημαίνει ότι πάνω στο διάνυσμα εκκίνησης $|s\rangle$ δρα πρώτα μια τυχαία στροφή η οποία είναι ένας μοναδιακός τελεστής και παράγεται από την αντίστοιχη Χαμιλτονιανή H του συστήματος μέσω της ισότητας

$$U = \exp\left(-i\hbar t H\right).$$

Επιλέγουμε να είναι $U = U_{\pi/4}$, δηλαδή μια $\pi/4$-στροφή και έστω $H_{\pi/4}$ η αντίστοιχη Χαμιλτονιανή για την οποία είναι

$$U_{\pi/4} = \exp\left(-iH_{\pi/4}\right) \qquad \text{με} \quad t = 1, \hbar = 1.$$

Σκοπός μας είναι να αντικαταστήσουμε αυτή τη στροφή με μια απεικόνιση στην οποία θα υπεισέρχεται ο κβαντικός θόρυβος, και γι' αυτό θα βρούμε πρώτα πώς διαταράσσεται η $\pi/4$-στροφή εξαιτίας του εξωτερικού θορύβου.
Γνωρίζουμε ότι (**[9] Chuang-Yamamoto**) για να βρούμε την πραγματική Χαμιλτονιανή μιας Κβαντικής λογικής πύλης πρέπει να προσθέσουμε στην ιδανική Χαμιλτονιανή έναν όρο ο οποίος στην περίπτωση διαταραχής της γωνίας που είναι και αυτή που μας ενδιαφέρει, είναι ο

$$\frac{x}{2}(I-\sigma_z)\otimes\sigma_y$$

όπου ο μη αρνητικός αριθμός $x \geq 0$ δηλώνει την επίδραση του περιβάλλοντος.
Τότε, υπό την επίδραση αυτού του θορύβου, η Χαμιλτονιανή $H_{\pi/4}$ του συστήματος γίνεται:

$$H_R = H_{\frac{\pi}{4}} + H_{env} = \frac{\pi}{4}\sigma_y \otimes I + \frac{x}{2}(I-\sigma_z)\otimes\sigma_y \ .$$

► Κατασκευή του μοναδιακού τελεστή εξέλιξης

Σύμφωνα με τα παραπάνω ο αντίστοιχος μοναδιακός τελεστής εξέλιξης στον οποίο έχει ληφθεί υπόψη ο θόρυβος θα είναι:

$$\begin{aligned} U_R &= \exp(-iH_R) \\ &= \exp\left(-i\left(\frac{\pi}{4}\sigma_y\otimes I + \frac{x}{2}\left(I-\sigma_z\right)\otimes\sigma_y\right)\right) \\ &= \exp\left(-\frac{i\pi}{4}\sigma_y\otimes I - \frac{ix}{2}I\otimes\sigma_y + \frac{ix}{2}\sigma_z\otimes\sigma_y\right) \end{aligned}$$

ή ισοδύναμα

$$\boxed{U_R = \exp\left(I\otimes\left(-ix/2\right)\sigma_y\right)\cdot\exp\left(\sigma_y\otimes\left(-i\pi/4\right)I + \sigma_z\otimes\left(ix/2\right)\sigma_y\right)} \quad (1).$$

Η τελευταία ισχύει διότι ο πίνακας $I\otimes\left(-ix/2\right)\sigma_y$ είναι πολλαπλάσιο της μονάδας, άρα θα μετατίθεται με τον $\sigma_y\otimes\left(-i\pi/4\right)I + \sigma_z\otimes\left(ix/2\right)\sigma_y$.
Θα υπολογίσουμε τώρα τα εκθετικά που εμφανίζονται στην (1). Για τον πρώτο όρο του γινομένου έχουμε ότι ισχύει:

$$\begin{aligned} \exp\left(I\otimes\left(-ix/2\right)\sigma_y\right) &= \exp\begin{pmatrix}\left(-ix/2\right)\sigma_y & 0\\ 0 & \left(-ix/2\right)\sigma_y\end{pmatrix} \\ &= \begin{pmatrix}\exp\left(-ix/2\right)\sigma_y & 0\\ 0 & \exp\left(-ix/2\right)\sigma_y\end{pmatrix}. \end{aligned}$$

Για τον δεύτερο όρο θα χρησιμοποιήσουμε την παρακάτω ειδική μορφή της ταυτότητας Baker-Campbell-Hausdorff (BCH formula) :

$$\exp\left(\sigma_x\otimes\alpha_1 + \sigma_y\otimes\alpha_2 + \sigma_z\otimes\alpha_3\right) = \left(\cosh\alpha\right)\otimes I + \left(\frac{\sinh\alpha}{\alpha}\right)\left(\sigma_x\otimes\alpha_1 + \sigma_y\otimes\alpha_2 + \sigma_z\otimes\alpha_3\right)$$

στην οποία είναι $\alpha = \left(\alpha_1^2+\alpha_2^2+\alpha_3^2\right)^{1/2}$.
Για να εφαρμόσουμε αυτή την ταυτότητα στη συγκεκριμένη περίπτωση θεωρούμε

$$\alpha_1 = 0\,,\ \alpha_2 = \left(-i\pi/4\right)I \ \text{ και } \ \alpha_3 = \left(ix/2\right)\sigma_y\,.$$

Τότε θα είναι

$$\alpha = \left(\alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)^{1/2} = i\mu(x) I\,, \qquad \text{με } \mu(x) = \sqrt{\frac{x^2}{4} + \frac{\pi^2}{16}} \text{ για } x \geq 0\,.$$

Είναι φανερό ότι $\mu(x) > 0$ για κάθε $x \geq 0$, άρα ο α αντιστρέφεται και

$$\alpha^{-1} = \frac{-i}{\mu(x)} I\,.$$

Ακόμα

$$\cosh\alpha = \frac{1}{2}\left(\exp\alpha + \exp(-\alpha)\right)$$

$$= \frac{1}{2}\left[\exp\begin{pmatrix} i\mu(x) & 0 \\ 0 & i\mu(x) \end{pmatrix} + \exp\begin{pmatrix} -i\mu(x) & 0 \\ 0 & -i\mu(x) \end{pmatrix}\right]$$

$$= \frac{1}{2}\left[\begin{pmatrix} \exp(i\mu(x)) & 0 \\ 0 & \exp(i\mu(x)) \end{pmatrix} + \begin{pmatrix} \exp(-i\mu(x)) & 0 \\ 0 & \exp(-i\mu(x)) \end{pmatrix}\right].$$

Άρα $\cosh\alpha = \cos\mu(x) I$ και με αντίστοιχο τρόπο θα είναι $\sinh\alpha = i\sin\mu(x) I$.
Εφαρμόζοντας την ταυτότητα BCH και αντικαθιστώντας τα γνωστά θα έχουμε ότι

$$\exp\left(\sigma_y \otimes (-i\pi/4) I + \sigma_z \otimes (ix/2)\sigma_y\right) =$$

$$= (\cosh\alpha) \otimes I + \left(\frac{\sinh\alpha}{\alpha}\right)\left(\begin{pmatrix} 0 & -(\pi/4) I \\ (\pi/4) I & 0 \end{pmatrix} + \begin{pmatrix} (ix/2)\sigma_y & 0 \\ 0 & -(ix/2)\sigma_y \end{pmatrix}\right)$$

$$= \begin{pmatrix} \cos\mu(x) I + \dfrac{ix\sin\mu(x)}{2\mu(x)}\sigma_y & -\dfrac{\pi\sin\mu(x)}{4\mu(x)} I \\ \dfrac{\pi\sin\mu(x)}{4\mu(x)} I & \cos\mu(x) I - \dfrac{ix\sin\mu(x)}{2\mu(x)}\sigma_y \end{pmatrix}.$$

Παρατηρούμε τώρα ότι στην (1) έχουμε ένα γινόμενο πινάκων των οποίων τα στοιχεία προκύπτουν μετά από πράξεις μεταξύ των

$$I, \cos\mu(x) I, \sigma_y \quad \text{και} \quad \exp\left(-(ix/2)\sigma_y\right) = \cos(x/2) I - i\sin(x/2)\sigma_y$$

οι οποίοι μετατίθενται ανά οποιαδήποτε δυο. Επομένως θα είναι

$$\boxed{U_R = \begin{pmatrix} \left(\cos\mu(x) I + \dfrac{ix}{2}\delta(x)\sigma_y\right) e^{\frac{-ix\sigma_y}{2}} & -\dfrac{\pi}{4}\delta(x) e^{\frac{-ix\sigma_y}{2}} \\ \dfrac{\pi}{4}\delta(x) e^{\frac{-ix\sigma_y}{2}} & \left(\cos\mu(x) I - \dfrac{ix}{2}\delta(x)\sigma_y\right) e^{\frac{-ix\sigma_y}{2}} \end{pmatrix}} \quad (2)$$

έχοντας συμβολίσει $\delta(x) = \sin\mu(x)/\mu(x)$.

Ο παραπάνω πίνακας δίνει τον τελεστή μιας $\pi/4$-στροφής στην οποία έχει προσμετρηθεί ο θόρυβος που εισάγει το εξωτερικό περιβάλλον και παρατηρούμε ότι για $x = 0$ ισχύει το αναμενόμενο $U_R = U_{\pi/4} \otimes I$ ■

2.2.2. Κατασκευή των τριών τελεστών αναζήτησης υπό την επίδραση Κβαντικού θορύβου.

► Επαναδιατύπωση του αλγόριθμου Grover

Αρχικά παρατηρούμε ότι ο γνωστός αλγόριθμος Grover μπορεί να επαναδιατυπωθεί ισοδύναμα με τον ακόλουθο τρόπο: Αντί να αναζητούμε το στοιχείο $|x_0\rangle$ μέσα από τη βάση δεδομένων $D = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$, μπορούμε να θεωρήσουμε την βάση δεδομένων $\Pi = \{|i\rangle\langle i|\}_{i=1}^{N} = \{\rho_i\}_{i=1}^{N}$ που ορίζεται από τους αντίστοιχους προβολικούς τελεστές (καθαρές καταστάσεις) των στοιχείων της D και να ζητάμε τον ρ_{x_0}. Στην περίπτωση αυτή ο αντίστοιχος τελεστής αναζήτησης θα απεικονίζει το ρ_s στο $U_G \rho_s U_G^{\dagger}$.
Αυτό προκύπτει φυσιολογικά αν σκεφτούμε ότι τώρα πλέον ζητάμε να βρούμε έναν πίνακα πυκνότητας και η εξέλιξη ενός τέτοιου πίνακα γενικά δίνεται από την ισότητα:

$$\rho' = X\rho X^{\dagger}$$

για κάποιον μοναδιακό X. Ακριβέστερα δίνεται από την απεικόνιση:

$$AdX : \Pi \to \Pi \qquad \text{(α)} \qquad \text{ώστε}$$

$$\Pi \ni \rho \to AdX(\rho) = X\rho X^{\dagger}$$

για κάποιον μοναδιακό X. Επιπλέον, αν οι X, Y είναι κάποιοι μοναδιακοί, η εξέλιξη του ρ υπό τις διαδοχικές δράσεις των X και Y θα δίνεται από την:

$$AdXY(\rho) = AdX(AdY(\rho))$$

διότι προφανώς είναι

$$\begin{aligned} AdXY(\rho) &= XY\rho(XY)^{\dagger} \\ &= X\left(Y\rho Y^{\dagger}\right)X^{\dagger}. \end{aligned}$$

Στη συνέχεια, εργαζόμενοι σε αυτό το πλαίσιο, θα δείξουμε περιληπτικά το ήδη γνωστό αποτέλεσμα για την επιτυχία του αλγόριθμου σε $O\left(\sqrt{N}\right)$ επαναλήψεις.

Ο αντίστοιχος τελεστής αναζήτησης Grover θα δρα τώρα στο ρ_s ως εξής:

$$\begin{aligned} E_G(\rho_s) \equiv AdUAdI_sAdU^{+}AdI_{x_0}(\rho_s) &= Ad\left(UI_sU^{\dagger}I_{x_0}\right) \\ &= AdU_G \\ &= U_G\rho_sU_G^{\dagger}. \end{aligned}$$

Λαμβάνοντας υπ' όψιν ότι $U = U_{\pi/4} = R_{\pi/4}$ και τα λήμματα 0.2. και 0.3. θα είναι

$$U_G = -R_{\pi/4}I_{\vartheta}R_{\pi/4}{}^{\dagger}I_{\pi} = I_{\vartheta-\pi/2}I_0 = R_{\pi/2-\vartheta} = R_{\pi/2-\vartheta} = e^{i\sigma_y(\pi/2-\vartheta)}$$

άρα $$E_G(\rho_s) = e^{i\sigma_y(\pi/2-\vartheta)}\rho_s e^{-i\sigma_y(\pi/2-\vartheta)}$$

και $$E_G^m(\rho_s) \equiv \rho_s^{(m)} = e^{i\sigma_y m(\pi/2-\vartheta)}\rho_s e^{-i\sigma_y m(\pi/2-\vartheta)}.$$

Από την διαγωνοποίηση του ρ_s προκύπτει ότι

$$\rho_s = \begin{pmatrix} 1/\sqrt{N} & -\sqrt{(N-1)/N} \\ \sqrt{(N-1)/N} & 1/\sqrt{N} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{N} & \sqrt{(N-1)/N} \\ -\sqrt{(N-1)/N} & 1/\sqrt{N} \end{pmatrix}$$

και επειδή είναι $\rho_{x_0} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

θα έχουμε ότι:

$$\rho_s = \exp\left(i\alpha\sigma_y\right) \cdot \rho_{x_0} \cdot \exp\left(-i\alpha\sigma_y\right), \text{ με } \alpha = \cos^{-1}(1/\sqrt{N}).$$

Άρα θα είναι

$$E_G^m(\rho_s) \equiv \rho_s^{(m)} = e^{i\sigma_y\left[m(\pi/2-\vartheta)+\alpha\right]} \rho_{x_0} e^{-i\sigma_y\left[m(\pi/2-\vartheta)+\alpha\right]}$$

ή

$$E_G^m(\rho_s) \equiv \rho_s^{(m)} = \begin{pmatrix} \cos^2\omega & -\sin\omega\cos\omega \\ -\sin\omega\cos\omega & \sin^2\omega \end{pmatrix}, \text{ με } \quad \omega = m\left(\pi/2-\vartheta\right)+\alpha.$$

Ως γωνιακή αξιοπιστία ορίζεται ο αριθμός

$$f_a \equiv \cos\gamma = \frac{\left\langle E_G^m(\rho_s), \rho_{x_0} \right\rangle}{\left\| E_G^m(\rho_s) \right\| \left\| \rho_{x_0} \right\|}$$

όπου το εσωτερικό γινόμενο είναι $\left\langle E_G^m(\rho_s), \rho_{x_0} \right\rangle = \frac{1}{2} Tr(E_G^m(\rho_s)\rho_{x_0})$.

Μετά τις πράξεις θα πάρουμε ότι

$$f_a = \cos^2\left[m\left(\pi/2-\vartheta\right)+\alpha\right].$$

Χωρίς βλάβη της γενικότητας μπορούμε να θεωρούμε ότι το πλήθος m των επαναλήψεων είναι άρτιος θετικός ακέραιος, δηλ. $m = 2k$, άρα

$$f_a = \cos^2\left(-2k\vartheta+\alpha\right) = \cos^2\left(-m\vartheta+\alpha\right).$$

Με επιχειρήματα αντίστοιχα με αυτά της Πρότασης 1.2. έχουμε ότι $m = O\left(\sqrt{N}\right)$ ■

Το γεγονός ότι θέλουμε να αντικαταστήσουμε την $\pi/4$-στροφή η οποία είναι η δράση ενός μοναδιακού τελεστή με έναν άλλο μη μοναδιακό τελεστή στον οποίο θα εμφανίζεται η επίδραση του περιβάλλοντος, σημαίνει ότι πλέον η αναζήτηση εμπλέκει μικτές καταστάσεις. Άρα η εξέλιξη του ρ δεν θα περιγράφεται πλέον από την παραπάνω απεικόνιση (α) αλλά από μια γενικότερη η οποία θα απεικονίζει το σύνολο Π προβολικών τελεστών στην κυρτή του θήκη

$$f : \Pi \to hull(\Pi) \qquad \text{ώστε τώρα}$$

$$\Pi \ni \rho \mapsto f(\rho) = \left(AdW_0 I_s W_0^+ I_{x_0} + AdW_1 I_s W_1^+ I_{x_0} \right)(\rho)$$

όπου τα W_0, W_1 θα είναι οι γεννήτορες ενός CPTP. Επιλέγοντας κατάλληλα αυτούς τους γεννήτορες θα κατασκευάσουμε τους τρεις τελεστές αναζήτησης που προαναγγείλαμε.

► Κατασκευή του πρώτου και γενικότερου τελεστή αναζήτησης E_R

Σύμφωνα με τα παραπάνω ο γενικός τελεστής αναζήτησης Grover υπό κβαντικό θόρυβο θα είναι μια απεικόνιση της μορφής

$$E_R : \Pi \to hull(\Pi)$$
$$E_R = AdR_0 I_s R_0^\dagger I_{x_0} + AdR_1 I_s R_1^\dagger I_{x_0}$$

όπου οι $\{R_0, R_1\}$ είναι οι γεννήτορες ενός CPTP και ως γνωστό ισχύει η συνθήκη Kraus:

$$\sum_{i=0,1} R_i^\dagger R_i = I$$

Επίσης είναι

$$R_i = \langle i | U_R | 0 \rangle \qquad \text{με } i = 0,1.$$

Έχοντας υπολογίσει στην προηγούμενη παράγραφο τον τελεστή U_R είμαστε έτοιμοι να αποδείξουμε την παρακάτω πρόταση.

<u>Πρόταση 2.2.1.</u> :

Η απεικόνιση

$$E_R : \Pi \to hull(\Pi)$$
$$E_R = AdR_0 I_s R_0^\dagger I_{x_0} + AdR_1 I_s R_1^\dagger I_{x_0}$$

η οποία επάγεται από το CPTP που έχει γεννήτορες $R_i = \langle i | U_R | 0 \rangle$ με $i = 0,1$, *ορίζεται από τους τελεστές*

$$R_0 = (\cos \mu(x) I + \tfrac{ix}{2} \delta(x) \sigma_y) e^{-\frac{ix}{2}\sigma_y} \text{ και } R_1 = \frac{\pi}{4} \delta(x) e^{-\frac{ix}{2}\sigma_y}$$

$$\text{με } \delta(x) = \sin \mu(x) / \mu(x),\ \mu(x) = \sqrt{\frac{x^2}{4} + \frac{\pi^2}{16}},\ x \geq 0.$$

Απόδειξη :

Είναι γνωστό [12] ότι η CPTP απεικόνιση που αντιστοιχεί στον U_R δίνεται από την ισότητα

$$\rho \to Tr_{env}(U_R \rho \otimes |0\rangle\langle 0| U_R^\dagger) = \sum_{i=0,1} R_i \rho R_i^\dagger$$

και ότι ισχύει

$$R_i = \langle i | U_R | 0 \rangle \quad \text{με } i = 0,1 .$$

Αντικαθιστώντας σε αυτή τον U_R που έχουμε ήδη βρει και $|0\rangle = (0 \quad 1)^T$, $|1\rangle = (1 \quad 0)^T$ προκύπτουν αμέσως οι παραπάνω τελεστές Kraus ■

Σχόλιο: Ο συμβολισμός που εισήχθη σε αυτή την πρόταση θα εξακολουθήσει να χρησιμοποιείται και σε όλα τα επόμενα εκτός αν κάπου δηλωθεί κάτι διαφορετικό.

► **Κατασκευή του δεύτερου και του τρίτου τελεστή αναζήτησης**

Μετά από την κατασκευή του γενικού τελεστή αναζήτησης, σκεπτόμαστε ότι θα ήταν επίσης λογικό να κατασκευάσουμε και έναν άλλο τελεστή αναζήτησης με ένα πιο εκλεπτυσμένο κριτήριο, την μοναδιακότητα των τελεστών Kraus, η οποία είναι γενικά μια απολύτως επιθυμητή ιδιότητα, αφού όπως έχουμε ήδη δει ο αλγόριθμος επιτρέπει ελευθερία ως προς την ομάδα $SU(2)$. Αυτό μπορεί να διερευνηθεί με δυο τρόπους:

1ος τρόπος:

Εξετάζοντας πότε οι R_0, R_1 είναι συγχρόνως μοναδιακοί.

