

5 Κβαντική Αναζήτηση: Ο Αλγόριθμος του Grover

Στα προηγούμενα κεφάλαια αναπτύξαμε όλο το απαραίτητο υπόβαθρο: το qubit και τη σφαίρα του Bloch, τις πύλες ενός qubit, τα κυκλώματα πολλαπλών qubit, και τελικά ένα καθολικό σύνολο πυλών, ικανό να υλοποιήσει, τουλάχιστον καταρχήν, οποιονδήποτε μοναδιαίο μετασχηματισμό πάνω σε οποιονδήποτε αριθμό qubit. Το ερώτημα που μένει ανοιχτό, και που είναι φυσικά το πιο ενδιαφέρον από όλα, είναι το εξής: τι μπορούμε πραγματικά να υπολογίσουμε με αυτά τα κυκλώματα, που να μην μπορούμε να το κάνουμε (τουλάχιστον όχι το ίδιο γρήγορα) με έναν κλασικό υπολογιστή;

Σε αυτό το κεφάλαιο θα απαντήσουμε το ερώτημα αυτό για ένα πρώτο, θεμελιώδες πρόβλημα: την αναζήτηση μέσα σε ένα μη ταξινομημένο σύνολο δεδομένων, όπου η μόνη πληροφορία που έχουμε είναι μία διαδικασία που μας λέει αν ένα συγκεκριμένο στοιχείο είναι ή δεν είναι η λύση που ψάχνουμε. Θα μελετήσουμε αναλυτικά τον αλγόριθμο του Grover (1996), ο οποίος λύνει το πρόβλημα αυτό με τετραγωνική επιτάχυνση σε σχέση με κάθε δυνατό κλασικό αλγόριθμο: από τάξη μεγέθους N ερωτήσεων (όπου N το πλήθος των στοιχείων) σε τάξη μεγέθους $\sqrt{N}$.

Θα ακολουθήσουμε την εξής πορεία. Πρώτα θα διατυπώσουμε με ακρίβεια το πρόβλημα της αναζήτησης και θα θυμηθούμε, χωρίς αποδείξεις, την κλασική του πολυπλοκότητα (ενότητα 5.1). Στη συνέχεια θα ορίσουμε το κβαντικό «μαντείο» (oracle), το κύκλωμα-μαύρο-κουτί μέσω του οποίου το πρόβλημα «εισάγεται» σε ένα κβαντικό κύκλωμα (ενότητα 5.2). Θα κατασκευάσουμε κατόπιν τον τελεστή της επανάληψης του Grover και θα δείξουμε, γεωμετρικά, γιατί η επαναλαμβανόμενη εφαρμογή του οδηγεί ολοένα και πιο κοντά στη λύση (ενότητα 5.3). Θα δούμε πώς κατασκευάζεται η αρχική κατάσταση του αλγορίθμου (ενότητα 5.4), και τέλος θα υπολογίσουμε πόσες επαναλήψεις χρειάζονται, ορίζοντας παράλληλα με αυστηρότητα τον συμβολισμό $O(\cdot)$ που χρησιμοποιούμε για να περιγράψουμε την πολυπλοκότητα κάθε αλγορίθμου (ενότητα 5.5).

5.1 Το πρόβλημα της αναζήτησης και η κλασική πολυπλοκότητα

Ας θεωρήσουμε ένα σύνολο N στοιχείων $x_0, x_1, \dots, x_{N-1}$, και ας υποθέσουμε ότι θέλουμε να βρούμε εκείνα (ή έστω ένα από εκείνα) που ικανοποιούν κάποια συγκεκριμένη ιδιότητα. Μπορούμε να περιγράψουμε οποιοδήποτε τέτοιο πρόβλημα αναζήτησης μέσω μίας συνάρτησης f πάνω στους δείκτες $i = 0, 1, \dots, N - 1$,

$$f(i) = \begin{cases} 1, & \text{αν το } x_i \text{ είναι λύση του προβλήματος,} \\ 0, & \text{διαφορετικά,} \end{cases}$$

δηλαδή η αναζήτηση ανάγεται πάντα στην εύρεση ενός (ή περισσότερων) δεικτών i με $f(i) = 1$.

Το σημαντικό χαρακτηριστικό που θα υποθέσουμε εδώ είναι ότι το σύνολο είναι *μη ταξινομημένο*: δεν έχουμε καμία επιπλέον δομή (όπως π.χ. μία διάταξη) που να μας επιτρέπει να «μαντέψουμε» πού βρίσκεται η λύση. Η μόνη πληροφορία που έχουμε στη διάθεσή μας είναι η δυνατότητα να *ελέγχουμε* ένα συγκεκριμένο x_i , δηλαδή να υπολογίσουμε το $f(i)$ για όποιο i επιλέξουμε. Αυτό είναι το λεγόμενο μοντέλο του *μαύρου κουτιού*, ή *μαντείου* (oracle): θεωρούμε το f δεδομένο, χωρίς να μας ενδιαφέρει πώς υπολογίζεται εσωτερικά, και μετράμε την «δουλειά» που κάνει ο αλγόριθμος μέσω του πλήθους των ερωτήσεων που θέτει στο μαντείο.

Η προφανής, γραμμική αναζήτηση (linear search) ελέγχει τα στοιχεία ένα-ένα, $i = 0, 1, 2, \dots$, μέχρι να βρεθεί κάποιο με $f(i) = 1$. Αν υπάρχει ακριβώς μία λύση, στη χειρότερη περίπτωση χρειάζονται N ερωτήσεις (η λύση είναι η τελευταία που ελέγχουμε), ενώ κατά μέσο όρο χρειάζονται περίπου $N/2$. Και οι δύο αυτές ποσότητες είναι, όπως θα ορίσουμε αυστηρά στην ενότητα 5.5, τάξης μεγέθους N , δηλαδή $O(N)$. Το πιο σημαντικό είναι ότι, χωρίς επιπλέον δομή, κανένας κλασικός αλγόριθμος δεν μπορεί να κάνει καλύτερα από $O(N)$ ερωτήσεις στη χειρότερη περίπτωση: αφού η μόνη πληροφορία που αποκτάμε είναι μία απάντηση ναι/όχι ανά ερώτηση, και δεν υπάρχει καμία δομή να μας καθοδηγήσει ποιο στοιχείο να ελέγξουμε επόμενο, δεν υπάρχει τρόπος να αποκλείσουμε πολλά στοιχεία ταυτόχρονα με μία μόνο ερώτηση. Δεν θα αποδείξουμε εδώ αυτό το (διαισθητικά αναμενόμενο) κλασικό κάτω φράγμα, απλώς θα το χρησιμοποιήσουμε ως σημείο αναφοράς.

Αξίζει να τονίσουμε τη διαφορά με την *δυαδική αναζήτηση* (binary search), που πετυχαίνει $O(\log N)$ σε ένα ταξινομημένο σύνολο: εκεί η επιπλέον δομή (η διάταξη) είναι ακριβώς αυτό που επιτρέπει σε κάθε ερώτηση

να αποκλείει τα μισά εναπομείναντα στοιχεία. Στο μη ταξινομημένο πρόβλημα που μας απασχολεί εδώ δεν υπάρχει τέτοια δομή να εκμεταλλευτούμε, και το $O(N)$ είναι το καλύτερο δυνατό, κλασικά.

Το ερώτημα είναι λοιπόν: μπορεί ένας κβαντικός υπολογιστής, χρησιμοποιώντας υπέρθεση, να κάνει καλύτερα από $O(N)$ ερωτήσεις στο ίδιο ακριβώς πρόβλημα, χωρίς καμία πρόσθετη δομή; Η απάντηση, όπως θα δούμε, είναι ναι: ο αλγόριθμος του Grover χρειάζεται μόνο $O(\sqrt{N})$ ερωτήσεις.