2ος τρόπος:

Εξετάζοντας για ποιες τιμές του θορύβου οι γεννήτορες γίνονται οι πλησιέστεροι μοναδιακοί στους ήδη υπάρχοντες R_0, R_1. Τότε ο νέος τελεστής θα είναι γεωμετρικά η βέλτιστη προσέγγιση στον ήδη υπάρχοντα E_R αλλά και θα διατηρεί ως ένα βαθμό την ιδιότητα της μοναδιακότητας.

Σύμφωνα με την πρώτη από τις ανωτέρω οπτικές γωνίες, παρατηρούμε ότι από την μορφή των R_0, R_1 (γινόμενο εκθετικού του σ_y με έναν άλλο τελεστή) προκύπτει ότι για να είναι και οι δυο συγχρόνως μοναδιακοί είτε κάποιος από αυτούς μηδέν, θα πρέπει είτε $\cos\mu(x) = 0$, είτε $\sin\mu(x) = 0$, αντίστοιχα.

Πράγματι, αν είναι $\sin\mu(x) = 0$, τότε $\delta(x) = \sin\mu(x)/\mu(x) = 0$, άρα

$$R_0 = \pm \exp\left(-(ix/2)\sigma_y\right) \text{ και } R_1 = 0 .$$

Από την $\sin\mu(x) = 0$ έπεται ότι: $x_\kappa = \pi\sqrt{4\kappa^2 - \frac{1}{4}}$ με $\kappa \in \mathbb{N}_+$. Στο εξής, αυτές οι τιμές του θορύβου θα ονομάζονται **«x πρώτου είδους»** και το σύνολό τους θα συμβολίζεται

$$G_1 = \left\{ x_\kappa > 0 : x_\kappa = \pi\sqrt{4\kappa^2 - \frac{1}{4}} \right\}, \ \kappa \in \mathbb{N}_+ .$$

Στην περίπτωση αυτή παρατηρούμε ότι **ο θόρυβος δεν επηρεάζει τον αλγόριθμο διότι ο τελεστής αναζήτησης ανάγεται στην adjoint δράση ενός μοναδιακού πίνακα**

$U_G = R_0(x)$ με $x \in G_1$, άρα και ο αλγόριθμος ανάγεται ακριβώς στην μορφή που περιέγραψε ο Grover.

Αν τώρα είναι $\cos\mu(x) = 0$, τότε $x_\lambda = \pi\sqrt{4\lambda^2 + 4\lambda + 3/4}$, με $\lambda \in \mathbb{N} \bigcup \{0\}$.

Αντίστοιχα με τα παραπάνω, αυτές τις τιμές του θορύβου θα τις ονομάζουμε **«x δεύτερου είδους»** και το σύνολό τους θα συμβολίζεται

$$G_2 = \left\{ x_\lambda > 0 : x_\lambda = \pi\sqrt{4\lambda^2 + 4\lambda + 3/4} \right\},\ \lambda \in \mathbb{N}.$$

Για $x = x_\lambda$ θα έχουμε

$$\mu(x_\lambda) = \sqrt{\frac{x_\lambda^{\,2}}{4} + \frac{\pi^2}{16}} = \lambda\pi + \pi/2,\ \ \cos\mu(x_\lambda) = 0,$$

και

$$\delta^2(x_\lambda) = \frac{\sin^2(\mu(x_\lambda))}{\mu^2(x_\lambda)} = \frac{1}{(\lambda\pi + \pi/2)^2} > 0$$

άρα $$\delta(x_\lambda) = \pm\frac{1}{\lambda\pi + \pi/2}.$$

Επομένως οι αρχικοί τελεστές Kraus θα γίνουν:

$$R_0 = (\cos\mu(x_\lambda) I + \tfrac{ix_\lambda}{2}\delta(x_\lambda)\sigma_y) e^{-\frac{ix_\lambda}{2}\sigma_y} \ \text{ και } \ R_1 = \frac{\pi}{4}\delta(x_\lambda) e^{-\frac{ix_\lambda}{2}\sigma_y}$$

ή

$$R_0 = \tfrac{ix_\lambda}{2}\delta(x_\lambda)\sigma_y e^{-\frac{ix_\lambda}{2}\sigma_y} \neq 0 \ \text{ και } \ R_1 = \frac{\pi}{4}\delta(x_\lambda) e^{-\frac{ix_\lambda}{2}\sigma_y} \neq 0$$

και είναι και οι δυο μοναδιακοί.

Οι τιμές του $x > 0$ για τις οποίες είναι $x \notin G_1 \bigcup G_2$ θα θεωρούνται ως **«x τρίτου είδους»**, και δεν θα χρησιμοποιήσουμε κάποιο ιδιαίτερο σύμβολο για το σύνολό τους.

Παρατήρηση :

Από την κατασκευή των συνόλων G_1, G_2 είναι προφανές ότι ισχύει

$$G_1 \bigcap G_2 = \varnothing,$$

η ένωσή τους είναι το σύνολο

$$G \equiv G_1 \bigcup G_2 = \left\{ x_n > 0 : x_n = \pi\sqrt{n^2 - \frac{1}{4}} \right\} \ \text{με } n \in \mathbb{N}$$

και επίσης $x_\kappa = x_{2n}$, $x_\lambda = x_{2n+1}$.

Παρατηρούμε ακόμα ότι τα σημεία (n, x_n) με $n \in \mathbb{N}$ ανήκουν στον δεξιό κλάδο της υπερβολής (C) με εξίσωση

$$\frac{x^2}{(1/2)^2} - \frac{y^2}{(\pi/2)^2} = 1.$$

Η υπερβολή αυτή έχει πλάγιες ασύμπτωτες τις ευθείες $(\varepsilon_1), (\varepsilon_2)$ με εξισώσεις $\psi = \pi x$ και $\psi = -\pi x$ αντίστοιχα.

Αυτό σημαίνει ότι καθώς $n \to +\infty$ η ασυμπτωτική συμπεριφορά των «x πρώτου και δεύτερου είδους» θα είναι $x_n \approx \pi n$, με $n \in \mathbb{N}$.

► **Ο δεύτερος τελεστής αναζήτησης** E_W

Ο δεύτερος τελεστής αναζήτησης E_W κατασκευάζεται από τα « x δεύτερου είδους» σύμφωνα με τον ακόλουθο ορισμό.

Ορισμός 2.2.1. :

Ορίζουμε ως

$$E_W : \Pi \to hull(\Pi)$$
$$E_W = AdW_0 I_s W_0^\dagger I_{x_0} + AdW_1 I_s W_1^\dagger I_{x_0},$$

την απεικόνιση η οποία επάγεται από το CPTP που έχει γεννήτορες

$$W_0 = \tfrac{ix_\lambda}{2}\delta(x_\lambda)\sigma_y e^{-\frac{ix_\lambda}{2}\sigma_y} \quad \text{και} \quad W_1 = \frac{\pi}{4}\delta(x_\lambda)e^{-\frac{ix_\lambda}{2}\sigma_y},\ x_\lambda \in G_2.$$

Παρατήρηση:

Είναι φανερό ότι οι W_0, W_1 είναι αριθμητικά πολλαπλάσια μοναδιακών τελεστών αλλά όχι μοναδιακοί, και ότι πληρούν την συνθήκη Kraus αφού είναι ειδικές περιπτώσεις των R_0, R_1.

► **Ο τρίτος τελεστής αναζήτησης** E_V

Στη συνέχεια θα κατασκευάσουμε τον τρίτο τελεστή αναζήτησης ακολουθώντας την δεύτερη από τις προαναφερθείσες οπτικές γωνίες. Θα δούμε ότι αυτό μπορεί να γίνει αν και μόνο αν ο θόρυβος δεν παίρνει τις τιμές των « x πρώτου είδους», δηλαδή αν και μόνο αν ο αλγόριθμος δεν επανέρχεται στην κλασική του μορφή. Οι τιμές των « x δεύτερου είδους» είναι επιτρεπτές σ' αυτή την κατασκευή και μάλιστα οδηγούν σε μια ιδιαίτερα ενδιαφέρουσα ειδική περίπτωση. Όπως θα δούμε στην μελέτη της αξιοπιστίας του αλγόριθμου, για αυτές τις τιμές ο τελεστής $E_V(\rho_s)$ γίνεται προβολικός.

.

Πρόταση 2.2.2. :

Έστω E_V *η απεικόνιση*

$$E_V : \Pi \to hull(\Pi)$$

η οποία παράγεται από το CPTP με μοναδιακούς γεννήτορες $Y_0 = \frac{1}{\sqrt{2}}V_0$, $Y_1 = \frac{1}{\sqrt{2}}V_1$ *, ώστε οι* V_0, V_1 *να είναι οι πλησιέστεροι μοναδιακοί προς τους* R_0, R_1.

Τότε θα ισχύουν

$$V_0 = \left(R_0 R_0^\dagger\right)^{-1/2} \cdot R_0 = e^{i(\psi(x)-\frac{x}{2})\sigma_y} \qquad \textit{και}$$
$$V_1 = \left(R_1 R_1^\dagger\right)^{-1/2} \cdot R_1 = e^{-\frac{ix}{2}\sigma_y},$$

με τη συνάρτηση $\psi(x)$ *να ορίζεται από την ισότητα*

$$[\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)]\cos^2\psi(x)=\cos^2\mu(x)$$

και την μη αρνητική πραγματική παράμετρο x *που δηλώνει την επίδραση του περιβάλλοντος να παίρνει τιμές από το σύνολο* $[0,+\infty)\setminus G_1$

Απόδειξη :

Χρησιμοποιώντας τα αποτελέσματα της Πρότασης 2.2.1. έχουμε ότι:

$$\left(R_0R_0^\dagger\right)^{1/2}=\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}I$$

άρα $$\det\left(\left(R_0R_0^\dagger\right)^{1/2}\right)=\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}.$$

Παρατηρούμε ότι για $x>0$ είναι

$$\det\left(\left(R_0R_0^\dagger\right)^{1/2}\right)=\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}>0$$

και για $x=0$ είναι

$$\det\left(\left(R_0R_0^\dagger\right)^{1/2}\right)=\left(\cos^2\mu(0)\right)^{1/2}=1/\sqrt{2}>0\,.$$

Αυτό σημαίνει ότι ο πίνακας $\left(R_0R_0^\dagger\right)^{1/2}$ είναι αντιστρέψιμος για κάθε $x\geq 0$ και

$$\left(R_0R_0^\dagger\right)^{-1/2}=\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{-1/2}I\ .$$

Τότε ο πλησιέστερος μοναδιακός προς τον R_0 θα είναι ο $V_0=\left(R_0R_0^\dagger\right)^{-1/2}R_0$, δηλαδή ο

$$V_0=\left[\frac{\cos\mu(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}}\cdot I+i\frac{\frac{x}{2}\delta(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}}\cdot\sigma_y\right]\cdot e^{-\frac{ix}{2}\sigma_y}.$$

Εξ' αιτίας της ισότητας

$$\left(\frac{\cos\mu(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}}\right)^2+\left(\frac{\frac{x}{2}\delta(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}}\right)^2=1$$

θα υπάρχει γωνία $\psi(x)$ ώστε να ισχύουν οι

$$\cos\psi(x)=\frac{\cos\mu(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}} \quad \text{και} \quad \sin\psi(x)=\frac{\frac{x}{2}\delta(x)}{\left(\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right)^{1/2}}.$$

Επίσης θα είναι:

$$\left[\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right]\cdot\cos^2\psi(x)=\cos^2\mu(x).$$

Συνεπώς

$$\boxed{\frac{1}{\sqrt{2}}V_0=\frac{1}{\sqrt{2}}\left(\cos\psi(x)+i\sin\psi(x)\sigma_y\right)\cdot e^{-\frac{ix}{2}\sigma_y}=\frac{1}{\sqrt{2}}e^{i\left(\psi(x)-\frac{x}{2}\right)\sigma_y}}.$$

Ακολουθώντας αντίστοιχη διαδικασία για τον δεύτερο γεννήτορα αρχικά θα έχουμε ότι

$$\left(R_1R_1^\dagger\right)^{1/2}=\frac{\pi}{4}\delta(x)I\ .$$

Ο πίνακας αυτός έχει ορίζουσα

$$\det\left(\left(R_1R_1^\dagger\right)^{1/2}\right)=\frac{\pi}{4}\delta(x)$$

η οποία είναι **ίση με μηδέν** αν και μόνο αν

$$\delta(x)=0 \ \text{ή} \ \sin\mu(x)=0$$

ή

$$\sqrt{\frac{x^2}{4}+\frac{\pi^2}{16}}=\kappa\pi$$

ή

$$x=\pi\sqrt{4\kappa^2-\frac{1}{4}} \quad \text{με} \ \kappa\in\mathbb{N}_+$$

άρα αν και μόνο αν $x\in G_1$.

Επομένως διακρίνουμε τις εξής δυο περιπτώσεις:

1) Αν $x\notin G_1$ τότε υπάρχει ο αντίστροφος του πίνακα $\left(R_1R_1^\dagger\right)^{1/2}$ και είναι ο

$$\left(R_1R_1^\dagger\right)^{-1/2}=\frac{4}{\pi\delta(x)}I\ .$$

Τότε ο πλησιέστερος μοναδιακός προς τον R_1 θα είναι ο $V_0=\left(R_1R_1^\dagger\right)^{-1/2}R_1$, δηλαδή ο

$$\boxed{V_1=\left(R_1R_1^\dagger\right)^{-1/2}R_1=e^{-\frac{ix}{2}\sigma_y}}$$

οπότε θα είναι

$$\boxed{\frac{1}{\sqrt{2}}V_1 = \frac{1}{\sqrt{2}}\left(R_1 R_1^{\dagger}\right)^{-1/2} R_1 = \frac{1}{\sqrt{2}}e^{-\frac{ix}{2}\sigma_y}}.$$

2) Αν $x \in G_1$, τότε $\sin\mu(x) = 0$, άρα $R_0 = \pm\exp\left(-(ix/2)\sigma_y\right)$ και $R_1 = 0$ ■

2.3. Προσδιορισμός της αξιοπιστίας του αλγόριθμου Grover υπό Κβαντικό θόρυβο

Στην συνέχεια θα εξετάσουμε την αποτελεσματικότητα του αλγόριθμου για τους τελεστές αναζήτησης E_R, E_W και E_V. Για το σκοπό αυτό θα υπολογίσουμε *την ακτινική* και *την γωνιακή αξιοπιστία* του αλγόριθμου, οι οποίοι ποσοτικοποιούν δυο εύλογα γεωμετρικά κριτήρια. Γνωρίζουμε ότι κάθε πίνακας πυκνότητας, αναπαριστάνεται με ένα διάνυσμα στη σφαίρα (μπάλα) του Bloch. Η *ακτινική αξιοπιστία* είναι το εσωτερικό γινόμενο δυο διανυσμάτων αυτής της σφαίρας: του διανύσματος που αναπαριστά το αντικείμενο της αναζήτησης με το διάνυσμα που αναπαριστά κάθε στιγμή τη δράση του τελεστή αναζήτησης, ενώ η *γωνιακή αξιοπιστία* είναι το συνημίτονο της γωνίας αυτών των διανυσμάτων όπως αυτό προκύπτει από το εσωτερικό γινόμενο. Μέσω της ακτινικής αξιοπιστίας κατανοούμε την προβολή του ενός διανύσματος πάνω στο άλλο και μέσω της γωνιακής αξιοπιστίας προσδιορίζουμε την γωνία τους. Ακριβέστερα, έστω π.χ. ο τελεστής αναζήτησης

$$E_V = \frac{1}{2}\left(AdV_0 I_s V_0^{\dagger} I_{x_0} + AdV_1 I_s V_1^{\dagger} I_{x_0}\right)$$

ο οποίος δρα στην βάση δεδομένων Π ξεκινώντας από τον πίνακα πυκνότητας $\rho_s = |s\rangle\langle s|$. Μετά από m το πλήθος δράσεις θα έχει παραχθεί το στοιχείο

$$E_V^m(\rho_s) = E_V^m(|s\rangle\langle s|) \in hull(\Pi).$$

Ως *ακτινική αξιοπιστία* του αλγόριθμου ορίζεται το εσωτερικό γινόμενο

$$f_r = \left\langle E_V^m(\rho_s), \rho_{x_0} \right\rangle = \frac{1}{2} Tr(E_V^m(\rho_s)\rho_{x_0})$$

και όπως έχουμε αναφέρει και προηγουμένως, ως γωνιακή αξιοπιστία ορίζεται ο αριθμός

$$f_a \equiv \cos\gamma = \frac{\left\langle E_V^m(\rho_s), \rho_{x_0} \right\rangle}{\left\| E_V^m(\rho_s) \right\| \left\| \rho_{x_0} \right\|}.$$

Αντίστοιχα μεγέθη ορίζουμε και για τον E_W. Για τον E_R, λόγω της υπολογιστικής δυσκολίας που εμφανίζει η παραπάνω αντιμετώπιση, θα χρησιμοποιήσουμε ένα πιο άμεσο γεωμετρικό τρόπο λύσης.

► **Η αξιοπιστία του δεύτερου τελεστή αναζήτησης** E_W

<u>Πρόταση 2.3.1.</u> :

Αν χρησιμοποιηθεί ως τελεστής αναζήτησης ο E_W *, η ακτινική αξιοπιστία του αλγόριθμου καταρρέει εκθετικά, αλλά για πολύ μεγάλες τιμές του θορύβου η γωνιακή αξιοπιστία γίνεται ίση με ένα σε* $O\left(\sqrt{N}\right)$ *επαναλήψεις.*

<u>Απόδειξη</u> :

Σύμφωνα με όσα έχουμε βρει μέχρι τώρα είναι:

$$W_0 = \tfrac{ix_\lambda}{2}\delta(x_\lambda)\sigma_y e^{-\frac{ix_\lambda}{2}\sigma_y} = \tfrac{x_\lambda}{2}\delta(x_\lambda)e^{\frac{i\pi}{2}\sigma_y}e^{-\frac{ix_\lambda}{2}\sigma_y} = \tfrac{x_\lambda}{2}\delta(x_\lambda)e^{-\frac{i(x_\lambda-\pi)}{2}\sigma_y}$$

και

$$W_1 = \frac{\pi}{4}\delta(x_\lambda)e^{-\frac{ix_\lambda}{2}\sigma_y} \quad .$$

Άρα θα είναι:

$$E_W = AdW_0 I_s W_0^\dagger I_{x_0} + AdW_1 I_s W_1^\dagger I_{x_0}$$

ή

$$E_W = \left(W_0 I_s W_0^\dagger I_{x_0}\right)\rho_s\left(W_0 I_s W_0^\dagger I_{x_0}\right)^\dagger + \left(W_1 I_s W_1^\dagger I_{x_0}\right)\rho_s\left(W_1 I_s W_1^\dagger I_{x_0}\right)^\dagger .$$

Εξαιτίας των παραπάνω και των λημμάτων 0.2. και 0.3. θα είναι:

$$W_0 I_s W_0^\dagger I_{x_0} = \tfrac{x_\lambda^2}{4}\delta^2(x_\lambda)e^{-\frac{i(x_\lambda-\pi)}{2}\sigma_y} I_s e^{\frac{i(x_\lambda-\pi)}{2}\sigma_y} I_{x_0}$$

$$= \tfrac{x_\lambda^2}{4}\delta^2(x_\lambda)R_{(\pi-x_\lambda)/2} I_\vartheta R^\dagger_{(\pi-x_\lambda)/2} I_\pi$$
$$= \tfrac{x_\lambda^2}{4}\delta^2(x_\lambda) I_{x_\lambda+\vartheta-\pi} I_\pi$$
$$= \tfrac{x_\lambda^2}{4}\delta^2(x_\lambda)R_{2\pi-x_\lambda-\vartheta}$$
$$= -\tfrac{x_\lambda^2}{4}\delta^2(x_\lambda)R_{\pi-x_\lambda-\vartheta}$$
$$= -\tfrac{x_\lambda^2}{4}\delta^2(x_\lambda)e^{i\sigma_y(\pi-x_\lambda-\vartheta)} \qquad \text{και}$$

$$W_1 I_s W_1^\dagger I_{x_0} = \tfrac{\pi^2}{16}\delta^2(x_\lambda)e^{-\frac{ix_\lambda}{2}\sigma_y} I_s e^{\frac{ix_\lambda}{2}\sigma_y} I_{x_0}$$
$$= \tfrac{\pi^2}{16}\delta^2(x_\lambda)R_{-x_\lambda/2} I_\vartheta R^\dagger_{-x_\lambda/2} I_\pi$$
$$= \tfrac{\pi^2}{16}\delta^2(x_\lambda) I_{\vartheta+x_\lambda} I_\pi$$

$$= \tfrac{\pi^2}{16}\delta^2(x_\lambda)R_{\pi-\vartheta-x_\lambda}$$
$$= \tfrac{\pi^2}{16}\delta^2(x_\lambda)e^{i\sigma_y(\pi-x_\lambda-\vartheta)}.$$

(εδώ ας παρατηρήσουμε ότι και οι δυο όροι ανάγονται τελικά σε αριθμητικά πολλαπλάσια του ίδιου εκθετικού του σ_y).

Επομένως θα είναι

$$E_W(\rho_s) = \left(W_0 I_s W_0^\dagger I_{x_0}\right)\rho_s\left(W_0 I_s W_0^\dagger I_{x_0}\right)^\dagger + \left(W_1 I_s W_1^\dagger I_{x_0}\right)\rho_s\left(W_1 I_s W_1^\dagger I_{x_0}\right)^\dagger$$
$$= \tfrac{x_\lambda^4}{16}\delta^4(x_\lambda)e^{i\sigma_y(\pi-x_\lambda-\vartheta)}\rho_s e^{-i\sigma_y(\pi-x_\lambda-\vartheta)} + \tfrac{\pi^4}{256}\delta^4(x_\lambda)e^{i\sigma_y(\pi-x_\lambda-\vartheta)}\rho_s e^{-i\sigma_y(\pi-x_\lambda-\vartheta)}$$
$$= \tfrac{16x_\lambda^4+\pi^4}{256}\delta^4(x_\lambda)e^{i\sigma_y(\pi-x_\lambda-\vartheta)}\rho_s e^{-i\sigma_y(\pi-x_\lambda-\vartheta)},$$

οπότε για κάθε θετικό ακέραιο m θα έχουμε:

$$E_W^m(\rho_s) = \left(\tfrac{16x_\lambda^4+\pi^4}{256}\right)^m \delta^{4m}(x_\lambda)e^{\left[i\sigma_y m(\pi-x_\lambda-\vartheta)\right]}\rho_s e^{-\left[i\sigma_y m(\pi-x_\lambda-\vartheta)\right]}$$

ή

$$E_W^m(\rho_s) = \left(\tfrac{16x_\lambda^4+\pi^4}{256}\right)^m \delta^{4m}(x_\lambda)e^{i\sigma_y\omega}\rho_s e^{-i\sigma_y\omega}$$
$$\text{με } \omega = m(\pi - x_\lambda - \vartheta).$$

Όπως έχουμε δει, η διαγωνοποίηση του ρ_s δίνει

$$\rho_s = \begin{pmatrix} 1/\sqrt{N} & -\sqrt{(N-1)/N} \\ \sqrt{(N-1)/N} & 1/\sqrt{N} \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1/\sqrt{N} & \sqrt{(N-1)/N} \\ -\sqrt{(N-1)/N} & 1/\sqrt{N} \end{pmatrix}$$

ή $\rho_s = \exp\left(i\alpha\sigma_y\right)\cdot\rho_{x_0}\cdot\exp\left(-i\alpha\sigma_y\right)$, με $\alpha = \cos^{-1}(1/\sqrt{N})$.

Τότε θα είναι

$$E_W^m(\rho_s) = \left(\tfrac{16x_\lambda^4+\pi^4}{256}\right)^m \delta^{4m}(x_\lambda)e^{i\sigma_y(\omega+\alpha)}\rho_{x_0}e^{-i\sigma_y(\omega+\alpha)}$$

$$= \left(\tfrac{16x_\lambda^4+\pi^4}{256}\right)^m \delta^{4m}(x_\lambda)\begin{pmatrix} \cos^2(\omega+\alpha) & -\sin(\omega+\alpha)\cos(\omega+\alpha) \\ -\sin(\omega+\alpha)\cos(\omega+\alpha) & \sin^2(\omega+\alpha) \end{pmatrix}$$

άρα η ακτινική αξιοπιστία θα είναι:

$$f_r = \left\langle E_W^m(\rho_s), \rho_{x_0}\right\rangle = \frac{1}{2}Tr(E_W^m(\rho_s)\rho_{x_0})$$
$$= \frac{1}{2}\left(\tfrac{16x_\lambda^4+\pi^4}{256}\right)^m \delta^{4m}(x_\lambda)\cos^2(\omega+\alpha).$$

Όμως είναι

$x_\lambda = \pi\sqrt{4\lambda^2+4\lambda+3/4}$ και $\delta(x_\lambda) = \pm\dfrac{1}{\lambda\pi+\pi/2}$, οπότε μετά την αντικατάσταση και τις απλοποιήσεις θα πάρουμε:

$$f_r = \left(1 - \frac{32\lambda^2+32\lambda+6}{256\lambda^4+512\lambda^3+352\lambda^2+96\lambda+10}\right)^m \cos^2(\omega+\alpha).$$

Για κάθε τιμή του $\lambda \geq 0$, ο αριθμός που είναι βάση στο παραπάνω εκθετικό είναι θετικός και μικρότερος του ένα, άρα $\lim_{m\to+\infty} f_r = 0$ ως γινόμενο μηδενικής επί φραγμένη.

Η γωνιακή αξιοπιστία θα είναι :

$$f_a \equiv \cos\gamma = \frac{\left\langle E_W^m(\rho_s), \rho_{x_0}\right\rangle}{\left\|E_W^m(\rho_s)\right\|\left\|\rho_{x_0}\right\|}$$
$$= \cos^2(\omega+\alpha).$$

Θα είναι $f_a = 1$ όταν $\cos(\omega+a) = \pm 1$ ή

$\cos(m\pi - mx_\lambda - m\vartheta + a) = \pm 1$ ή

$\cos(-mx_\lambda - m\vartheta + a) = \pm 1$.

Επιλέγοντας «x δευτέρου είδους» με $\lambda \gg 0$ είναι $x_\lambda = \pi\sqrt{4\lambda^2+4\lambda+3/4} \approx 2\pi\lambda$, και η $\cos(-mx_\lambda - m\vartheta + a) = \pm 1$ θα γίνει $\cos(-m\vartheta + a) = \pm 1$, οπότε κατά τα γνωστά έχουμε ότι αυτό συμβαίνει για $m = O\left(\sqrt{N}\right)$ ■

<u>Πρόταση 2.3.2.</u> :

Η ακτινική και η γωνιακή αξιοπιστία του αλγόριθμου Grover με τελεστή αναζήτησης E_V είναι αντίστοιχα

$$f_r = \frac{1+\cos^m\left(2\psi(x)\right)\cos T}{4} \qquad \textit{και}$$

$$f_a \equiv \cos\gamma = \frac{1}{\sqrt{2}}\cdot\frac{1+\cos^m\left(2\psi(x)\right)\cos T}{\sqrt{1+\cos^{2m}\left(2\psi(x)\right)}}, \qquad \textit{θεωρώντας}$$

$T \equiv T(x,N) = 2\left(m\psi(x) - m\gamma_2(x,N) - \alpha\right)$, $\gamma_2(x,N) = \pi + x - \vartheta$,

$\vartheta = \sin^{-1}(-2\sqrt{N-1}/N)$, $\alpha = \cos^{-1}(1/\sqrt{N})$ *και* $x \notin G_1$.

<u>Απόδειξη</u> :

Είναι

$$E_V = \frac{1}{2}\left(AdV_0 I_s V_0^\dagger I_{x_0} + AdV_1 I_s V_1^\dagger I_{x_0}\right)$$

άρα

$$E_V\left(\rho_s\right)=\frac{1}{2}\left[\left(V_0 I_s V_0^{\dagger} I_{x_0}\right)\rho_s\left(V_0 I_s V_0^{\dagger} I_{x_0}\right)^{\dagger}+\left(V_1 I_s V_1^{\dagger} I_{x_0}\right)\rho_s\left(V_1 I_s V_1^{\dagger} I_{x_0}\right)^{\dagger}\right].$$

Χρησιμοποιώντας την γνωστή ταυτότητα

$$\exp\left(i\vartheta\sigma_y\right)=\left(\cos\vartheta\right)I+i\left(\sin\vartheta\right)\sigma_y=R_{\vartheta}\ ,$$

τα Λήμματα 0.2. και 0.3., το ότι οι ανακλάσεις I_{x_0} και I_s είναι ανακλάσεις γωνιών π και ϑ αντίστοιχα, και θεωρώντας $\varphi\left(x\right)=\psi\left(x\right)-\frac{x}{2}$, η παραπάνω ισότητα για το $E_V\left(\rho_s\right)$ γίνεται

$$E_V\left(\rho_s\right)=\frac{1}{2}\left(e^{i\left(\pi-\theta-2\varphi(x)\right)\sigma_y}\rho_s e^{-i\left(\pi-\vartheta-2\varphi(x)\right)\sigma_y}+e^{i\left(\pi+x-\vartheta\right)\sigma_y}\rho_s e^{-i\left(\pi+x-\vartheta\right)\sigma_y}\right)$$

ή

$$E_V\left(\rho_s\right)=\frac{1}{2}e^{i\gamma_1\sigma_y}\rho_s e^{-i\gamma_1\sigma_y}+\frac{1}{2}e^{i\gamma_2\sigma_y}\rho_s e^{-i\gamma_2\sigma_y}$$

ή

$$\boxed{E_V\left(\rho_s\right)=\frac{1}{2}\left(Ade^{i\gamma_1\sigma_y}\left(\rho_s\right)+Ade^{i\gamma_2\sigma_y}\left(\rho_s\right)\right)}$$

με $\gamma_1\equiv\gamma_1\left(x,N\right)=\pi-\theta-2\varphi\left(x\right)$, και $\gamma_2\equiv\gamma_2\left(x,N\right)=\pi+x-\vartheta$.

Οι πίνακες $e^{i\gamma_1\sigma_y}$, $e^{i\gamma_2\sigma_y}$ είναι πίνακες στροφής, άρα αντιμετατίθενται, και επομένως για κάθε θετικό ακέραιο m μπορούμε να εφαρμόσουμε τον τύπο του διωνυμικού αναπτύγματος και να πάρουμε ότι

$$E_V^m\left(\rho_s\right)=\left[\frac{1}{2}\left(Ade^{i\gamma_1\sigma_y}+Ade^{i\gamma_2\sigma_y}\right)\right]^m\left(\rho_s\right)$$

ή

$$\boxed{E_V^m\left(\rho_s\right)=\frac{1}{2^m}\sum_{\nu=0}^{m}\binom{m}{\nu}e^{i\left[(m-\nu)\gamma_2+\nu\gamma_1\right]\sigma_y}\rho_s e^{-i\left[(m-\nu)\gamma_2+\nu\gamma_1\right]\sigma_y}}\quad(3).$$

Από την διαγωνοποίηση του ρ_s προκύπτει ότι

$$\rho_s=\begin{pmatrix}1/\sqrt{N} & -\sqrt{(N-1)/N}\\ \sqrt{(N-1)/N} & 1/\sqrt{N}\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}1/\sqrt{N} & \sqrt{(N-1)/N}\\ -\sqrt{(N-1)/N} & 1/\sqrt{N}\end{pmatrix}$$

ή

$$\rho_s=\begin{pmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}$$

ή

$$\rho_s=\exp\left(i\alpha\sigma_y\right)\cdot\rho_{x_0}\cdot\exp\left(-i\alpha\sigma_y\right).$$

Συνεπώς η (3) ισοδύναμα γράφεται

$$E_V^m\left(\rho_s\right)=\frac{1}{2^m}\sum_{\nu=0}^{m}\binom{m}{\nu}e^{-iA(\nu)\sigma_y}\rho_{x_0}e^{iA(\nu)\sigma_y}\quad ,$$

με $A(\nu)=-[(m-\nu)\gamma_2+\nu\gamma_1+\alpha]$, και σε μορφή 2x2 πίνακα

$$E_V^m\left(\rho_s\right)=\frac{1}{2^{m+1}}\begin{bmatrix}2^m+\sum_{\nu=0}^{m}\binom{m}{\nu}\cos 2A(\nu) & \sum_{\nu=0}^{m}\binom{m}{\nu}\sin 2A(\nu)\\ \sum_{\nu=0}^{m}\binom{m}{\nu}\sin 2A(\nu) & 2^m-\sum_{\nu=0}^{m}\binom{m}{\nu}\cos 2A(\nu)\end{bmatrix}.$$

Εφαρμόζοντας γνωστές τριγωνομετρικές ταυτότητες του Tchebycheff θα έχουμε ότι:

$$\sum_{\nu=0}^{m}\binom{m}{\nu}\cdot\begin{Bmatrix}\cos 2A(\nu)\\ \sin 2A(\nu)\end{Bmatrix}=\sum_{\nu=0}^{m}\binom{m}{\nu}\cdot\begin{Bmatrix}\cos\left(4\psi(x)\nu-2m\gamma_2-2\alpha\right)\\ \sin\left(4\psi(x)\nu-2m\gamma_2-2\alpha\right)\end{Bmatrix}$$

$$=2^m\cos^m\left(2\psi(x)\right)\begin{Bmatrix}\cos\left(2m\psi(x)-2m\gamma_2-2\alpha\right)\\ \sin\left(2m\psi(x)-2m\gamma_2-2\alpha\right)\end{Bmatrix}=2^m\cos^m\left(2\psi(x)\right)\begin{Bmatrix}\cos T\\ \sin T\end{Bmatrix},$$

με $\mathrm{T}=2m\psi(x)-2m\gamma_2-2\alpha$.

Τελικά η αναπαράσταση του $E_V^m\left(\rho_s\right)$ σε μορφή 2x2 πίνακα μπορεί να δοθεί με πιο συμπυκνωμένη γραφή ως

$$\boxed{E_V^m\left(\rho_s\right)=\frac{1}{2}\begin{bmatrix}1+\cos^m\left(2\psi(x)\right)\cos T & \cos^m\left(2\psi(x)\right)\sin T\\ \cos^m\left(2\psi(x)\right)\sin T & 1-\cos^m\left(2\psi(x)\right)\cos T\end{bmatrix}}.$$

Άρα η ακτινική αξιοπιστία θα είναι

$$f_r=\left\langle E_V^m(\rho_s),\rho_{x_0}\right\rangle=\frac{1}{2}Tr(E_V^m(\rho_s)\rho_{x_0})$$

ή

$$f_r=\frac{1+\cos^m\left(2\psi(x)\right)\cos T}{4}$$

και η γωνιακή αξιοπιστία θα είναι

$$f_a=\frac{1}{\sqrt{2}}\cdot\frac{1+\cos^m\left(2\psi(x)\right)\cos T}{\sqrt{1+\cos^{2m}\left(2\psi(x)\right)}}\ \blacksquare$$

► Συμπεράσματα για την αξιοπιστία

Για $x\notin G_1$, είναι $\delta(x)\neq 0,\ \sin\mu(x)\neq 0$.

Επομένως

$$\left|\cos\mu(x)\right|<1 \text{ και } 0\le\cos^2\psi(x)<1$$

διότι $$\left[\cos^2\mu(x)+\frac{x^2}{4}\delta^2(x)\right]\cdot\cos^2\psi(x)=\cos^2\mu(x).$$

Ακόμα είναι $-1\le\cos 2\psi(x)=2\cos^2\psi(x)-1<1$. Αν είναι επιπλέον και $\cos\psi(x)\neq 0$, ή ισοδύναμα $\cos\mu(x)\neq 0$, τότε $x\notin G_1\bigcup G_2$. Άρα $-1<\cos 2\psi(x)<1$ και αυτό σημαίνει ότι για $m\to\infty$ θα είναι $f_r\to 1/4$ και $f_a\to 1/\sqrt{2}$, δηλαδή $\gamma\to\pm\pi/4$. Το αποτέλεσμα αυτό είναι αξιοποιήσιμο σε χρόνο $m=O\left(\sqrt{N}\right)\to\infty$ αποκλειστικά σε πολύ μεγάλες βάσεις δεδομένων. Τότε προκύπτει ότι το διάνυσμα $\overrightarrow{\delta^{(m)}}$ που απεικονίζει στη σφαίρα Bloch το $E_V^m(\rho_s)$ δεν καταλήγει να έχει μηδενικό μήκος (διότι $f_r\to 1/4$), και τείνει να έχει γωνιακή απόσταση $\gamma=\pm\pi/4$ από το αντίστοιχο διάνυσμα για το αντικείμενο αναζήτησης. Άρα μπορούμε να εντοπίσουμε μια περιοχή της διεύθυνσης του τελευταίου στο χώρο. Συγκεκριμένα, το $\overrightarrow{\delta^{(m)}}$ θα ανήκει σε μια περιοχή της επιφάνειας μιας στερεάς γωνίας η οποία έχει κορυφή το κέντρο της μπάλας, ώστε κάθε διάνυσμα στην επιφάνεια αυτής της στερεάς γωνίας να σχηματίζει με το διάνυσμα που αναπαριστά τον τελεστή – στόχο γωνία τείνουσα στο $\pm\pi/4$. **Είναι βέβαια φανερό ότι στην περίπτωση αυτή δεν είναι δυνατόν να εντοπίσουμε το διάνυσμα - στόχο αλλά μπορούμε να κάνουμε το εξής: να κατασκευάσουμε την επιφάνεια S που ορίζεται από τις θέσεις των $\overrightarrow{\delta^{(m)}}$ για $m=O\left(\sqrt{N}\right)\to\infty$, και να βρούμε την περιγεγραμμένη και την εγγεγραμμένη σ' αυτήν (κωνική) στερεά γωνία της μπάλας «εγκλωβίζοντας» έτσι την S μεταξύ δυο στερεών γωνιών. Στη συνέχεια μπορούμε να βρούμε τα ακτινικά διανύσματα της μπάλας τα οποία έχουν φορείς τους άξονες συμμετρίας αυτών των στερεών γωνιών. Το ζητούμενο (μοναδιαίου μήκους) διάνυσμα θα είναι πολύ κοντά σε αυτά τα δυο διανύσματα.**

► Η ειδική περίπτωση του προβολικού τελεστή

<u>Πρόταση 2.3.3.</u> :

Ο τελεστής $E_V(\rho_s)$ είναι προβολικός τελεστής για $x\in G_2$ (x δευτέρου είδους) και για πολύ μεγάλες τιμές του θορύβου ο αλγόριθμος είναι αποτελεσματικός (έχει πιθανότητα επιτυχίας ίση με ένα) σε $O\left(\sqrt{N}\right)$ επαναλήψεις.

<u>Απόδειξη</u> :

Όπως έχουμε δει παραπάνω, αν $x\in G_2$, τότε $\cos\mu(x)=0$ και ισοδύναμα είναι $\cos\psi(x)=0$, άρα $\cos\left(2\psi(x)\right)=2\cos^2\left(\psi(x)\right)-1=-1$.

Αυτό σημαίνει ότι για κάθε $x\in G_2$ και για κάθε θετικό ακέραιο m είναι

$$\rho^{(m)}\equiv E_V^m(\rho_s)=\frac{1}{2}\begin{bmatrix}1+\cos^m\left(2\psi(x)\right)\cos T & \cos^m\left(2\psi(x)\right)\sin T\\ \cos^m\left(2\psi(x)\right)\sin T & 1-\cos^m\left(2\psi(x)\right)\cos T\end{bmatrix}$$

$$=\frac{1}{2}\begin{bmatrix}1+(-1)^m\cos T & (-1)^m\sin T\\ (-1)^m\sin T & 1-(-1)^m\cos T\end{bmatrix}\equiv Q.$$

Θα δείξουμε τώρα ότι ο Q είναι προβολικός τελεστής.