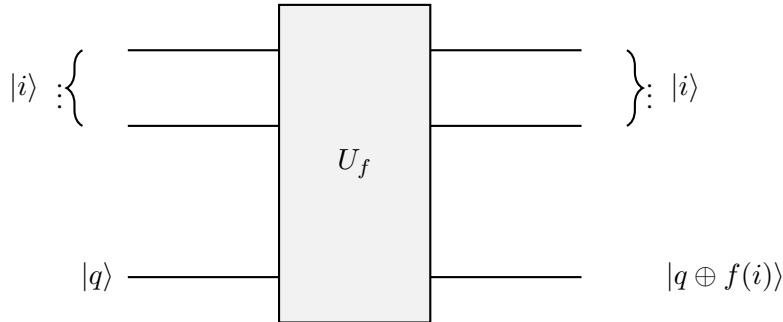
5.2 Το κβαντικό «μαντείο» (oracle)

Για να «εισάγουμε» το πρόβλημα της προηγούμενης ενότητας σε ένα κβαντικό κύκλωμα, κωδικοποιούμε κάθε δείκτη $i \in \{0, 1, \dots, N-1\}$ ως έναν αριθμό n qubit, με $N = 2^n$, ακριβώς όπως κωδικοποιούσαμε τους συνδυασμούς bit στο προηγούμενο κεφάλαιο (ενότητα 4): η κατάσταση της υπολογιστικής βάσης $|i\rangle$ αντιστοιχεί στη δυαδική αναπαράσταση του i . Το $|i\rangle$ θα το ονομάζουμε *qubit-δείκτη* (index register).

Υποθέτουμε ότι υπάρχει ένα κβαντικό κύκλωμα, το *μαντείο*, που υλοποιεί τη συνάρτηση f . Επειδή κάθε κβαντικό κύκλωμα (χωρίς μέτρηση) είναι μοναδιαίο, άρα αντιστρέψιμο, δεν μπορούμε απλώς να απεικονίσουμε $|i\rangle \rightarrow |f(i)\rangle$: όπως ακριβώς είδαμε με το κβαντικό AND και OR (παραδείγματα 4.8, 4.9), μία τέτοια απεικόνιση χάνει πληροφορία (πολλά i μπορεί να δίνουν το ίδιο $f(i)$) και άρα δεν μπορεί να είναι αντιστρέψιμη. Η λύση είναι η ίδια που χρησιμοποιήσαμε εκεί: προσθέτουμε ένα βοηθητικό (ancilla) qubit-στόχο $|q\rangle$, και ορίζουμε το μαντείο ως τον μοναδιαίο τελεστή $\hat{U}_f$ με

$$\hat{U}_f |i\rangle |q\rangle = |i\rangle |q \oplus f(i)\rangle.$$

Το $\hat{U}_f$ είναι πράγματι αντιστρέψιμο (είναι η ίδια η αντίστροφή του: εφαρμόζοντάς το δύο φορές επαναφέρουμε το $|q\rangle$ στην αρχική του τιμή, αφού $(q \oplus f(i)) \oplus f(i) = q$), και το qubit-δείκτη $|i\rangle$ παραμένει πάντα αμετάβλητο. Σε ένα κύκλωμα το παριστάνουμε ως εξής:



Στα επόμενα δεν θα μας απασχολήσει καθόλου πώς υλοποιείται εσωτερικά το $\hat{U}_f$: το αντιμετωπίζουμε ως ένα μαύρο κουτί, και ο μόνος «πόρος» που μετράμε είναι το πλήθος των φορών που το καλούμε.

Το πραγματικά χρήσιμο τέχνασμα, που θα χρησιμοποιήσουμε σε όλο το υπόλοιπο κεφάλαιο, είναι να προετοιμάσουμε το βοηθητικό qubit όχι στην $|0\rangle$ ή στην $|1\rangle$, αλλά στην κατάσταση

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

Αν $f(i) = 0$, το $\hat{U}_f$ αφήνει το $|-\rangle$ αμετάβλητο,

$$\hat{U}_f |i\rangle |-\rangle = \frac{1}{\sqrt{2}} |i\rangle (|0 \oplus 0\rangle - |1 \oplus 0\rangle) = \frac{1}{\sqrt{2}} |i\rangle (|0\rangle - |1\rangle) = |i\rangle |-\rangle.$$

Αν όμως $f(i) = 1$, τα δύο qubit της υπέρθεσης «ανταλλάσσουν θέση»,

$$\hat{U}_f |i\rangle |-\rangle = \frac{1}{\sqrt{2}} |i\rangle (|0 \oplus 1\rangle - |1 \oplus 1\rangle) = \frac{1}{\sqrt{2}} |i\rangle (|1\rangle - |0\rangle) = -|i\rangle |-\rangle.$$