Αυτό μπορεί να γίνει είτε κάνοντας αμέσως τις πράξεις και $Q^2 = \ldots = Q$ κλπ, είτε αν δούμε ότι ο πίνακας Q είναι τύπου 2x2 και έχει ιδιοτιμές μηδέν και ένα, αφού το διάνυσμα ιδιοτιμών του $\rho^{(m)}$ ξέρουμε ότι είναι γενικά το:

$$\lambda_m = \begin{bmatrix} \dfrac{1+\left|\cos^m\left(2\psi(x)\right)\right|}{2} \\ \dfrac{1-\left|\cos^m\left(2\psi(x)\right)\right|}{2} \end{bmatrix}.$$

Θα βρούμε τώρα ένα διάνυσμα $\left|\psi'\right\rangle = \begin{pmatrix} \mu \\ \nu \end{pmatrix}$ ώστε $Q = \left|\psi'\right\rangle\left\langle\psi'\right|$. Ισχύουν οι παρακάτω:

$$Q = \left|\psi'\right\rangle\left\langle\psi'\right|$$

ή

$$\frac{1}{2}\begin{bmatrix} 1+(-1)^m\cos T & (-1)^m \sin T \\ (-1)^m \sin T & 1-(-1)^m\cos T \end{bmatrix} = \begin{bmatrix} \mu^2 & \mu\nu \\ \mu\nu & \nu^2 \end{bmatrix}$$

ή

$$\begin{bmatrix} \dfrac{1+\cos(T+m\pi)}{2} & \dfrac{\sin(T+m\pi)}{2} \\ \dfrac{\sin(T+m\pi)}{2} & \dfrac{1-\cos(T+m\pi)}{2} \end{bmatrix} = \begin{bmatrix} \mu^2 & \mu\nu \\ \mu\nu & \nu^2 \end{bmatrix}$$

ή

$$\begin{bmatrix} \cos^2\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) & \sin\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right)\cos\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \\ \sin\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right)\cos\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) & \sin^2\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \end{bmatrix} = \begin{bmatrix} \mu^2 & \mu\nu \\ \mu\nu & \nu^2 \end{bmatrix}.$$

Από τα διαγώνια στοιχεία θα είναι

$$\begin{cases} \mu = \pm\cos\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \\ \nu = \pm\sin\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \end{cases}$$

και για να επαληθεύεται η ισότητα στα αντιδιαγώνια στοιχεία θα πρέπει:

$$\text{είτε} \quad \begin{cases} \mu = \cos\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \\ \nu = \sin\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \end{cases}, \text{ είτε} \begin{cases} \mu = -\cos\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \\ \nu = -\sin\left(\dfrac{T}{2}+\dfrac{m\pi}{2}\right) \end{cases}$$

Επομένως, με διαφορά ενός προσήμου, θα είναι:

$$|\psi'\rangle = \begin{pmatrix} \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{T}{2} + \frac{m\pi}{2}\right) \\ \sin\left(\frac{T}{2} + \frac{m\pi}{2}\right) \end{pmatrix}$$

Επομένως η πιθανότητα επιτυχίας του αλγόριθμου είναι ίση με :

$$\left|\langle x_0 | \psi' \rangle\right|^2 = \cos^2\left(\frac{T}{2} + \frac{m\pi}{2}\right) = \cos^2\left(m\pi - m\gamma_2 - \alpha\right)$$

$$\boxed{\left|\langle \mathbf{x_0} | \boldsymbol{\psi}' \rangle\right|^2 = \cos^2\left(\mathbf{m\gamma_2 + \alpha}\right)}.$$

Ο αλγόριθμος θα είναι επιτυχής αν $|\psi'\rangle = \pm|x_0\rangle$, δηλαδή όταν

$$\left|\langle x_0 | \psi' \rangle\right|^2 = \cos^2\left(m\gamma_2 + a\right) = 1 \quad \text{ή}$$

$$\cos\left(m\gamma_2 + a\right) = \pm 1 \quad \text{ή}$$

$$\cos\left[m\left(\pi + \pi\sqrt{4\lambda^2 + 4\lambda + 3/4} - \vartheta\right) + \alpha\right] = \pm 1 \quad \text{ή}$$

$$(-1)^m \cos\left[m\left(\pi\sqrt{4\lambda^2 + 4\lambda + 3/4} - \vartheta\right) + \alpha\right] = \pm 1 \quad \text{ή}$$

$$\cos\left[m\left(\pi\sqrt{4\lambda^2 + 4\lambda + 3/4} - \vartheta\right) + \alpha\right] = \pm 1.$$

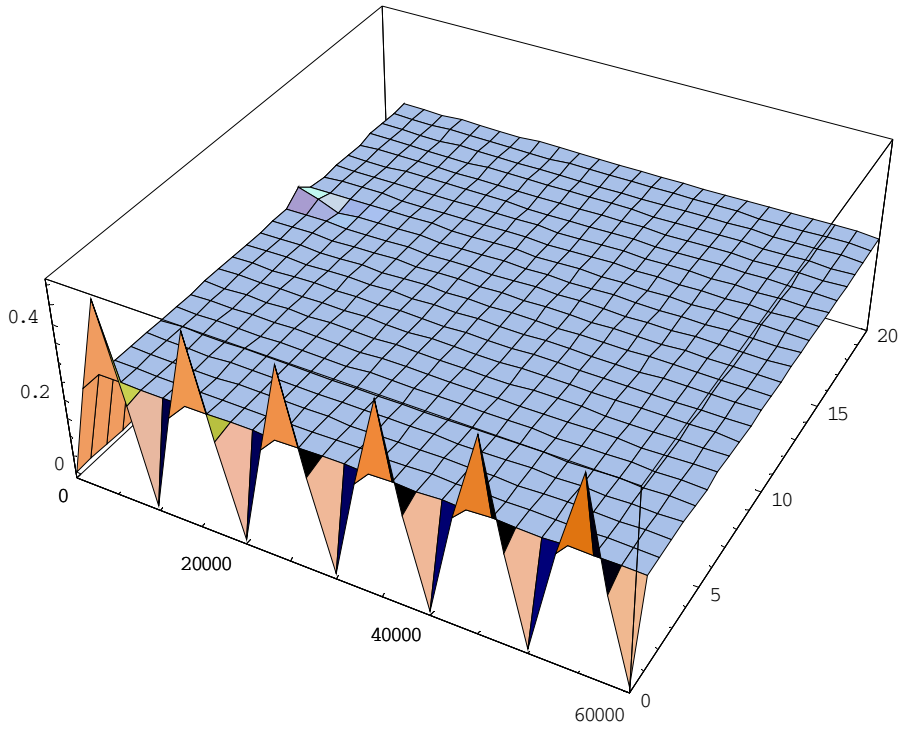
Επιλέγοντας «x δευτέρου είδους» με $\lambda \gg 0$ είναι $x_\lambda = \pi\sqrt{4\lambda^2 + 4\lambda + 3/4} \approx 2\pi\lambda$, η παραπάνω θα γίνει $\cos\left(-m\vartheta + a\right) = \pm 1$, οπότε κατά τα γνωστά έχουμε ότι αυτό συμβαίνει για $m = O\left(\sqrt{N}\right)$ ■

► Γραφικές παραστάσεις της ακτινικής και της γωνιακής αξιοπιστίας

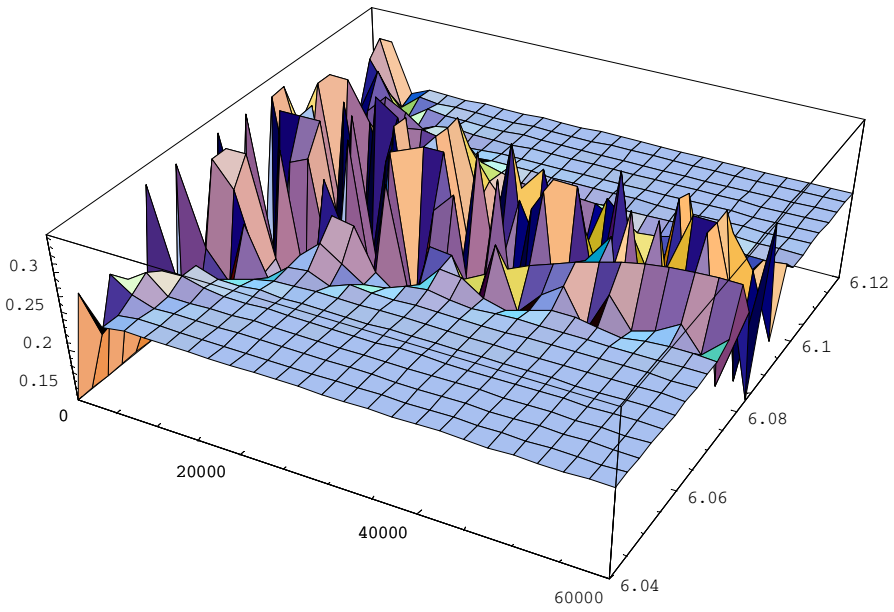
Τα αποτελέσματα της πρότασης 2.3.2. επιβεβαιώνονται αριθμητικά από τις παρακάτω γραφικές παραστάσεις. Ως πρόβλημα αναζήτησης έχουμε θεωρήσει την αναζήτηση ενός στοιχείου μέσα από την μη δομημένη βάση δεδομένων που ορίζει ένας παγκόσμιος τηλεφωνικός κατάλογος με $5 \cdot 10^9$ στοιχεία-αριθμούς τηλεφώνων. Στον άξονα xx' μετράμε τον αριθμό m των επαναλήψεων και έχουμε θεωρήσει ότι είναι $0 \le m \le 60000$ (αφού γενικά μας ενδιαφέρει $m \approx \frac{\pi}{4}\sqrt{N} = O\left(\sqrt{N}\right)$), στον άξονα yy' μετράμε τον θόρυβο θεωρώντας ότι $0 \le y \le 20$, και άξονα zz' μετράμε την αξιοπιστία.
Για την ακτινική αξιοπιστία

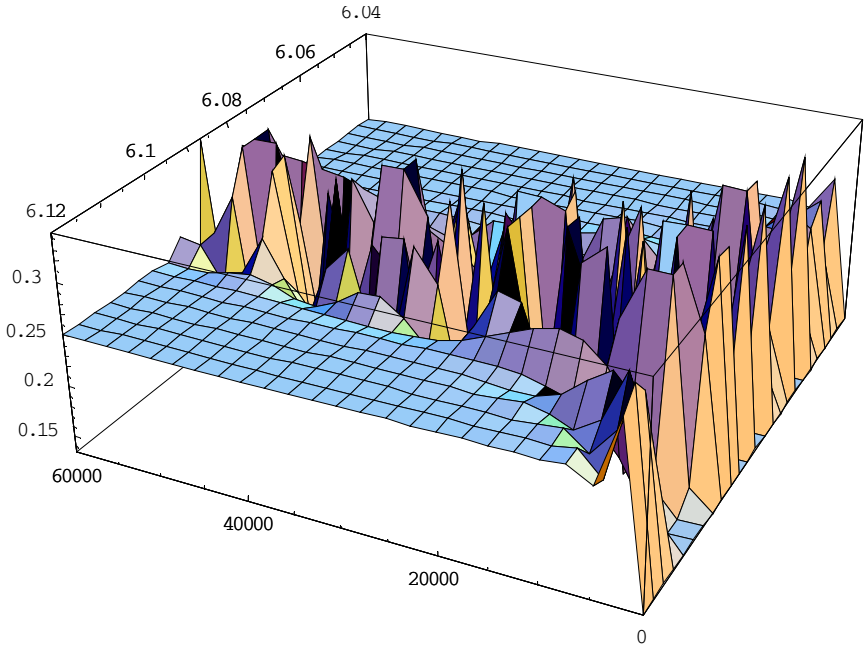
$$f_r = \frac{1 + \cos^m\left(2\psi\left(x\right)\right)\cos T}{4}$$

προκύπτει η πρώτη γραφική παράσταση και επιβεβαιώνεται ότι $\lim_{m \to +\infty} f_r = 0.25 = 1/4$.



Στην περίπτωση των «καλών x πρώτου είδους» η γραφική παράσταση παρουσιάζει ιδιάζουσα συμπεριφορά και, όπως φαίνεται στο παρακάτω σχήμα, προφανώς χάνεται η σύγκλιση $\lim_{m\to+\infty} f_r = 0.25 = 1/4$, πράγμα αναμενόμενο αφού τότε ο τελεστής γίνεται μοναδιακός και ο αλγόριθμος επανέρχεται στην κλασική του μορφή, άρα δεν περιγράφεται από αυτό το μοντέλο.
(γραφική παράσταση της ακτινικής αξιοπιστίας σε περιοχή του πρώτου «καλού x πρώτου είδους» που είναι περίπου 6.08, από δυο οπτικές γωνίες).

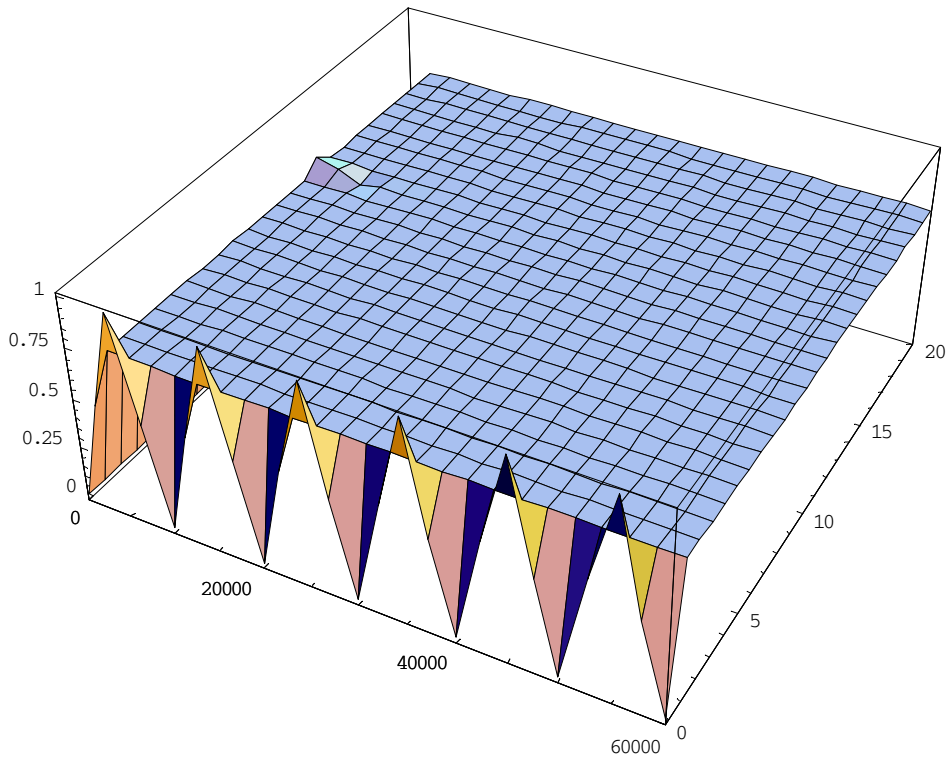


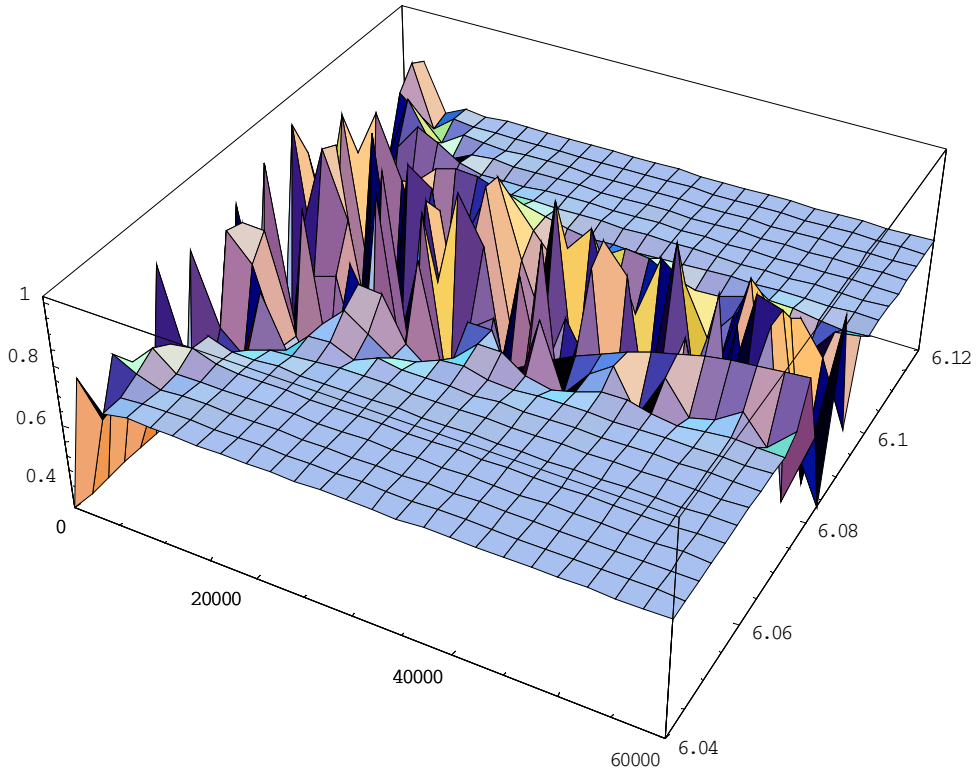


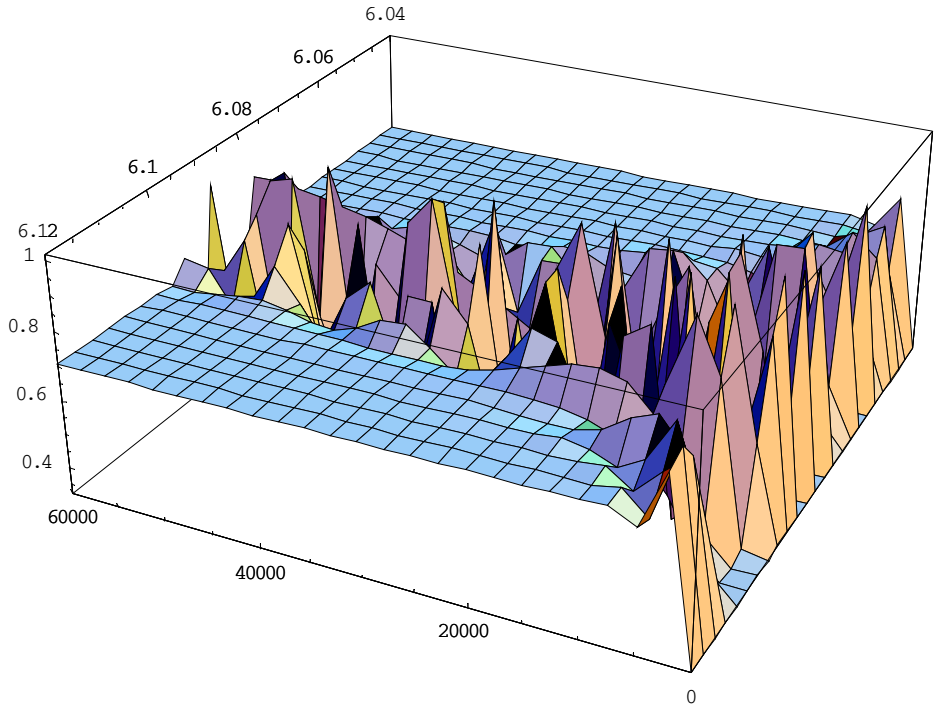
Για την γωνιακή αξιοπιστία

$$f_a \equiv \cos\gamma = \frac{1}{\sqrt{2}} \cdot \frac{1+\cos^m\left(2\psi\left(x\right)\right)\cos T}{\sqrt{1+\cos^{2m}\left(2\psi\left(x\right)\right)}}$$

έχουμε τις ακόλουθες γραφικές παραστάσεις και επιβεβαιώνονται τα αντίστοιχα συμπεράσματα.




1
0.8
0.6
0.4
0
20000
40000
60000
6.04
6.06
6.08
6.1
6.12


6.04
6.06
6.08
6.1
6.12
1
0.8
0.6
0.4
60000
40000
20000
0

► Η περίπτωση του πρώτου και γενικότερου τελεστή αναζήτησης

Συνεχίζουμε την διερεύνηση για την αξιοπιστία του αλγόριθμου Grover υπό την επίδραση Κβαντικού θορύβου θέτοντας τα προηγούμενα ερωτήματα για την ακτινική και τη γωνιακή αξιοπιστία και στην περίπτωση που έχουμε ως τελεστή αναζήτησης τον πρώτο και γενικότερο. Επειδή οι αντίστοιχοι αλγεβρικοί υπολογισμοί (διώνυμο του Newton κλπ) που απαιτούνται για την τυχαία δύναμή του και τον προσδιορισμό των αξιοπιστιών είναι αρκετά πιο περίπλοκοι, επιλέξαμε να προσδιορίσουμε το διάνυσμα που αναπαριστά αυτόν τον τελεστή στη σφαίρα του Bloch υπολογίζοντας απ' ευθείας τις συντεταγμένες του. Για τον σκοπό αυτό θα εισάγουμε μερικούς συμβολισμούς και θα αποδείξουμε δυο Λήμματα.

► Συμβολισμοί

Για κάθε $x > 0$ ορίζουμε τις συναρτήσεις:

$$f(x) = \cos\frac{x}{2}\cos\mu(x) + \frac{x}{2}\sin\frac{x}{2}\delta(x)$$

$$g(x) = \frac{x}{2}\cos\frac{x}{2}\delta(x) - \sin\frac{x}{2}\cos\mu(x)$$

$$h(x) = \frac{\pi}{4}\delta(x)\cos\frac{x}{2}$$

$$\varphi(x) = -\frac{\pi}{4}\delta(x)\sin\frac{x}{2}$$

$$F \equiv F(x,N) = \left(g^2(x) - f^2(x)\right)\frac{N-2}{N} + 4f(x)g(x)\frac{\sqrt{N-1}}{N}$$

$$G \equiv G(x,N) = \left(g^2(x) - f^2(x)\right)\frac{2\sqrt{N-1}}{N} - 2f(x)g(x)\frac{N-2}{N}$$

$$H \equiv H(x,N) = \left(\varphi^2(x) - h^2(x)\right)\frac{N-2}{N} + 4h(x)\varphi(x)\frac{\sqrt{N-1}}{N}$$

$$\Phi \equiv \Phi(x,N) = \left(\varphi^2(x) - h^2(x)\right)\frac{2\sqrt{N-1}}{N} - 2h(x)\varphi(x)\frac{N-2}{N}$$

$$\Sigma_1 = -2FG - 2\mathrm{H}\Phi$$

$$\Sigma_2 = F^2 - G^2 + \mathrm{H}^2 - \Phi^2$$

$$P = F^2 + G^2 + \mathrm{H}^2 + \Phi^2$$

$$S_1 = \frac{\Sigma_1}{P}, S_2 = \frac{\Sigma_2}{P}$$

$$\omega = \arccos\frac{S_2}{\sqrt{S_1^2 + S_2^2}}$$

Στο πρώτο Λήμμα δίνουμε κάποιες ισότητες που θα χρειαστούμε στη συνέχεια και δυο ανισότητες οι οποίες εκτός των άλλων εξασφαλίζουν και ότι οι S_1, S_2, ω είναι καλά ορισμένες.

Λήμμα 2.3.1. : *Για κάθε* $x>0$ *ισχύουν τα παρακάτω:*

(1) $f^2+g^2+h^2+\varphi^2=1$

(2) $H^2+\Phi^2=\left(h^2+\varphi^2\right)^2$

(3) $F^2+G^2+H^2+\Phi^2=\left(f^2+g^2\right)^2+\left(h^2+\varphi^2\right)^2$

$$=1+2\left(h^2+\varphi^2\right)^2-2\left(h^2+\varphi^2\right)\le 1$$

(4) $0<\Sigma_1^2+\Sigma_2^2\le 1$

με την ισότητα στις (3), (4) να ισχύει για $x\in G_1$.

Απόδειξη :

Όλες οι ισότητες αποδεικνύονται αμέσως με αντικατάσταση και απλές πράξεις. Για την ανισότητα στην (3) βλέπουμε ότι

$$1+2\left(h^2+\varphi^2\right)^2-2\left(h^2+\varphi^2\right)=1+2\left(h^2+\varphi^2\right)\left(h^2+\varphi^2-1\right)$$

$$=1-2\left(h^2+\varphi^2\right)\left(f^2+g^2\right)\le 1.$$

Για την (4) εργαζόμαστε ως εξής:

Εάν για κάποιο $x>0$ ήταν $\Sigma_1^2+\Sigma_2^2=0$, τότε θα είχαμε ότι $\Sigma_1=\Sigma_2=0$, άρα

$$\begin{cases} -2FG-2\mathrm{H}\Phi=0 \\ F^2-G^2+\mathrm{H}^2-\Phi^2=0 \end{cases} \quad \text{ή}$$

$$\left(F+iG\right)^2+\left(H+i\Phi\right)^2=0 \quad \text{ή}$$

$$F+iG=\pm\left(H+i\Phi\right)i \quad \text{ή}$$

$$\begin{cases} F=-\Phi \\ G=H \end{cases} \vee \begin{cases} F=\Phi \\ G=-H \end{cases}$$

άρα σε κάθε περίπτωση

$$F^2+G^2+H^2+\Phi^2=2\left(H^2+\Phi^2\right)=2\left(h^2+\varphi^2\right)^2 .$$

Από αυτήν και την (2) είναι

$$h^2+\varphi^2=1/2$$

οπότε μετά την αντικατάσταση και τις πράξεις

$$\delta^2\left(x\right)=8/\pi^2$$

ή ισοδύναμα

$$\sin^2\mu\left(x\right)=\frac{8}{\pi^2}\mu^2\left(x\right) \qquad (5).$$

Θα δείξουμε ότι η (5) δεν είναι δυνατόν να ισχύει για $x>0$

Αν ήταν $x>\pi/2$, τότε

$$\mu^2\left(x\right)=\frac{x^2}{4}+\frac{\pi^2}{16}>\frac{\pi^2}{8}$$

άρα από (5) θα είναι $\sin^2\mu(x)>1$ το οποίο είναι αδύνατο.

Επομένως για $x>\pi/2$ είναι $\Sigma_1^2+\Sigma_2^2>0$.

Αν ήταν $0<x\le\pi/2$, τότε η συνάρτηση

$$l(x)=\sin^2\mu(x)-\frac{8}{\pi^2}\mu^2(x),\quad \text{με } 0<x\le\pi/2,$$

είναι συνεχής στο διάστημα $(0,\pi/2]$ και παραγωγίσιμη στο $(0,\pi/2)$ με παράγωγο

$$\begin{aligned} l'(x)&=\mu'(x)\sin 2\mu(x)-\frac{8}{\pi^2}2\mu(x)\mu'(x)\\ &=\frac{x}{2}\left(\frac{\sin 2\mu(x)}{\mu(x)}-\frac{8}{\pi^2}\right)\quad \text{αφού}\quad 2\mu(x)\mu'(x)=x/2. \end{aligned}$$

Κατασκευαστικά, για κάθε $x\in(0,\pi/2)$ είναι:

$$\frac{\pi}{4}<\mu(x)<\frac{\pi}{2\sqrt{2}}\qquad (6)\qquad \text{και}$$

$$\frac{\sqrt{2}}{\pi}<\frac{1}{2\mu(x)}<\frac{2}{\pi}\qquad (7).$$

Από την (6) προκύπτει ότι η γωνία $2\mu(x)$ ανήκει στο δεύτερο τεταρτημόριο χωρίς να είναι άκρο του, άρα ισχύει

$$0<\sin 2\mu(x)<1\qquad (8).$$

Πολλαπλασιάζοντας τις (7) και (8) παίρνουμε

$$0<\frac{\sin 2\mu(x)}{2\mu(x)}<\frac{2}{\pi}<\frac{8}{\pi^2}.$$

Αυτό σημαίνει ότι για κάθε $x\in(0,\pi/2)$ είναι $l'(x)<0$, και επειδή η συνάρτηση l είναι συνεχής στο διάστημα $(0,\pi/2]$ θα είναι και γνησίως φθίνουσα στο $(0,\pi/2]$. Άρα το σύνολο τιμών της θα είναι

$$l\big((0,\pi/2]\big)=\Big[l(\pi/2),\lim_{x\to0^-}l(x)\Big)=\big[l(\pi/2),0\big)$$

διότι

$$\begin{aligned} \lim_{x\to0^-}l(x)&=\lim_{x\to0^-}\left(\sin^2\mu(x)-\frac{8}{\pi^2}\mu^2(x)\right)\\ &=\sin^2\mu(0)-\frac{8}{\pi^2}\mu^2(0)\\ &=\frac{1}{2}-\frac{8}{\pi^2}\frac{\pi^2}{16}=0. \end{aligned}$$

Επομένως $l(x)<0$ στο διάστημα $(0,\pi/2]$ και τελικά για κάθε $x>0$ είναι $\Sigma_1^2+\Sigma_2^2>0$.

Ακόμα είναι

$$\begin{aligned}\Sigma_1^2+\Sigma_2^2 &= \left(-2FG-2H\Phi\right)^2+\left(F^2-G^2+H^2-\Phi^2\right)^2\\ &= \left(F^2+G^2+H^2+\Phi^2\right)^2-4\left(F\Phi-GH\right)^2\\ &\le \left(F^2+G^2+H^2+\Phi^2\right)^2\le 1 \qquad (8).\end{aligned}$$

και εξαιτίας της (3)

Η ισότητα στην (3) ισχύει αν και μόνο αν είναι

$$h^2+\varphi^2=1 \quad \text{ή} \quad h^2+\varphi^2=0\,.$$

Αν ίσχυε η πρώτη από αυτές, τότε από (1) θα ήταν

$$f^2+g^2=0$$

η οποία μετά από τις πράξεις δίνει την αδύνατη $\cos\mu(x)=\sin\mu(x)=0$. Από την δεύτερη μετά την αντικατάσταση και τις πράξεις παίρνουμε $\delta(x)=0$, ή ισοδύναμα $x\in G_1$. Η ισότητα στην (4) ισχύει αν και μόνο αν ισχύει η ισότητα στην (8) άρα πάλι για $x\in G_1$ ■

Στο επόμενο Λήμμα θα προσδιορίσουμε το διάνυσμα πάνω στη σφαίρα Bloch που προκύπτει μετά από μια δράση του τελεστή αναζήτησης E_R πάνω στο αντίστοιχο διάνυσμα του «στόχου»-πίνακα πυκνότητας $\rho_s=|s\rangle\langle s|$, και θα δώσουμε επίσης μια ισότητα από την οποία προκύπτουν οι συντεταγμένες αυτού του διανύσματος μετά από n δράσεις του E_R.

<u>Λήμμα 2.3.2.</u> : *Έστω ότι ο πίνακας πυκνότητας $\rho_s=|s\rangle\langle s|$ αναπαριστάνεται στη σφαίρα του Bloch από το διάνυσμα $(x_1,x_2,x_3)^{\mathrm{T}}$. Τότε στη σφαίρα αυτή:*

1) *Μετά από n δράσεις του E_R, για τις συντεταγμένες του διανύσματος που αναπαριστά τον $E_R^n(\rho_s)$ ισχύει $x_i^{(n)}=Tr\left\{\left(E_R^n\right)^{\dagger}(\sigma_i)\rho_s\right\}$ για $i=1,2,3$ και κάθε θετικό ακέραιο n.*
2) *Ο πίνακας $E_R(\rho_s)$ αναπαριστάνεται από το διάνυσμα $\left(x_1^{(1)},x_2^{(1)},x_3^{(1)}\right)^{\mathrm{T}}=\left(\Sigma_2x_1+\Sigma_1x_3,Px_2,-\Sigma_1x_1+\Sigma_2x_3\right)^{\mathrm{T}}$.*

<u>Απόδειξη</u> :

Ορίζουμε τους τελεστές $M_k=R_kI_sR_k^{\dagger}I_{x_0}$ (9) για $k=1,2$, και τότε είναι:

$$\begin{aligned}E_R(\rho_s) &= \left(R_0I_sR_0^{\dagger}I_{x_0}\right)\rho_s\left(R_0I_sR_0^{\dagger}I_{x_0}\right)^{\dagger}+\left(R_1I_sR_1^{\dagger}I_{x_0}\right)\rho_s\left(R_1I_sR_1^{\dagger}I_{x_0}\right)^{\dagger}\\ &= M_0\rho_sM_0^{\dagger}+M_1\rho_sM_1^{\dagger}\,.\end{aligned}$$

Από την (9) με αντικατάσταση των ήδη γνωστών 2x2 πινάκων θα πάρουμε
:

$$M_0=\begin{pmatrix}F & G\\ -G & F\end{pmatrix} \text{ και } M_1=\begin{pmatrix}H & \Phi\\ -\Phi & H\end{pmatrix}.$$

Επίσης

$$\left(E_R\right)^{\dagger}\left(\sigma_i\right)=M_0^{\dagger}\sigma_i M_0+M_1^{\dagger}\sigma_i M_1 \text{ με } i=1,2,3\,.$$

Για $i=1,2,3$ πάλι μετά από αντικατάσταση στην προηγούμενη και τις πράξεις προκύπτουν

$$\left(E_R\right)^{\dagger}\left(\sigma_1\right)=\begin{pmatrix}\Sigma_1 & \Sigma_2\\ \Sigma_2 & -\Sigma_1\end{pmatrix},\ \left(E_R\right)^{\dagger}\left(\sigma_2\right)=P\sigma_2 \text{ και } \left(E_R\right)^{\dagger}\left(\sigma_3\right)=\begin{pmatrix}\Sigma_2 & -\Sigma_1\\ -\Sigma_1 & -\Sigma_2\end{pmatrix}.$$

Θα αποδείξουμε επαγωγικά την πρώτη ισότητα του Λήμματος

Γνωρίζουμε ότι ισχύουν $\rho_s=\frac{1}{2}\left(I+\sum_{i=1}^{3}x_i\sigma_i\right)$ και $x_i=Tr\left(\sigma_i\rho_s\right)$ για $i=1,2,3$.

Μετά την πρώτη δράση ($n=1$)του τελεστή αναζήτησης, για $i=1,2,3$, θα είναι

$$\begin{aligned}x_i^{(1)}&=Tr\left(\sigma_i\rho_s^{(1)}\right)\\&=Tr\left(\sigma_i\left(M_0\rho_s M_0^{\dagger}+M_1\rho_s M_1^{\dagger}\right)\right)\\&=Tr\left(\sigma_i M_0\rho_s M_0^{\dagger}\right)+Tr\left(\sigma_i M_1\rho_s M_1^{\dagger}\right)\\&=Tr\left(M_0^{\dagger}\sigma_i M_0\rho_s\right)+Tr\left(M_1^{\dagger}\sigma_i M_1\rho_s\right)\\&=Tr\left(M_0^{\dagger}\sigma_i M_0\rho_s+M_1^{\dagger}\sigma_i M_1\rho_s\right)\\&=Tr\left(\left(M_0^{\dagger}\sigma_i M_0+M_1^{\dagger}\sigma_i M_1\right)\rho_s\right)\\&=Tr\left(\left(E_R\right)^{\dagger}\left(\sigma_i\right)\rho_s\right).\end{aligned}$$

Έστω ότι η ζητούμενη ισχύει για $n=k$, δηλαδή έστω ότι για $i=1,2,3$ είναι

$$x_i^{(k)}=Tr\left\{\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)\rho_s\right\} \qquad (10).$$

Για $n=k+1$ και για $i=1,2,3$ έχουμε:

$$\begin{aligned}x_i^{(k+1)}&=Tr\left(\sigma_i\rho_s^{(k+1)}\right)\\&=Tr\left(\sigma_i\left(\rho_s^{(1)}\right)^{(k)}\right)\\&=Tr\left\{\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)\rho_s^{(1)}\right\}\\&=Tr\left\{\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)\left(M_0\rho_s M_0^{\dagger}+M_1\rho_s M_1^{\dagger}\right)\right\}\\&=Tr\left(\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_0\rho_s M_0^{\dagger}\right)+Tr\left(\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_1\rho_s M_1^{\dagger}\right)\\&=Tr\left(M_0^{\dagger}\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_0\rho_s\right)+Tr\left(M_1^{\dagger}\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_1\rho_s\right)\\&=Tr\left(\left(M_0^{\dagger}\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_0+M_1^{\dagger}\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)M_1\right)\rho_s\right)\\&=Tr\left\{E_R^{\dagger}\left(\left(E_R^k\right)^{\dagger}\left(\sigma_i\right)\right)\rho_s\right\}\\&=Tr\left\{\left(E_R^{k+1}\right)^{\dagger}\left(\sigma_i\right)\rho_s\right\}\end{aligned}$$

και αυτό ακριβώς συμπληρώνει την επαγωγική απόδειξη.
Η δεύτερη ισότητα του Λήμματος προκύπτει άμεσα για $n=1$ από αυτήν που μόλις δείξαμε με αντικατάσταση γνωστών πινάκων και απλές πράξεις.■

Παρατήρηση :

Ο πίνακας πυκνότητας ρ_s είναι ο

$$\rho_s = |s\rangle\langle s| = \begin{bmatrix} \frac{1}{N} & \frac{\sqrt{N-1}}{N} \\ \frac{\sqrt{N-1}}{N} & \frac{N-1}{N} \end{bmatrix}$$

άρα το αντίστοιχο διάνυσμα στη σφαίρα θα έχει συντεταγμένες $x_i = Tr\left(\sigma_i \rho_s\right)$ για $i=1,2,3$

$$x_1 = \frac{2\sqrt{N-1}}{N}\ ,\ x_2 = 0\ ,\ x_3 = \frac{2-N}{N}$$

Έχοντας υπόψη και την παραπάνω παρατήρηση είμαστε πλέον έτοιμοι να δείξουμε την ακόλουθη πρόταση

Πρόταση 2.3.4. :

Μετά από $n \in \mathbb{N}$ *δράσεις του τελεστή* E_R *πάνω στον πίνακα πυκνότητας* $\rho_s = |s\rangle\langle s|$, *το διάνυσμα που αναπαριστά στην σφαίρα Bloch τον* $E_R^n\left(\rho_s\right)$ *έχει συντεταγμένες*

$$\begin{cases} x_1^{(n)} = \left(\sqrt{\Sigma_1^2 + \Sigma_2^2}\right)^n \left[\cos\left(n\omega\right)x_1 + \sin\left(n\omega\right)x_3\right] \\ \\ x_2^{(n)} = Px_2 = 0 \\ x_3^{(n)} = \left(\sqrt{\Sigma_1^2 + \Sigma_2^2}\right)^n \left[-\sin\left(n\omega\right)x_1 + \cos\left(n\omega\right)x_3\right]. \end{cases}$$

Η ακτινική και η γωνιακή αξιοπιστία του αλγόριθμου είναι αντίστοιχα ίσες με

$$f_r = \left(\sqrt{\Sigma_1^2 + \Sigma_2^2}\right)^n \cos\left(n\omega - \vartheta\right) \text{ και } f_a = \cos\left(n\omega - \vartheta\right).$$

Απόδειξη :

Εξ' αιτίας των

$$\left(E_R\right)^{\dagger}\left(\sigma_1\right)=\begin{pmatrix}\Sigma_1 & \Sigma_2\\ \Sigma_2 & -\Sigma_1\end{pmatrix},\ \left(E_R\right)^{\dagger}\left(\sigma_2\right)=P\sigma_2,\ \left(E_R\right)^{\dagger}\left(\sigma_3\right)=\begin{pmatrix}\Sigma_2 & -\Sigma_1\\ -\Sigma_1 & -\Sigma_2\end{pmatrix}$$ και

$$\left(x_1^{(1)},x_2^{(1)},x_3^{(1)}\right)^{\mathrm{T}}=\left(\Sigma_2x_1+\Sigma_1x_3,Px_2,-\Sigma_1x_1+\Sigma_2x_3\right)^{\mathrm{T}}$$ και

$$\omega=\arccos\frac{S_2}{\sqrt{S_1^2+S_2^2}}$$

έπεται αμέσως ότι

$$\begin{bmatrix}x_1^{(1)}\\ x_2^{(1)}\\ x_3^{(1)}\end{bmatrix}=\begin{bmatrix}\Sigma_2 & 0 & \Sigma_1\\ 0 & P & 0\\ -\Sigma_1 & 0 & \Sigma_2\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=P\sqrt{S_1^2+S_2^2}\begin{bmatrix}\cos\omega & 0 & \sin\omega\\ 0 & \dfrac{1}{\sqrt{S_1^2+S_2^2}} & 0\\ -\sin\omega & 0 & \cos\omega\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}.$$

Ύστερα από $n\in\square$ δράσεις του τελεστή αναζήτησης, το αντίστοιχο διάνυσμα στη σφαίρα Bloch θα είναι το

$$\vec{\delta}\equiv\overrightarrow{\delta^{(n)}}\left(\rho_s\right)=\left(x_1^{(n)},x_2^{(n)},x_3^{(n)}\right)$$

για τις συντεταγμένες του οποίου ισχύει

$$\begin{bmatrix}x_1^{(n)}\\ x_2^{(n)}\\ x_3^{(n)}\end{bmatrix}=\left(\sqrt{\Sigma_1^2+\Sigma_2^2}\right)^n\begin{bmatrix}\cos\omega & 0 & \sin\omega\\ 0 & \dfrac{1}{\sqrt{S_1^2+S_2^2}} & 0\\ -\sin\omega & 0 & \cos\omega\end{bmatrix}^n\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}$$ ή

$$\begin{bmatrix}x_1^{(n)}\\ x_2^{(n)}\\ x_3^{(n)}\end{bmatrix}=\left(\sqrt{\Sigma_1^2+\Sigma_2^2}\right)^n\begin{bmatrix}\cos n\omega & 0 & \sin n\omega\\ 0 & \dfrac{1}{\left(\sqrt{S_1^2+S_2^2}\right)^n} & 0\\ -\sin n\omega & 0 & \cos n\omega\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}$$ ή

$$\begin{cases}x_1^{(n)}=\left(\sqrt{\Sigma_1^2+\Sigma_2^2}\right)^n\left[\cos\left(n\omega\right)x_1+\sin\left(n\omega\right)x_3\right]\\ x_2^{(n)}=Px_2=0\\ x_3^{(n)}=\left(\sqrt{\Sigma_1^2+\Sigma_2^2}\right)^n\left[-\sin\left(n\omega\right)x_1+\cos\left(n\omega\right)x_3\right].\end{cases}$$

(υπενθυμίζουμε ότι είναι $S_1 = \frac{\Sigma_1}{P}, S_2 = \frac{\Sigma_2}{P}$, $x_2 = 0$).