Στις δύο περιπτώσεις μαζί,

$$\hat{U}_f |i\rangle |-\rangle = (-1)^{f(i)} |i\rangle |-\rangle.$$

Δηλαδή, όσο το βοηθητικό qubit παραμένει στο $|-\rangle$ (και παραμένει, ακριβώς στο $|-\rangle$, σε κάθε κλήση του μαντείου), το μόνο που αλλάζει είναι μία *φάση* $(-1)^{f(i)}$ πάνω στο qubit-δείκτη: το φαινόμενο αυτό λέγεται *ανάδραση φάσης* (phase kickback). Μπορούμε λοιπόν να ξεχάσουμε εντελώς το βοηθητικό qubit (αρκεί να το προετοιμάσουμε μία φορά στην αρχή, όπως θα δούμε στην ενότητα 5.4) και να σκεφτόμαστε το μαντείο σαν έναν τελεστή που δρα μόνο πάνω στο qubit-δείκτη,

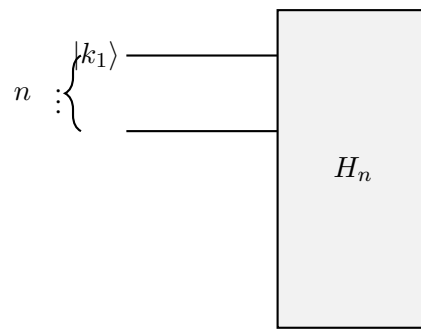
$$\hat{O} |i\rangle = (-1)^{f(i)} |i\rangle,$$

τον οποίο θα ονομάζουμε *τελεστή φάσης* του μαντείου. Ο $\hat{O}$ είναι αυτός που θα χρησιμοποιήσουμε αποκλειστικά στη συνέχεια.

5.3 Η επανάληψη του Grover

Ο μετασχηματισμός Hadamard $\hat{H}_n$

Το πρώτο συστατικό της κβαντικής αναζήτησης είναι ο μετασχηματισμός Hadamard πάνω σε όλα τα n qubit του qubit-δείκτη ταυτόχρονα, δηλαδή απλώς n ανεξάρτητες πύλες Hadamard, μία σε κάθε qubit:

$$\hat{H}_n = \underbrace{\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}}_{n \text{ φορές}}.$$


Χρησιμοποιώντας τη γνωστή δράση μίας πύλης Hadamard πάνω σε ένα bit της υπολογιστικής βάσης, $\mathbf{H} |k\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^k |1\rangle)$ (ενότητα 3.13), και το ότι το ταυυστικό γινόμενο εφαρμόζεται qubit προς qubit (ενότητα 2.9), για μία κατάσταση $|k\rangle = |k_1\rangle \otimes \cdots \otimes |k_n\rangle$ της υπολογιστικής βάσης παίρνουμε

$$\hat{H}_n |k\rangle = \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^n (|0\rangle + (-1)^{k_\ell} |1\rangle) = \frac{1}{2^{n/2}} \sum_b (-1)^{\mathbf{b} \cdot \mathbf{k}} |b\rangle,$$

όπου το άθροισμα είναι πάνω σε όλες τις 2^n καταστάσεις $|b\rangle = |b_1\rangle \otimes \cdots \otimes |b_n\rangle$ της υπολογιστικής βάσης, και $\mathbf{b} \cdot \mathbf{k} = b_1 k_1 + \cdots + b_n k_n$. Η ειδική περίπτωση $k = 0$, δηλαδή $|k\rangle = |0 \cdots 0\rangle$, θα μας απασχολήσει συνέχεια:

$$\hat{H}_n |0\rangle = \frac{1}{2^{n/2}} \sum_b |b\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle =: |\psi\rangle.$$

Δηλαδή ο $\hat{H}_n$, εφαρμοσμένος στην κατάσταση $|0 \cdots 0\rangle$, παράγει μία *ομοιόμορφη υπέρθεση* $|\psi\rangle$ όλων των N δεικτών, με το ίδιο πλάτος $1/\sqrt{N}$ σε καθέναν: ακριβώς αυτό που χρειαζόμαστε ως αφετηρία, αφού δεν έχουμε a priori κανέναν λόγο να προτιμήσουμε κάποιον δείκτη έναντι κάποιου άλλου.