Το αντικείμενο της αναζήτησης είναι ο πίνακας πυκνότητας

$$\rho_{x_0} = |x_0\rangle\langle x_0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

ο οποίος κατά τα γνωστά αναπαριστάνεται στη σφαίρα από το διάνυσμα $\overrightarrow{\rho_{x_0}}$ το οποίο έχει συντεταγμένες $x_i = Tr\left(\sigma_i \rho_{x_0}\right)$ για $i = 1,2,3$, άρα $\overrightarrow{\rho_{x_0}} = (0,0,1)$. Επομένως για την ακτινική και την γωνιακή αξιοπιστία θα έχουμε:

$$f_r = \left\langle \overrightarrow{\rho_{x_0}}, \vec{\delta} \right\rangle = \left(\sqrt{\Sigma_1^2 + \Sigma_2^2}\right)^n \cos(n\omega - \vartheta) \text{ και } f_a = \cos(n\omega - \vartheta).$$

Επειδή για $0 < x \notin G$ είναι $0 < \Sigma_1^2 + \Sigma_2^2 < 1$, θα ισχύει ότι $\lim_{n \to +\infty} \left\langle \overrightarrow{\rho_{x_0}}, \vec{\delta} \right\rangle = 0$, πράγμα το οποίο σημαίνει ότι στην περίπτωση αυτή ο αλγόριθμος καταρρέει εκθετικά.

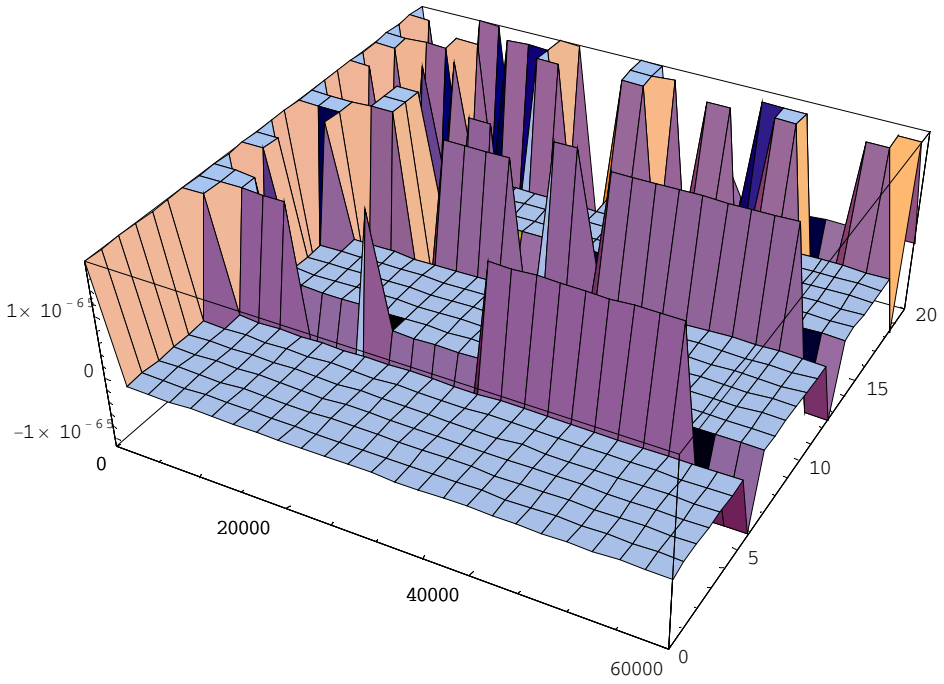
Όταν είναι $x \in G_1$, από την Πρόταση 2.2.1. έπεται αμέσως ότι ο R_0 είναι μοναδιακός και $R_1 = 0$. Τότε ο τελεστής αναζήτησης E_R είναι η adjoint δράση ενός μοναδιακού τελεστή και ο αλγόριθμος ανάγεται στην κλασική του μορφή ως προς την αποτελεσματικότητα και την ταχύτητα αναζήτησης . Επίσης όταν είναι $x \in G_2$, τότε ο τελεστής αναζήτησης E_R γίνεται E_W και ισχύουν τα αποτελέσματα της Πρότασης 2.3.2.■

► **Γραφικές παραστάσεις της ακτινικής και της γωνιακής αξιοπιστίας**

Χρησιμοποιώντας τα ίδια δεδομένα με αυτά που χρησιμοποιήσαμε και στην περίπτωση του δεύτερου τελεστή αναζήτησης κατασκευάζουμε την γραφική παράσταση της

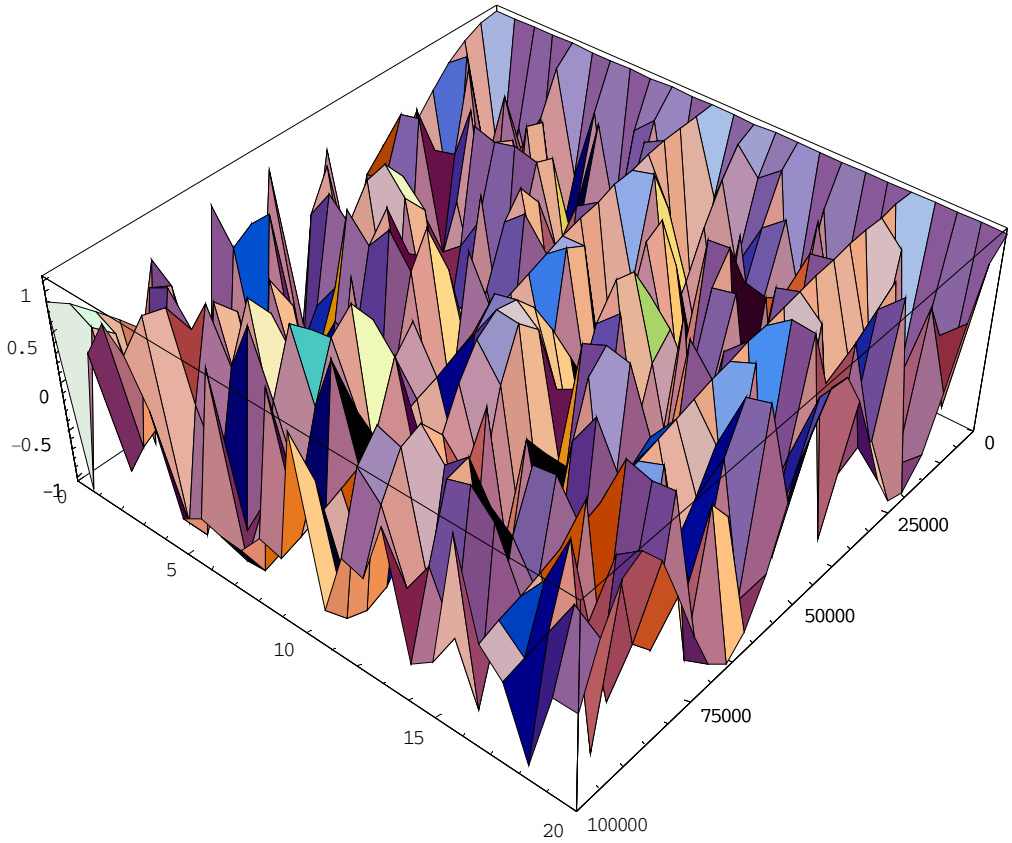
$$f_r = \left(\sqrt{\Sigma_1^2 + \Sigma_2^2}\right)^n \cos\left(n\omega - \vartheta\right).$$

Η κατάρρευση του αλγόριθμου είναι φανερή και γίνεται αρκετά νωρίς (σε μικρό αριθμό δοκιμών).



Ακολουθεί η γραφική παράσταση της γωνιακής αξιοπιστίας (έως 100.000 δοκιμές).

$$f_a = \cos\left(n\omega - \vartheta\right)$$



Κεφάλαιο 3

Εντροπία von Neumann στην αναζήτηση υπό Κβαντικό θόρυβο

Στα επόμενα εξετάζουμε την μεταβολή της κβαντικής εντροπίας von Neumann για τις τρεις περιπτώσεις των τελεστών αναζήτησης.

3.1. Εντροπία Von Neumann για τον τελεστή αναζήτησης E_V

Πρόταση 3.1. :

Η απεικόνιση

$$\rho \to E_V^m(\rho) \equiv \rho^{(m)},\ m \in N,$$

που ορίζεται ως

$$E_V = \frac{1}{2}\left(AdV_0 I_s V_0^\dagger I_{x_0} + AdV_1 I_s V_1^\dagger I_{x_0} \right)$$

και είναι ο τελεστής αναζήτησης που κατασκευάστηκε από το CPTP με γεννήτορες $Y_0 = \frac{1}{\sqrt{2}} V_0$, $Y_1 = \frac{1}{\sqrt{2}} V_1$, *ώστε οι* V_0, V_1 *να είναι οι μοναδιακοί τελεστές*

$$V_0 = \left(R_0 R_0^\dagger\right)^{-1/2} \cdot R_0 = e^{i(\psi(x)-\frac{x}{2})\sigma_y} \qquad \text{και}$$

$$V_1 = \left(R_1 R_1^\dagger\right)^{-1/2} \cdot R_1 = e^{-\frac{ix}{2}\sigma_y},$$

έχει τις ιδιότητες:

I) *Το διάνυσμα* $\lambda_m \equiv \lambda(\rho^{(m)})$ *των ιδιοτιμών του* $\rho^{(m)}$ *κατισχύεται* ([**14**], [**20**]), *από το διάνυσμα* λ *των ιδιοτιμών του* ρ *για κάθε* $x \notin G \setminus G_1$.

II) *Τα διανύσματα* λ_m *και* λ_{m+1} *συνδέονται μέσω του διπλοστοχαστικού πίνακα* $\Delta(x) = \begin{pmatrix} \delta(x) & 1-\delta(x) \\ 1-\delta(x) & \delta(x) \end{pmatrix}$, *με* $\delta(x) = \left(1 + \left|\cos\left(2\psi(x)\right)\right|\right)/2$, *από την ισότητα* $\lambda_{m+1} = \Delta(x) \cdot \lambda_m$, *και επίσης ισχύει* $\lambda_m = \left(\Delta(x)\right)^m \cdot \lambda$, *με* $\lambda \equiv \lambda_0 = (1,0)^{\mathrm{T}}$.

III) *Αυξάνει την Κβαντική εντροπία του αλγόριθμου όταν* $x \notin G_2$.

Απόδειξη:

Έστω $m \in \mathbb{N}$, $x \notin G$ και $\rho_s = |s\rangle\langle s|$. Στην πρόταση 2.3.1. έχουμε δείξει ότι για την απεικόνιση E_V και για κάθε θετικό ακέραιο m ισχύει:

$$E_V^m(\rho_s) = \frac{1}{2}\begin{bmatrix} 1+\cos^m\left(2\psi(x)\right)\cos T & \cos^m\left(2\psi(x)\right)\sin T \\ \cos^m\left(2\psi(x)\right)\sin T & 1-\cos^m\left(2\psi(x)\right)\cos T \end{bmatrix}.$$

Από την χαρακτηριστική εξίσωση αυτού του πίνακα έχουμε

$$\det\left(E_V^m(\rho_s) - \lambda I\right) = 0$$
$$\lambda^2 - Tr\left(E_V^m(\rho_s)\right)\cdot\lambda + \det\left(E_V^m(\rho_s)\right) = 0$$
$$\lambda^2 - \lambda + \frac{1}{4}\left(1-\cos^{2m}2\psi(x)\right) = 0,$$

άρα οι ιδιοτιμές του θα είναι οι αριθμοί

$$\left(1 \pm \left|\cos^m\left(2\psi(x)\right)\right|\right)\Big/2$$

και το διάνυσμα των ιδιοτιμών με φθίνουσα σειρά συντεταγμένων θα είναι το

$$\lambda_m = \begin{bmatrix} \dfrac{1+\left|\cos^m\left(2\psi(x)\right)\right|}{2} \\ \dfrac{1-\left|\cos^m\left(2\psi(x)\right)\right|}{2} \end{bmatrix}.$$

Επειδή $$\left|\cos^m\left(2\psi(x)\right)\right| \le 1$$

παρατηρούμε ότι θα ισχύουν οι

$$\frac{1+\left|\cos^m\left(2\psi(x)\right)\right|}{2} \ge \frac{1+\left|\cos^{m+1}\left(2\psi(x)\right)\right|}{2}$$
$$\frac{1+\left|\cos^m\left(2\psi(x)\right)\right|}{2} + \frac{1-\left|\cos^m\left(2\psi(x)\right)\right|}{2} = \frac{1+\left|\cos^{m+1}\left(2\psi(x)\right)\right|}{2} + \frac{1-\left|\cos^{m+1}\left(2\psi(x)\right)\right|}{2} = 1$$

Αυτό σημαίνει αμέσως ότι για κάθε $m \in \mathbb{N}$ είναι $\lambda_{m+1} \prec \lambda_m$ και λόγω της μεταβατικής ιδιότητας θα είναι $\lambda_m \prec \lambda \equiv \lambda_0 = (1,0)^{\mathrm{T}}$.

Ακόμα έχουμε

$$\Delta(x)\cdot\lambda_m = \begin{pmatrix} \delta(x) & 1-\delta(x) \\ 1-\delta(x) & \delta(x) \end{pmatrix}\cdot\lambda_m$$

$$= \begin{pmatrix} \left(1+\left|\cos\left(2\psi(x)\right)\right|\right)/2 & 1-\left(1+\left|\cos\left(2\psi(x)\right)\right|\right)/2 \\ 1-\left(1+\left|\cos\left(2\psi(x)\right)\right|\right)/2 & \left(1+\left|\cos\left(2\psi(x)\right)\right|\right)/2 \end{pmatrix} \cdot \begin{bmatrix} \dfrac{1+\left|\cos^{m}\left(2\psi(x)\right)\right|}{2} \\ \dfrac{1-\left|\cos^{m}\left(2\psi(x)\right)\right|}{2} \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{1+\left|\cos^{m+1}\left(2\psi(x)\right)\right|}{2} \\ \dfrac{1-\left|\cos^{m+1}\left(2\psi(x)\right)\right|}{2} \end{bmatrix}$$

$$= \lambda_{m+1}.$$

Θέτοντας διαδοχικά στην $\lambda_{m+1} = \Delta(x)\cdot\lambda_m$, όπου m τις τιμές $0,1,\ldots m-1$, και πολλαπλασιάζοντας κατά μέλη τις προκύπτουσες ισότητες, θα πάρουμε $\lambda_m = \left(\Delta(x)\right)^m \cdot \lambda$. Είναι γνωστό ότι για κάθε πίνακα πυκνότητας k, η κατά von Neumann Κβαντική εντροπία $S(k) = -Tr(k\log k)$ είναι συνάρτηση κοίλη κατά Schur. Έχουμε δείξει ότι $\lambda_{m+1} \prec \lambda_m$, άρα θα έχουμε αμέσως ότι για κάθε $m \in$ □ είναι

$$S\left(\rho_s^{(m+1)}\right) > S\left(\rho_s^{(m)}\right).$$

Έστω τώρα ότι $x \in G$. Τότε $x = \pi\sqrt{\kappa^2 - 1/4}$, άρα $\sqrt{\dfrac{x^2}{4}+\dfrac{\pi^2}{16}} = \kappa\pi/2$, και αυτό σημαίνει ότι $\mu(x) = \kappa\pi$ ή $\mu(x) = \kappa\pi + \pi/2$, ισοδύναμα $\sin\mu(x) = 0$ ή $\cos\mu(x) = 0$, δηλαδή $x \in G_1$ ή $x \in G_2$. Αν $x \in G_1$ ο αλγόριθμος επανέρχεται στην κλασική του μορφή, ενώ αν $x \in G_2$, τότε όπως έχουμε δείξει στο προηγούμενο Κεφάλαιο είναι

$$\rho^{(m)} \equiv E_V^m\left(\rho_s\right) = \frac{1}{2}\begin{bmatrix} 1+(-1)^m\cos T & (-1)^m\sin T \\ (-1)^m\sin T & 1-(-1)^m\cos T \end{bmatrix}.$$

και ο τελεστής $E_V^m\left(\rho_s\right)$ είναι προβολικός, άρα και στις δυο αυτές περιπτώσεις θα είναι $S\left(\rho^{(m)}\right) = 0$.

► **Αναλυτικός υπολογισμός του** $\left(\Delta(x)\right)^m$

Είδαμε ότι είναι $\Delta(x) = \begin{pmatrix} \delta(x) & 1-\delta(x) \\ 1-\delta(x) & \delta(x) \end{pmatrix}$, με $\delta(x) = \left(1+\left|\cos\left(2\psi(x)\right)\right|\right)/2$. Η διαγωνοποίηση του $\Delta(x)$ δίνει

$$\Delta(x) = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \left|\cos\left(2\psi(x)\right)\right| \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix},$$

άρα για κάθε θετικό ακέραιο m θα είναι

$$\left(\Delta(x)\right)^m = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \left|\cos\left(2\psi(x)\right)\right|^m \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \quad \text{ή}$$

$$= \frac{1}{2} \begin{pmatrix} 1+\left|\cos\left(2\psi(x)\right)\right|^m & 1-\left|\cos\left(2\psi(x)\right)\right|^m \\ 1-\left|\cos\left(2\psi(x)\right)\right|^m & 1+\left|\cos\left(2\psi(x)\right)\right|^m \end{pmatrix}.$$

► Φράγματα για την Κβαντική εντροπία

Δείξαμε ότι η Κβαντική εντροπία του αλγόριθμου αυξάνει όταν $x \notin G$. Είναι όμως ενδιαφέρον να δούμε αν είναι δυνατόν αφ' ενός να γίνει κάποια εκτίμηση για το πόσο αυξάνει από βήμα σε βήμα, και αφ' ετέρου να γίνει μια αντίστοιχη εκτίμηση για την αύξηση της εντροπίας από την εκκίνηση του αλγόριθμου έως κάποιο τυχαίο βήμα του. Για το σκοπό αυτό θα χρησιμοποιήσουμε την ανισότητα του Fannes [**4**] και θα δείξουμε ότι η ισχύει η παρακάτω πρόταση από την οποία προκύπτουν κάποια φράγματα για την εντροπία.

<u>Πρόταση 3.2.</u> :

Για κάθε θετικό ακέραιο m και $x \geq 0$ ισχύουν:

$$\text{i)} \ \left|S\left(\rho^{(m+1)}\right) - S\left(\rho^{(m)}\right)\right| \leq \mathrm{A}(x,m)$$

$$\mu\varepsilon \ \mathrm{A}(x,m) = \sqrt{2}\sin^2\left(\psi(x)\right)\left|\cos^m\left(2\psi(x)\right)\right| + \frac{1}{e\ln 2}$$

και

$$\text{ii)} \ \left|S\left(\rho^{(m)}\right)\right| \leq \mathrm{B}(x,m), \ \mu\varepsilon \ \mathrm{B}(x,m) =$$

$$\frac{1}{\sqrt{2}}\sqrt{1+\cos^m\left(2\psi(x)\right)\left(2\left(1-2/N\right)\cos T + \cos^m\left(2\psi(x)\right) - 4\left(\sqrt{N-1}/N\right)\sin T\right)} + \frac{1}{e\ln 2}$$

$$\text{iii)} \ \left|S\left(\rho^{(m+1)}\right) - S\left(\rho^{(m)}\right)\right| \leq \sqrt{2} + \frac{1}{e\ln 2},$$

$$\left|S\left(\rho^{(m)}\right)\right| \leq \sqrt{\frac{3}{2}} + \frac{1}{e\ln 2} < \sqrt{2} + \frac{1}{e\ln 2}.$$

<u>Απόδειξη</u>:

i) Έστω ρ, σ δυο (πεπερασμένης διάστασης) πίνακες πυκνότητας και έστω $D \equiv D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\| = \frac{1}{2}\sqrt{Tr\left[(\rho-\sigma)(\rho-\sigma)^\dagger\right]}$ η μετρική που επάγεται από την norm του ίχνους πίνακα. Ο Fannes έδειξε ότι αν έχουμε $0 \leq D \leq 1/(2e)$, τότε θα ισχύει

$\left|S(\rho)-S(\sigma)\right| \leq 2D\log(d) - 2D\log(2D)$, (1) με d να είναι η διάσταση του πίνακα πυκνότητας, στην συγκεκριμένη περίπτωση είναι $d=2$. Για μεγαλύτερες τιμές του D η (1) ισχύει σε μια ασθενέστερη εκδοχή $\left|S(\rho)-S(\sigma)\right| \leq 2D\log(d) + 1/(e\ln 2)$ (2). Στην περίπτωση

που εξετάζουμε θα είναι:

$D_m \equiv D\left(\rho^{(m+1)}, \rho^{(m)}\right) = \frac{1}{2}\sqrt{Tr\left[\left(\rho^{(m+1)} - \rho^{(m)}\right)^2\right]}$. Επειδή είναι

$$\rho^{(m)} = \frac{1}{2}\begin{bmatrix} 1+\cos^m\left(2\psi(x)\right)\cos T & \cos^m\left(2\psi(x)\right)\sin T \\ \cos^m\left(2\psi(x)\right)\sin T & 1-\cos^m\left(2\psi(x)\right)\cos T \end{bmatrix},$$

αντικαθιστώντας θα πάρουμε ότι :

$D_m = \frac{\sqrt{2}}{2}\sin^2\left(\psi(x)\right)\left|\cos^m\left(2\psi(x)\right)\right|$. Είναι φανερό ότι ισχύει

$0 \le D_m \le \sqrt{2}/2$, και είναι δυνατόν να ισχύει η ισότητα $D_m = \sqrt{2}/2$ όταν $\sin\left(\psi(x)\right) = \pm 1$. Επομένως θα ισχύει η ασθενέστερη εκδοχή της ανισότητας Fannes, δηλαδή η (2), άρα

$\left|S\left(\rho^{(m+1)}\right) - S\left(\rho^{(m)}\right)\right| \le 2D_m \log(2) + 1/(e\ln 2) = 2D_m + 1/(e\ln 2)$, ή

$\left|S\left(\rho^{(m+1)}\right) - S\left(\rho^{(m)}\right)\right| \le \sqrt{2}\sin^2\left(\psi(x)\right)\left|\cos^m\left(2\psi(x)\right)\right| + \frac{1}{e\ln 2}$ η οποία είναι η ζητούμενη.

ii) Έστω τώρα $D'_m \equiv D\left(\rho^{(m)}, \rho_s\right) = \frac{1}{2}\sqrt{Tr\left[\left(\rho^{(m)} - \rho_s\right)^2\right]}$.

Αντικαθιστώντας τα $\rho^{(m)}, \rho_s$, στην παραπάνω θα πάρουμε ότι

$$D'_m = \frac{1}{2\sqrt{2}}\sqrt{1+\cos^m\left(2\psi(x)\right)\left(2\left(1-2/N\right)\cos T + \cos^m\left(2\psi(x)\right) - 4\left(\sqrt{N-1}/N\right)\sin T\right)}$$

Παρατηρούμε ότι αν $x \in G$ είναι $\cos^2\left(\psi(x)\right) = 1$, άρα

$\cos\left(2\psi(x)\right) = 1$, οπότε

$0 \le D'_m \le \frac{1}{2}\sqrt{1+\left(1-2/N\right)\cos T - 2\left(\sqrt{N-1}/N\right)\sin T}$. Επίσης είναι

$\left(1-2/N\right)^2 + \left[-2\left(\sqrt{N-1}/N\right)\right]^2 = 4$, άρα θα είναι

$\left(1-2/N\right)\cos T - 2\left(\sqrt{N-1}/N\right)\sin T = 2\sin\left(T+\xi\right)$, με ξ να είναι η γωνία για την οποία $\sin\xi = \left(N-2\right)/N, \cos\xi = -\sqrt{N-1}/N$. Αυτό σημαίνει ότι $0 \le D'_m \le \frac{1}{2}\sqrt{1+2\sin\left(T+\xi\right)}$ και επομένως η μέγιστη τιμή του D'_m είναι $\max D'_m = \frac{1}{2}\sqrt{\frac{3}{2}}$, άρα πρέπει πάλι να εφαρμοστεί η (2).

Επειδή $\left|S\left(\rho^{(m)}\right)\right| = \left|S\left(\rho^{(m)}\right) - S\left(\rho\right)\right|$, εφαρμόζοντας την (2) προκύπτει η ζητούμενη.

iii) Προφανώς είναι $\mathrm{A}\left(x,m\right) \le \sqrt{2} + 1/(e\ln 2)$ για κάθε $x \ge 0$, και $m > 0$ ακέραιο. Ακόμα είναι $0 \le D'_m \le \frac{1}{2}\sqrt{\frac{3}{2}} < \frac{\sqrt{2}}{2}$.

Από αυτά και τις προηγούμενες ανισότητες στα i)- ii) προκύπτουν αμέσως οι αποδεικτέες ■

Ακολουθούν αντίστοιχα αποτελέσματα για την κβαντική εντροπία στην περίπτωση κατά την οποία ο τελεστής αναζήτησης είναι ο E_R. Είναι φανερό ότι αυτά θα ισχύουν και για τον E_W αφού αυτός είναι ειδική περίπτωση του E_R.

3.2. Εντροπία Von Neumann για τους τελεστές αναζήτησης E_R, E_W

<u>Λήμμα 3.1.</u> :

Αν ο πίνακας $E_R^m(\rho) \equiv \rho^{(m)}$ αναπαριστάνεται στη σφαίρα του Bloch από το διάνυσμα

$$\overrightarrow{x^{(m)}} = \left(x_1^{(m)}, x_2^{(m)}, x_3^{(m)} \right)^{\mathrm{T}},$$

τότε τα ιδιοδιανύσματά του είναι τα

$$\left|\psi_1^{(m)}\right\rangle = \left(1, -\left(\frac{x_3^{(m)} - \left(\Sigma_1^2 + \Sigma_2^2\right)^{\frac{m}{2}}}{x_1^{(m)}} \right) \right)^{\mathrm{T}}, \quad \left|\psi_2^{(m)}\right\rangle = \left(1, -\left(\frac{x_3^{(m)} + \left(\Sigma_1^2 + \Sigma_2^2\right)^{\frac{m}{2}}}{x_1^{(m)}} \right) \right)^{\mathrm{T}}.$$

<u>Απόδειξη</u>:

Αν $\vec{\sigma} = \left(\sigma_1, \sigma_2, \sigma_3\right)^{\mathrm{T}}$ και $\overrightarrow{x^{(m)}} = \left(x_1^{(m)}, x_2^{(m)}, x_3^{(m)} \right)^{\mathrm{T}}$, τότε είναι

$$\begin{aligned} \rho^{(m)} &= \frac{1}{2}\left(I + \overrightarrow{x^{(m)}} \cdot \vec{\sigma} \right) \\ &= \frac{1}{2}\begin{bmatrix} 1 + x_3^{(m)} & x_1^{(m)} - i x_2^{(m)} \\ x_1^{(m)} + i x_2^{(m)} & 1 - x_3^{(m)} \end{bmatrix}. \end{aligned}$$

Η χαρακτηριστική εξίσωση του $\rho^{(m)}$ θα είναι

$$\lambda^2 - Tr\left(\rho^{(m)}\right) \cdot \lambda + \det\left(\rho^{(m)}\right) = 0 \qquad \text{ή}$$

$$\lambda^2 - \lambda + \left[1 - \left(\left(x_1^{(m)}\right)^2 + \left(x_2^{(m)}\right)^2 + \left(x_3^{(m)}\right)^2 \right) \right] \Big/ 4 = 0$$

και εξαιτίας της Πρότασης 2.3.2. θα ισχύει

$$\begin{aligned} \left(x_1^{(m)}\right)^2 + \left(x_2^{(m)}\right)^2 + \left(x_3^{(m)}\right)^2 &= \left(x_1^{(m)}\right)^2 + \left(x_3^{(m)}\right)^2 \\ &= \left(\Sigma_1^2 + \Sigma_2^2\right)^m \end{aligned}$$

άρα

$$\lambda^2 - \lambda + \left[1 - \left(\Sigma_1^2 + \Sigma_2^2\right)^m \right] \Big/ 4 = 0 .$$

Αυτό σημαίνει ότι οι ιδιοτιμές του $\rho^{(m)}$ είναι

$$\lambda_{1,2} = \frac{1 \pm \left(\Sigma_1^2 + \Sigma_2^2\right)^{m/2}}{2}.$$

Λύνοντας τα ομογενή 2x2 γραμμικά συστήματα

$$\frac{1}{2}\begin{bmatrix} 1+x_3^{(m)} & x_1^{(m)} - ix_2^{(m)} \\ x_1^{(m)} + ix_2^{(m)} & 1-x_3^{(m)} \end{bmatrix} \cdot \begin{bmatrix} \xi \\ \eta \end{bmatrix} = \lambda_{1,2} \begin{bmatrix} \xi \\ \eta \end{bmatrix}$$

και χρησιμοποιώντας την $x_2^{(m)} = x_2 = 0$, παίρνουμε αμέσως τα ζητούμενα ιδιοδιανύσματα ■

Παρατήρηση:

Αν $d_j^{(m)} = \left\| \psi_j^{(m)} \right\|,\ j = 1,2$, τότε τα κανονικοποιημένα ιδιοδιανύσματα του $\rho^{(m)}$ είναι τα

$$\left|\phi_1^{(m)}\right\rangle = \left(\frac{1}{d_1^{(m)}}, -\left(\frac{x_3^{(m)} - \left(\Sigma_1^2 + \Sigma_2^2\right)^{\frac{m}{2}}}{d_1^{(m)} x_1^{(m)}} \right) \right)^{\mathrm{T}} \equiv (\lambda_0^{(m,1)}, \lambda_1^{(m,1)})^{\mathrm{T}}$$

$$\left|\phi_2^{(m)}\right\rangle = \left(\frac{1}{d_2^{(m)}}, -\left(\frac{x_3^{(m)} + \left(\Sigma_1^2 + \Sigma_2^2\right)^{\frac{m}{2}}}{d_2^{(m)} x_1^{(m)}} \right) \right)^{\mathrm{T}} \equiv (\lambda_0^{(m,2)}, \lambda_1^{(m,2)})^{\mathrm{T}}.$$

Επίσης

$$\left\langle \phi_2^{(m)} \middle| \phi_1^{(m)} \right\rangle = \frac{1}{d_1^{(m)} d_2^{(m)}} + \frac{\left(x_3^{(m)}\right)^2 - \left(\Sigma_1^2 + \Sigma_2^2\right)^m}{d_1^{(m)} d_2^{(m)} \left(x_1^{(m)}\right)^2}$$

$$= \frac{\left(x_1^{(m)}\right)^2 + \left(x_3^{(m)}\right)^2 - \left(\Sigma_1^2 + \Sigma_2^2\right)^m}{d_1^{(m)} d_2^{(m)} \left(x_1^{(m)}\right)^2}$$

$$= 0$$

Αυτό σημαίνει ότι το σύνολο $\left\{ \left| \varphi_r^{(m)} \right\rangle \right\}_{r=1,2}$ είναι ορθοκανονικό.

Πρόταση 3.3. :

Η απεικόνιση

$$\rho \to \rho' = E_R^m(\rho) \equiv \rho^{(m)},\ m \in N,$$

που ορίζεται ως

$$E_R = AdR_0 I_s R_0^{\dagger} I_{x_0} + AdR_1 I_s R_1^{\dagger} I_{x_0}$$

και είναι ο τελεστής αναζήτησης που κατασκευάστηκε από το CPTP με γεννήτορες R_0, R_1, *έχει τις ιδιότητες:*

I) Το διάνυσμα $\lambda_m \equiv \lambda(\rho^{(m)}) \equiv \lambda_{\rho'}$ *των ιδιοτιμών του* $\rho^{(m)}$ *κατισχύεται από το διάνυσμα* λ_ρ *των ιδιοτιμών του* ρ *για κάθε* $x \geq 0$, *και ισχύει* $\lambda_{m+1} \prec \lambda_m$.

II) Τα διανύσματα λ_m *και* λ_{m+1} *συνδέονται μέσω ενός* 2x2 *διπλοστοχαστικού πίνακα* $\Delta^{(m)}(x)$, *από την ισότητα* $\lambda_{m+1} = \Delta^{(m)}(x) \cdot \lambda_m$, *με στοιχεία*

$$\Delta^{(m)}_{r'r} = (f(x)B + g(x)C)^2 + (h(x)B + \varphi(x)C)^2 \qquad \text{όπου}$$

$$B = \lambda_0^{(m,r)}\lambda_0^{(m+1,r')} + \lambda_1^{(m,r)}\lambda_1^{(m+1,r')},\ C = \lambda_1^{(m,r)}\lambda_0^{(m+1,r')} - \lambda_0^{(m,r)}\lambda_1^{(m+1,r')},\ r, r' \in \{1,2\}.$$

III) Αυξάνει την Κβαντική εντροπία του αλγόριθμου όταν $x \notin G_1$.

Απόδειξη:

Για την απόδειξη της παραπάνω πρότασης θα χρησιμοποιήσουμε ένα θεώρημα του Chefles [**7**] σύμφωνα με το οποίο:

Αν ρ_1 *και* ρ_2 *είναι δυο πίνακες πυκνότητας οι οποίοι συνδέονται μέσω μιας πλήρους θετικής ιχνοδιατηρητικής απεικόνισης*

$$\rho_1 \to \rho_2 = \sum_k A_k \rho_1 A_k^\dagger$$

με γεννήτορες (τελεστές Kraus) A_k, *τότε:*

i) αν $\lambda(\rho_1)$, $\lambda(\rho_2)$ *είναι τα ιδιοδιανύσματα των* ρ_1 *και* ρ_2, *θα ισχύει* $\lambda(\rho_2) \prec \lambda(\rho_1)$ *αν και μόνο αν* $\sum_k A_k A_k^\dagger = I$.

ii) Ο διπλοστοχαστικός πίνακας S *για τον οποίο είναι* $\lambda(\rho_2) = S\lambda(\rho_1)$, *έχει στοιχεία*

$$S_{r'r} = \sum_k \left| \left\langle \varphi_{r'}^{(2)} \middle| A_k \middle| \varphi_r^{(1)} \right\rangle \right|^2 ,$$

όπου $\left\{ \left| \varphi_r^{(1)} \right\rangle \right\}$ *και* $\left\{ \left| \varphi_{r'}^{(2)} \right\rangle \right\}$ *είναι ορθοκανονικά σύνολα ιδιοδιανυσμάτων των* ρ_1 *και* ρ_2 *αντίστοιχα.*

Παρατηρούμε ότι από την Πρόταση 2.2.1. έπονται αμέσως οι $R_0 R_0^\dagger = R_0^\dagger R_0$, $R_1 R_1^\dagger = R_1^\dagger R_1$, (δηλαδή τα R_i είναι κανονικοί τελεστές) και εξ' αιτίας της συνθήκης Kraus θα είναι

$$\sum_{i=0,1} R_i R_i^\dagger = \sum_{i=0,1} R_i^\dagger R_i = I .$$

Σύμφωνα με το θεώρημα του Chefles, παίρνουμε αμέσως ότι $\lambda_{m+1} \prec \lambda_m$.

Στην προηγούμενη παρατήρηση είδαμε ότι το σύνολο $\left\{ \left| \varphi_r^{(m)} \right\rangle \right\}_{r=1,2}$ είναι ορθοκανονικό, οπότε από το ίδιο θεώρημα προκύπτει ότι ο διπλοστοχαστικός πίνακας $\Delta^{(m)}(x)$ που συνδέει τα λ_m και λ_{m+1} υπό την ισότητα $\lambda_{m+1} = \Delta^{(m)}(x) \cdot \lambda_m$ θα έχει στοιχεία:

$$\Delta^{(m)}_{r'r} = \sum_{\kappa=0,1} \left| \left\langle \phi_{r'}^{(m+1)} \middle| R_\kappa \middle| \phi_r^{(m)} \right\rangle \right|^2 ,\ \text{με}\ r, r' \in \{1,2\}$$

$$= \sum_{\kappa=0,1} \left| Tr\left(\left| \phi_r^{(m)} \right\rangle \left\langle \phi_{r'}^{(m+1)} \right| R_\kappa \right) \right|^2$$

$$= \left| Tr\left(\left| \phi_r^{(m)} \right\rangle \left\langle \phi_{r'}^{(m+1)} \right| R_0 \right) \right|^2 + \left| Tr\left(\left| \phi_r^{(m)} \right\rangle \left\langle \phi_{r'}^{(m+1)} \right| R_1 \right) \right|^2 .$$

Για το στοιχείο $\Delta_{11}^{(m)}$ θα είναι

$$\Delta_{11}^{(m)} = \left| Tr\left(\left| \phi_1^{(m)} \right\rangle \left\langle \phi_1^{(m+1)} \right| R_0 \right) \right|^2 + \left| Tr\left(\left| \phi_1^{(m)} \right\rangle \left\langle \phi_1^{(m+1)} \right| R_1 \right) \right|^2$$

$$= \left| Tr\left((\lambda_0^{(m,1)}, \lambda_1^{(m,1)})^{\mathrm{T}} (\lambda_0^{(m+1,1)}, \lambda_1^{(m+1,1)}) R_0 \right) \right|^2 + \left| Tr\left((\lambda_0^{(m,1)}, \lambda_1^{(m,1)})^{\mathrm{T}} (\lambda_0^{(m+1,1)}, \lambda_1^{(m+1,1)}) R_1 \right) \right|^2$$

Σύμφωνα με τους συμβολισμούς του Κεφαλαίου 2 και την Πρόταση 2.2.1. είναι

$$R_0 = \begin{pmatrix} f(x) & g(x) \\ -g(x) & f(x) \end{pmatrix} \text{ και } R_1 = \begin{pmatrix} h(x) & \varphi(x) \\ -\varphi(x) & h(x) \end{pmatrix}.$$

Μετά την εκτέλεση των πράξεων προκύπτει

$$\Delta_{11}^{(m)} = \left(f(x) \left(\lambda_0^{(m,1)} \lambda_0^{(m+1,1)} + \lambda_1^{(m,1)} \lambda_1^{(m+1,1)} \right) + g(x) \left(\lambda_1^{(m,1)} \lambda_0^{(m+1,1)} - \lambda_0^{(m,1)} \lambda_1^{(m+1,1)} \right) \right)^2$$
$$+ \left(h(x) \left(\lambda_0^{(m,1)} \lambda_0^{(m+1,1)} + \lambda_1^{(m,1)} \lambda_1^{(m+1,1)} \right) + \varphi(x) \left(\lambda_1^{(m,1)} \lambda_0^{(m+1,1)} - \lambda_0^{(m,1)} \lambda_1^{(m+1,1)} \right) \right)^2$$

άρα

$$\Delta_{11}^{(m)} = \left(f(x) B + g(x) C \right)^2 + \left(h(x) B + \varphi(x) C \right)^2 .$$

Αντίστοιχα εργαζόμαστε και για τα υπόλοιπα στοιχεία $\Delta_{r'r}^{(m)}$.
Τέλος, όπως και στην προηγούμενη Πρόταση 3.1. έχουμε ότι για κάθε $m \in \square$ ισχύει

$$S\left(\rho_s^{(m+1)} \right) > S\left(\rho_s^{(m)} \right)$$

διότι $\lambda_{m+1} \prec \lambda_m$ και η Κβαντική εντροπία είναι συνάρτηση κοίλη κατά Schur. Είναι προφανές ότι αν $R_1 = 0$ και R_0 είναι μοναδιακός, η παραπάνω εντροπία παραμένει σταθερή ■

<u>Ορισμός 3.1. :</u>

Έστω Q κάποιο κβαντικό σύστημα το οποίο περιγράφεται από ένα πίνακα πυκνότητας ρ_Q και ρ_{RQ} ο πίνακας πυκνότητας που περιγράφει την προβολικοποίηση του Q σε ένα ευρύτερο σύστημα RQ. Έστω ακόμα η CPTP απεικόνιση Ω με γεννήτορες Kraus $\{A_j\}_{j \in I}$ η οποία δρα στον προβολικό τελεστή ρ_{RQ} και δίνει τον $\rho_{RQ'}$, δηλαδή $\Omega\left(\rho_{RQ}\right) = \rho_{RQ'}$. Τότε η εντροπία ανταλλαγής του συστήματος Q με το περιβάλλον ορίζεται [**17**] *από την ισότητα:*

$$S_e = -Tr\left(\rho_{RQ'} \log \rho_{RQ'} \right).$$

Παρατήρηση:

Η εντροπία ανταλλαγής είναι εσωτερική ιδιότητα του συστήματος Q, δηλαδή εξαρτάται μόνο από αυτό και από την CPTP απεικόνιση. Αποδεικνύεται ότι $S_e = -Tr\left(W \log W\right)$, όπου

$$W_{ij} = Tr\left(A_i \rho_Q A_j^\dagger\right).$$

Ο συμβολισμός αυτός καθώς και οι επόμενοι, θα χρησιμοποιηθούν στην Πρόταση 3.4.