Θα χρειαστούμε επίσης δύο απλές ιδιότητες του $\hat{H}_n$: αφού $\mathbf{H}^2 = \mathbf{I}_2$ (η Hadamard είναι η αντίστροφη της) και $\mathbf{H}^T = \mathbf{H}$ (είναι πραγματικός, συμμετρικός πίνακας), οι ίδιες ιδιότητες περνάνε αυτόματα και στο ταυυστικό γινόμενο:

$$\hat{H}_n^2 = \hat{I}, \quad \hat{H}_n^T = \hat{H}_n.$$

Η επιλεκτική αλλαγή φάσης γύρω από το $|0\rangle$

Το δεύτερο συστατικό είναι ένας τελεστής $\hat{U}_0$ που αλλάζει πρόσημο σε κάθε στοιχείο της υπολογιστικής βάσης, εκτός από το $|0 \cdots 0\rangle$:

$$\hat{U}_0 |b\rangle = \begin{cases} |0\rangle, & b = 0, \\ -|b\rangle, & b \neq 0. \end{cases}$$

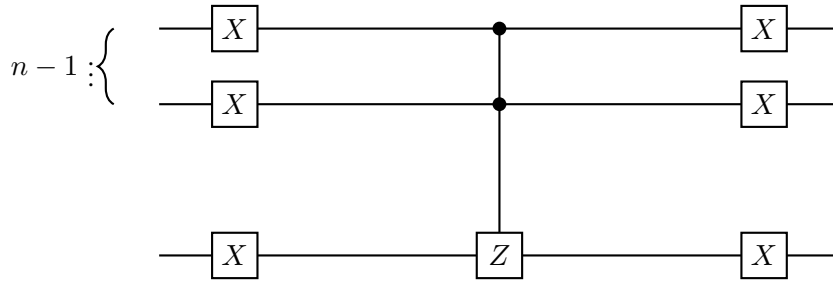
Χρησιμοποιώντας το σύμβολο Kronecker δ_{pq} ($= 1$ αν $p = q$, $= 0$ διαφορετικά) μπορούμε να γράψουμε συμπαγώς $\hat{U}_0 |b\rangle = -(-1)^{\delta_{b0}} |b\rangle$. Τα στοιχεία του αντίστοιχου πίνακα $u_{pq} = \langle p | \hat{U}_0 | q \rangle$ είναι

$$u_{pq} = \begin{cases} 1, & p = q = 0, \\ -1, & p = q \neq 0, \\ 0, & p \neq q, \end{cases}$$

που γράφονται όλα μαζί ως $u_{pq} = 2\delta_{p0}\delta_{q0} - \delta_{pq}$ (ελέγξτε: για $p = q = 0$ δίνει $2 - 1 = 1$, για $p = q \neq 0$ δίνει $0 - 1 = -1$, και για $p \neq q$ δίνει $0 - 0 = 0$). Ο πρώτος όρος είναι ακριβώς ο πίνακας του τελεστή προβολής $|0\rangle\langle 0|$ (ενότητα 1.23), πολλαπλασιασμένος επί 2, οπότε

$$U_0 = 2|0\rangle\langle 0| - I.$$

Ο $\hat{U}_0$ υλοποιείται με τεχνικές που ήδη γνωρίζουμε: αφού U_0 αλλάζει πρόσημο ακριβώς όταν τουλάχιστον ένα bit είναι 1, αρκεί μία $(n-1)$ -ελεγχόμενη πύλη Z (κατασκευάζεται απευθείας από το αποτέλεσμα της ενότητας 4.5, θέτοντας $U = Z$), «τυλιγμένη» ανάμεσα σε πύλες X σε κάθε qubit, ώστε το «όλα 1» της ελεγχόμενης Z να αντιστοιχεί στο «όλα 0» του αρχικού qubit:



Το κύκλωμα αυτό αλλάζει πρόσημο ακριβώς όταν, μετά τις πρώτες X , όλα τα qubit είναι $|1\rangle$, δηλαδή ακριβώς όταν $b = 0 \cdots 0$ πριν τις X : υλοποιεί δηλαδή τον πίνακα $\text{diag}(-1, 1, \dots, 1) = I - 2|0\rangle\langle 0| = -U_0$. Η καθολική φάση -1 δεν έχει καμία φυσική συνέπεια (ενότητα 3.1), όπως θα επιβεβαιώσουμε αμέσως παρακάτω, οπότε το κύκλωμα αυτό είναι, για όλους τους πρακτικούς σκοπούς, ο $\hat{U}_0$.

Ο τελεστής διάχυσης και η επανάληψη του Grover

Συνδυάζοντας τα δύο παραπάνω συστατικά ορίζουμε τον *τελεστή διάχυσης* (diffusion operator)

$$\hat{\Gamma} = \hat{H}_n \hat{U}_0 \hat{H}_n.$$

Χρησιμοποιώντας $U_0 = 2|0\rangle\langle 0| - I$ και $\hat{H}_n^2 = I$,

$$\hat{\Gamma} = \hat{H}_n (2|0\rangle\langle 0| - I) \hat{H}_n = 2\hat{H}_n |0\rangle\langle 0| \hat{H}_n - \hat{H}_n \hat{H}_n = 2(\hat{H}_n |0\rangle)(\langle 0| \hat{H}_n) - I.$$

Αφού $\hat{H}_n |0\rangle = |\psi\rangle$ και, χρησιμοποιώντας $\hat{H}_n^T = \hat{H}_n$, $\langle 0| \hat{H}_n = \langle \psi|$, καταλήγουμε στο

$$\hat{\Gamma} = 2|\psi\rangle\langle \psi| - I.$$

Ο τελεστής αυτός έχει μία ωραία γεωμετρική ερμηνεία: πάνω σε μία κατάσταση $|\phi\rangle$, ο $2|\psi\rangle\langle \psi|$ την προβάλλει στο $|\psi\rangle$ (πολλαπλασιασμένη επί 2), και αφαιρώντας το $|\phi\rangle$ παίρνουμε την *ανάκλαση* του $|\phi\rangle$ γύρω από το $|\psi\rangle$. Για αυτό το λόγο ο $\hat{\Gamma}$ λέγεται μερικές φορές «αναστροφή γύρω από τον μέσο όρο» (inversion about the mean).

Ο τελεστής της *επανάληψης του Grover* (Grover iteration) είναι απλώς ο συνδυασμός του τελεστή διάχυσης με το μαντέιο,

$$\hat{G} = \hat{\Gamma} \hat{O} = (2|\psi\rangle\langle \psi| - I) \hat{O}.$$

Γεωμετρική ανάλυση της δράσης του $\hat{G}$

Για να καταλάβουμε τι κάνει ο $\hat{G}$, χωρίζουμε τους N δείκτες σε δύο σύνολα, τις λύσεις και τις μη λύσεις,

$$S_1 = \{i : f(i) = 1\}, \quad S_0 = \{i : f(i) = 0\},$$

και συμβολίζουμε με $M = |S_1|$ το πλήθος των λύσεων (άρα $N - M = |S_0|$). Ορίζουμε τις δύο ομοιόμορφες υπερθέσεις

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{i \in S_1} |i\rangle, \quad |\psi_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{i \in S_0} |i\rangle,$$

οι οποίες, αφού τα S_0, S_1 δεν έχουν κοινά στοιχεία, είναι ορθοκανονικές μεταξύ τους, $\langle \psi_0 | \psi_1 \rangle = 0$.

Το $|\psi\rangle$ γράφεται πολύ απλά σε αυτή τη βάση: χωρίζοντας το άθροισμα που το ορίζει σε δύο κομμάτια,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} \sum_{i \in S_0} |i\rangle + \frac{1}{\sqrt{N}} \sum_{i \in S_1} |i\rangle = \sqrt{\frac{N-M}{N}} |\psi_0\rangle + \sqrt{\frac{M}{N}} |\psi_1\rangle.$$

Ορίζοντας μία γωνία $\theta \in [0, \pi]$ με

$$\cos \frac{\theta}{2} = \sqrt{\frac{N-M}{N}}, \quad \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}},$$

(που είναι πάντα δυνατό αφού το άθροισμα των τετραγώνων κάνει 1), γράφουμε συμπαγώς

$$|\psi\rangle = \cos \frac{\theta}{2} |\psi_0\rangle + \sin \frac{\theta}{2} |\psi_1\rangle.$$