Συμβολισμοί: Για την απεικόνιση $\rho \to \rho' = E_R^m(\rho)$ που ορίζεται ως

$$E_R = \frac{1}{2}\left(AdR_0 I_s R_0^\dagger I_{x_0} + AdR_1 I_s R_1^\dagger I_{x_0}\right)$$

εισάγουμε τους συμβολισμούς:

$$L_j = R_j \mathrm{I}_s R_j^\dagger \mathrm{I}_w = a_j e^{i\gamma_j \sigma_y} \text{ με } j = 0,1$$

$$\gamma_0 \equiv \gamma_0\left(x, N\right) = \pi - \vartheta - 2b_0$$

$$\gamma_1 \equiv \gamma_1\left(x, N\right) = \pi - \vartheta - 2b_1$$

$$\vartheta = \arcsin\left(\frac{2\sqrt{N-1}}{N}\right)$$

$$a_0 \equiv a_0\left(x\right) = \sqrt{\left(f\left(x\right)\right)^2 + \left(g\left(x\right)\right)^2}, a_1 \equiv a_1\left(x\right) = \sqrt{\left(h\left(x\right)\right)^2 + \left(\varphi\left(x\right)\right)^2}$$

$$b_0 \equiv b_0\left(x\right) = \arccos\left(\frac{f\left(x\right)}{\sqrt{\left(f\left(x\right)\right)^2 + \left(g\left(x\right)\right)^2}}\right)$$

$$b_1 \equiv b_1\left(x\right) = \arccos\left(\frac{h\left(x\right)}{\sqrt{\left(h\left(x\right)\right)^2 + \left(\varphi\left(x\right)\right)^2}}\right).$$

Πρόταση 3.4. :

Για την απεικόνιση $\rho \to \rho' = E_R^m(\rho) \equiv \rho^{(m)}$, $m \in N$, *η εντροπία ανταλλαγής με το περιβάλλον είναι:*

i) Σταθερά μηδενική, $S_e = 0$, *όταν* $x \in G$.

ii) Σταθερή (ανεξάρτητη του n*), ίση με* $S_e^{(n+1)} = -Tr\left(W^{(n+1)} \log W^{(n+1)}\right) = -\sum_{i=1,2} \mu_i \log \mu_i$,

όταν $x \notin G$, *με* $\mu_{1,2} = \frac{a_0^2 + a_1^2 \pm \sqrt{a_0^4 + a_1^4 + 2a_0^2 a_1^2 \cos 2\left(\gamma_1 - \gamma_0\right)}}{2}$, $n \in \mathbb{N}_+$.

Απόδειξη:

i) Αν $x \in G$, τότε $x = x_\kappa$, $R_1 = 0$, $R_0 = e^{-\frac{ix_\kappa}{2}\sigma_y}$, και

$$E_R\left(\rho\right) = \left(R_0 \mathrm{I}_s R_0^\dagger \mathrm{I}_w\right)\rho\left(R_0 \mathrm{I}_s R_0^\dagger \mathrm{I}_w\right)^\dagger = L_0 \rho {L_0}^\dagger = e^{i(\pi-\theta+x_\kappa)\sigma_y}\rho e^{-i(\pi-\theta+x_\kappa)\sigma_y}.$$

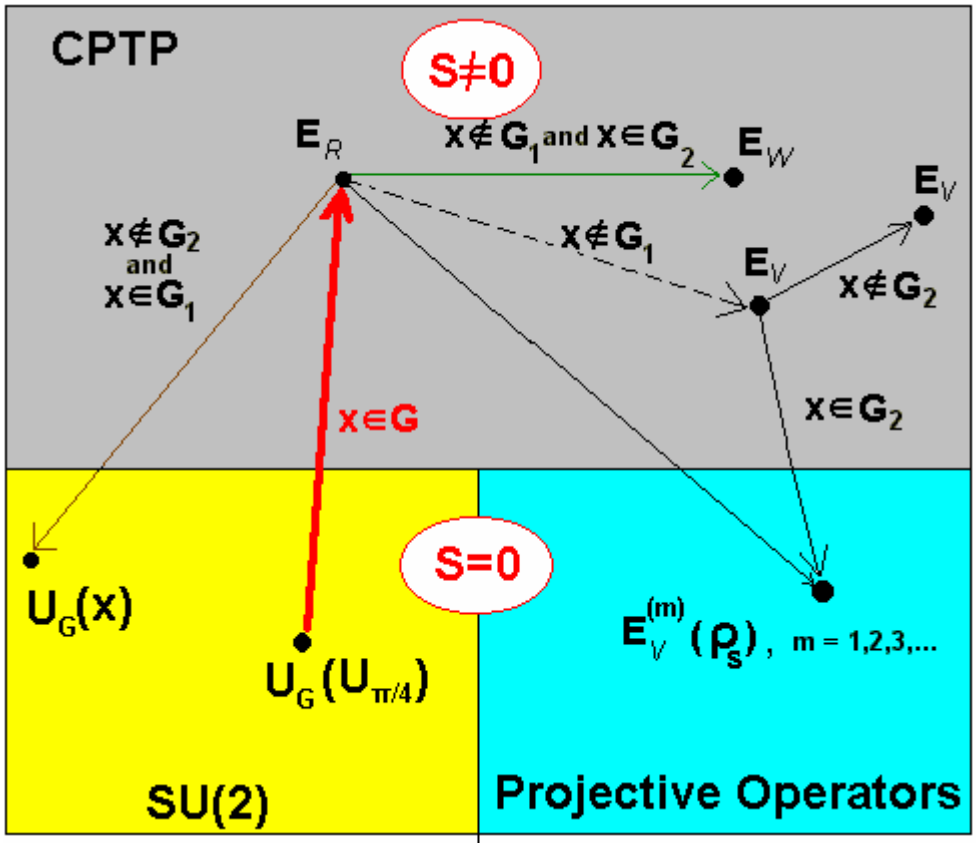
Επομένως για κάθε $n \in \mathbb{N}_+$ θα είναι $E_R{}^n\left(\rho\right) = e^{in(\pi-\theta+x_\kappa)\sigma_y}\rho e^{-in(\pi-\theta+x_\kappa)\sigma_y}$.

Τότε η εντροπία ανταλλαγής θα είναι $S_e^{(n+1)} = -Tr\left(W^{(n+1)} \log W^{(n+1)}\right)$ με $W_{ij}^{(n)} = Tr\left(L_i E_R{}^n\left(\rho\right) L_j^\dagger\right)$, για $j = 0,1$. Από τον ορισμό των L_j έχουμε ότι $L_1 = 0$ και $L_0 = e^{i(\pi-\theta+x_\kappa)\sigma_y}$, άρα αμέσως είναι $W_{01}^{(n)}, W_{10}^{(n)}, W_{11}^{(n)} = 0$. Επίσης $W_{00}^{(n)} = Tr\left(L_0 E_R{}^n\left(\rho\right) L_0^\dagger\right) = Tr\left(L_0^\dagger L_0 E_R{}^n\left(\rho\right)\right) = Tr\left(E_R{}^n\left(\rho\right)\right) = 1$, άρα $W^{(n)} = diag\left\{1,0\right\}$. Ο πίνακας $W^{(n)}$ έχει προφανώς ιδιοτιμές $\mu_{1,2} \in \left\{1,0\right\}$, άρα $S_e^{(n+1)} = -\sum_{i=1,2} \mu_i \log \mu_i = 0$. Εδώ έχουμε χρησιμοποιήσει ότι $0 \log 0 = 0$, πράγμα που φαίνεται εύκολα από το όριο $\lim_{x\to 0^+}\left(x \ln x\right) = 0$ αν χρησιμοποιήσουμε τον κατάλληλο κανόνα De l' Hospital.

ii) Από την Γραμμική Άλγεβρα γνωρίζουμε ότι για έναν πίνακα $A = \begin{bmatrix} \kappa & \lambda \\ \mu & \nu \end{bmatrix}, \kappa, \lambda, \mu, \nu \in C$, ισχύει ότι $Tr\left(e^{ia\sigma_y} A\right) = \left(\cos a\right) TrA + \left(\sin a\right)\left(\mu - \lambda\right)$. Είναι $W_{ij}^{(n+1)} = Tr\left(L_i E_R{}^n\left(\rho\right) L_j^\dagger\right) = Tr\left(L_j^\dagger L_i E_R{}^n\left(\rho\right)\right)$. Αν χρησιμοποιήσουμε την παραπάνω ισότητα για το ίχνος ενός 2x2 πίνακα και την εκθετική γραφή των L_j, δηλαδή $L_j = R_j \mathrm{I}_s R_j^\dagger \mathrm{I}_w = a_j e^{i\gamma_j \sigma_y}$, θα πάρουμε ότι : $W_{10}^{(n+1)} = a_0 a_1 \cos\left(\gamma_1 - \gamma_0\right)$, $W_{01}^{(n+1)} = a_0 a_1 \cos\left(\gamma_1 - \gamma_0\right)$, $W_{00}^{(n+1)} = a_0^2$ και ότι $W_{11}^{(n+1)} = a_1^2$. Από την χαρακτηριστική εξίσωση του $W^{(n+1)}$ προκύπτει αμέσως ότι οι ιδιοτιμές του είναι: $\mu_{1,2} = \dfrac{a_0^2 + a_1^2 \pm \sqrt{a_0^4 + a_1^4 + 2a_0^2 a_1^2 \cos 2\left(\gamma_1 - \gamma_0\right)}}{2}$, ανεξάρτητες του n, άρα η εντροπία ανταλλαγής θα είναι σταθερή (ανεξάρτητη του n) και ίση με $S_e^{(n+1)} = -Tr\left(W^{(n+1)} \log W^{(n+1)}\right) = -\sum_{i=1,2} \mu_i \log \mu_i$ ■

3.3. Γενική περιγραφή και τελικά συμπεράσματα

Τα αποτελέσματα αυτής της εργασίας παρουσιάζονται γενικά στο παρακάτω διάγραμμα:



Ο τελεστής έρευνας στον αλγόριθμο ταχείας αναζήτησης στοιχείου σε μια μη δομημένη βάση δεδομένων ορίστηκε από τον Grover να είναι το γινόμενο δυο ανακλάσεων Householder και αποδείχθηκε ότι υπάρχει ελευθερία ως προς την ομάδα $SU(2)$, με την έννοια ότι μπορεί να δράσει πάνω στο διάνυσμα εκκίνησης μια τυχαία στροφή.
Επιδιώκοντας να εξετάσουμε την συμπεριφορά του αλγόριθμου αν ληφθεί υπ' όψη ο θόρυβος που προέρχεται από το περιβάλλον, θεωρήσαμε ένα στοιχείο της $SU(2)$, μια $\pi/4$-στροφή, βρήκαμε πώς διαταράσσεται αυτή, και ποια θα είναι η καινούρια Χαμιλτονιανή του συστήματος. Κατόπιν είδαμε ότι ο τελεστής έρευνας μπορεί να εκφραστεί με θετικές ιχνοδιατηρητικές απεικονίσεις και να πάρει τρεις βασικές μορφές, τις E_R, E_V και E_W .
Η αποτελεσματικότητα του αλγόριθμου μετράται μέσω της ακτινικής και της γωνιακής αξιοπιστίας.
Η πρώτη και γενικότερη μορφή E_R του τελεστή έρευνας, είναι η άμεση συνέπεια της επίδρασης του θορύβου. Οι άλλες δυο ειδικότερες μορφές προέκυψαν από την διερεύνηση αφενός του αν θα ήταν δυνατόν οι γεννήτορες Kraus του E_R να είναι de facto μοναδιακοί, και αφετέρου από το ποια είναι η βέλτιστη γεωμετρική προσέγγιση στον E_R. Έτσι καταλήξαμε στο να θεωρούμε τρία ξένα μεταξύ τους είδη θορύβου:

Το 1^{ο} είδος θορύβου είναι εκείνο για το οποίο ο τελεστής E_R ανάγεται στην adjoint δράση μόνο ενός μοναδιακού πίνακα και ο αλγόριθμος ανάγεται στην κλασική του μορφή. Η περίπτωση αυτή είναι ισοδύναμη με την ιδανική κατά την οποία δεν υπάρχει καθόλου θόρυβος.

Το 2^{ο} είδος θορύβου είναι εκείνο για το οποίο ο τελεστής E_R έχει δυο μη μηδενικούς γεννήτορες Kraus οι οποίοι όμως είναι και οι δυο μοναδιακοί τελεστές. Στην περίπτωση αυτή τον συμβολίζουμε E_W .
Ως θόρυβος τρίτου είδους θεωρείται αυτός που δεν είναι ούτε πρώτου ούτε δεύτερου είδους.

Αν ο τελεστής έρευνας είναι ο E_R , τότε γενικά ο αλγόριθμος αποτυγχάνει να βρει το ζητούμενο αντικείμενο και αυξάνει την κβαντική εντροπία. Αυτό σημαίνει ότι η εξέλιξη του αρχικού προβολικού τελεστή-πίνακα πυκνότητας πιθανότητας, δίνει σε κάθε βήμα του αλγόριθμου ένα νέο πίνακα πυκνότητας πιθανότητας, του οποίου το διάνυσμα ιδιοτιμών κατισχύεται από το αντίστοιχο διάνυσμα του προηγούμενου βήματος, άρα η εξέλιξη του αλγόριθμου αυξάνει την κατά von Neumann εντροπία. Επίσης η εντροπία ανταλλαγής με το περιβάλλον παραμένει σταθερή σε κάθε βήμα του αλγόριθμου.
Στην ειδική περίπτωση που έχουμε ως τελεστή αναζήτησης τον E_W , ο αλγόριθμος αποτυγχάνει μεν να βρει το ζητούμενο αντικείμενο αλλά βρίσκει την διεύθυνσή του σε $O\left(\sqrt{N}\right)$ επαναλήψεις.

Αν ο θόρυβος δεν είναι πρώτου είδους, τότε κατασκευάζεται ο τελεστής E_V ο οποίος είναι ο γεωμετρικά πλησιέστερος προς τον E_R . Γενικά η αναζήτηση με τελεστή έρευνας τον E_V αποτυγχάνει να βρει το ζητούμενο αντικείμενο και αυξάνει την κβαντική εντροπία εκτός εάν ο θόρυβος είναι δεύτερου είδους. Εάν για τον E_V ο θόρυβος είναι δεύτερου είδους τότε, αυτός είναι προβολικός τελεστής σε κάθε βήμα, ο αλγόριθμος είναι αποτελεσματικός σε $O\left(\sqrt{N}\right)$ επαναλήψεις και η κβαντική εντροπία παραμένει μηδέν.

Είναι φανερό ότι οι συγκεκριμένες τιμές του θορύβου κάθε είδους εξαρτώνται από το ποια θα είναι η αρχική επιλογή στοιχείου της $SU\left(2\right)$, θα μπορούσε να είναι μια άλλη στροφή και όχι μια $\pi/4$ -στροφή, όμως η διερεύνηση παραμένει η ίδια.

Βιβλιογραφία

[1] L. Grover, “Quantum mechanics helps in searching for needle in a haystack,» Phys. Rev. Lett. **78,** 325-328 (1997).

[2] ACM: L. Grover, “A fast quantum mechanical algorithm for database search,” in Proc. 28th Ann. ACM Symp. On the Theory of Computing, (ACM Press, New York, 1996), pp. 212-218.

[3] L. Grover, “Quantum computers can search rapidly by using almost any transformation,» Phys. Rev. Lett. **80,** 4329-4332 (1998).

[4] K. M. R. Audenaer, “A Sharp Fannes-type Inequality for the von Neumann Entropy”, quant-ph/0610146.

[5] R. Bhatia, *Matrix Analysis*, Springer, Heidelberg (1997).

[6] PhysComp’96: M. Boyer, G. Brassard, P. Hoyer and A. Tapp, “Tight bounds on quantum searching,» in Proc. of 4th Workshop on Physics and Computation, pp. 36-43.

[7] A.Chefles, “Quantum Operations, State Transformations and Probabilities’’ quant-ph/0109060.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information,* (Cambridge Univ. Press. 2000).

[9] I. L. Chuang and Y. Yamamoto, “Creation of a persistent bit using error correction» Phys. Rev. A. **55**, 114-127 (1997).

[10] D. Ellinas and C. Konstandakis, Proc. International Conference of Quantum Information, ICQI-2001, (quant-ph/0110010).

[11] D. Ellinas and C. Konstandakis, “Quantum Noise, Information and Robustness in Quantum Database Search”, CP734, *Quantum Communication, Measurement and Computing,* edited by S. M. Barnett et al.

[12] M. Keyl, “Fundamentals of Quantum Information Theory”, quant-ph/0202122.

[13] K. Kraus, *States, Effects and Operations* (Springer, 1983).

[14] A. W. Marshall and I. Olkin, *Inequalities: Theory of majorization and applications* (Academic Press, 1979).

[15] R. T. Perry, *The Temple of Quantum Computing,* (version 1.1, 2006, http://www.toqc.com/TOQCv1_1.pdf).

[16] J. Preskill, *Lecture Notes for Physics 229: Quantum Computation and Information* (California Institute of Technology, September 1998).

[17] B. Schumacher and M. D. Westmoreland, Phys. Rev. A. 56, 131-138 (1997).

[18] B. Schumacher, “Quantum coding”, Phys. Rev. A 51, 2738 (1995).

[19] Wartrous, *CPSC 519: Introduction to Quantum Computation*, (University of Calgary, 2005).

[20] A. Uhlmann, Wiss. Z. Karl-Marx-Univ. Leipzig **20**, 633 (1971) .

[21] Ανδρουλιδάκης Ιωάννης, *Αλγόριθμος Διαστατικής Ελάττωσης Διμερών Εναγκαλισμένων Κβαντικών Συστημάτων,* Διπλωματική Διατριβή Μ.Δ.Ε., Πολυτ.Κρήτης, Γενικό Τμήμα, Τομέας Μαθηματικών, Χανιά 2004.

[22] Κροντήρης Ιωάννης, *Κβαντική Θεωρία Πληροφορίας,* Διπλωματική εργασία, Πολυτ.Κρήτης, Τμήμα ΗΜΜΥ, Χανιά, 2001.