Ας δούμε τώρα πώς δρουν οι $\hat{O}$ και $\hat{\Gamma}$ πάνω στα $|\psi_0\rangle, |\psi_1\rangle$. Ο τελεστής φάσης του μαντείου αφήνει αμετάβλητο κάθε $|i\rangle$ με $i \in S_0$ και αλλάζει πρόσημο σε κάθε $|i\rangle$ με $i \in S_1$, οπότε, από τη γραμμικότητα,

$$\begin{aligned} \hat{O} |\psi_0\rangle &= \frac{1}{\sqrt{N-M}} \sum_{i \in S_0} \hat{O} |i\rangle = \frac{1}{\sqrt{N-M}} \sum_{i \in S_0} |i\rangle = |\psi_0\rangle, \\ \hat{O} |\psi_1\rangle &= \frac{1}{\sqrt{M}} \sum_{i \in S_1} \hat{O} |i\rangle = -\frac{1}{\sqrt{M}} \sum_{i \in S_1} |i\rangle = -|\psi_1\rangle. \end{aligned}$$

Δηλαδή, μέσα στο επίπεδο που παράγουν τα $|\psi_0\rangle, |\psi_1\rangle$, ο $\hat{O}$ γράφεται ως ο πίνακας

$$\mathbf{O} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(στη βάση $|\psi_0\rangle, |\psi_1\rangle$). Παρατηρήστε επίσης ότι, αφού ο $\hat{O}$ απεικονίζει κάθε $|\psi_0\rangle, |\psi_1\rangle$ ξανά μέσα στο ίδιο επίπεδο, το επίπεδο αυτό είναι *αναλλοίωτο* κάτω από τον $\hat{O}$.

Το ίδιο ισχύει και για τον $\hat{\Gamma}$: αφού $|\psi\rangle$ ανήκει στο επίπεδο $\{|\psi_0\rangle, |\psi_1\rangle\}$, για οποιοδήποτε $|\phi\rangle = a|\psi_0\rangle + b|\psi_1\rangle$ μέσα στο επίπεδο, το $\hat{\Gamma}|\phi\rangle = 2\langle\psi|\phi\rangle|\psi\rangle - |\phi\rangle$ είναι επίσης μέσα στο επίπεδο (διαφορά δύο διανυσμάτων του επιπέδου). Άρα το ίδιο επίπεδο είναι αναλλοίωτο και κάτω από τον $\hat{\Gamma}$, άρα και κάτω από τον $\hat{G} = \hat{\Gamma}\hat{O}$: μπορούμε λοιπόν να μελετήσουμε τη δράση του $\hat{G}$ αποκλειστικά μέσα σε αυτό το δισδιάστατο επίπεδο, αγνοώντας εντελώς όλες τις άλλες διαστάσεις του χώρου.

Για να βρούμε τον πίνακα του $\hat{\Gamma} = 2|\psi\rangle\langle\psi| - \hat{I}$ σε αυτή τη βάση, γράφουμε $c = \cos(\theta/2)$, $s = \sin(\theta/2)$, οπότε $|\psi\rangle = c|\psi_0\rangle + s|\psi_1\rangle$, και ο τελεστής προβολής $|\psi\rangle\langle\psi|$ έχει πίνακα

$$\begin{bmatrix} c \\ s \end{bmatrix} \begin{bmatrix} c & s \end{bmatrix} = \begin{bmatrix} c^2 & cs \\ cs & s^2 \end{bmatrix}.$$

Άρα, χρησιμοποιώντας $\cos \theta = 2c^2 - 1 = 1 - 2s^2$ και $\sin \theta = 2cs$,

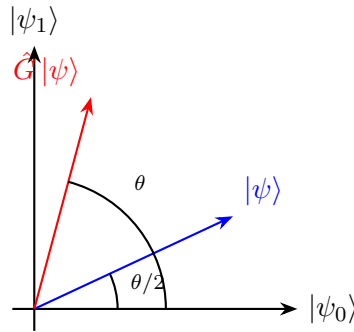
$$\mathbf{\Gamma} = 2 \begin{bmatrix} c^2 & cs \\ cs & s^2 \end{bmatrix} - \mathbf{I} = \begin{bmatrix} 2c^2 - 1 & 2cs \\ 2cs & 2s^2 - 1 \end{bmatrix} = \begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix}.$$

Πολλαπλασιάζοντας με τον $\mathbf{O}$,

$$\mathbf{G} = \mathbf{\Gamma O} = \begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Αναγνωρίζουμε αμέσως τον πίνακα αυτόν: είναι ακριβώς ο πίνακας μίας στροφής κατά γωνία θ στο επίπεδο, αντίστοιχος (αλλά διαφορετικός) από τους πίνακες στροφής $\mathbf{R}_x, \mathbf{R}_y, \mathbf{R}_z$ που συναντήσαμε στη σφαίρα του Bloch: εκεί στρέφαμε την κατάσταση ενός qubit γύρω από έναν άξονα, εδώ στρέφουμε το διάνυσμα των συντελεστών (a, b) μέσα στο πραγματικό επίπεδο που παράγουν τα $|\psi_0\rangle, |\psi_1\rangle$. Η αναλογία με τις περιστροφές, που μας συνόδευσε σε όλο το προηγούμενο κεφάλαιο, εμφανίζεται λοιπόν ξανά, με διαφορετική μορφή, και στην καρδιά του αλγορίθμου αναζήτησης.

Αφού λοιπόν ο $\hat{G}$ δρα ως στροφή κατά γωνία θ μέσα στο επίπεδο $\{|\psi_0\rangle, |\psi_1\rangle\}$, και το $|\psi\rangle$ βρίσκεται εκεί σε γωνία $\theta/2$ από τον άξονα $|\psi_0\rangle$, η εφαρμογή του $\hat{G}$ μεταφέρει το $|\psi\rangle$ σε γωνία $\theta/2 + \theta = 3\theta/2$:



(οι γωνίες στο σχήμα είναι ενδεικτικές, όχι σε κλίμακα). Επαναλαμβάνοντας k φορές, κάθε φορά προσθέτουμε άλλη μία γωνία θ , οπότε

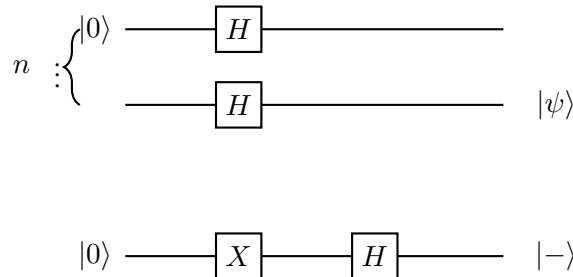
$$\hat{G}^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |\psi_0\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |\psi_1\rangle.$$

Βλέπουμε λοιπόν καθαρά τι κάνει ο αλγόριθμος: ξεκινώντας πολύ κοντά στο $|\psi_0\rangle$ (μακριά από τη λύση, αφού θ είναι μικρό όταν $M \ll N$), κάθε επανάληψη του $\hat{G}$ στρέφει την κατάσταση κατά θ προς το $|\psi_1\rangle$ (όλο και πιο κοντά στη λύση), και αρκεί να επιλέξουμε τον σωστό αριθμό επαναλήψεων K ώστε το $\hat{G}^K |\psi\rangle$ να βρεθεί όσο πιο κοντά γίνεται στο $|\psi_1\rangle$. Θα υπολογίσουμε ακριβώς αυτό το K στην ενότητα 5.5.

5.4 Κατασκευή της αρχικής κατάστασης

Έχουμε πλέον όλα τα κομμάτια που χρειαζόμαστε: μένει να δούμε πώς ξεκινάει, στην πράξη, ολόκληρο το κύκλωμα. Χρησιμοποιούμε $n+1$ qubit συνολικά: τα n qubit του qubit-δείκτη, αρχικοποιημένα στην $|0 \dots 0\rangle$, και ένα βοηθητικό qubit, αρχικοποιημένο στην $|0\rangle$, το οποίο θα χρησιμοποιήσουμε για την ανάδραση φάσης της ενότητας 5.2.

Εφαρμόζουμε τον $\hat{H}_n$ στα πρώτα n qubit, ώστε να πάρουμε την ομοιόμορφη υπέρθεση $|\psi\rangle$ (ενότητα 5.3), και τον συνδυασμό πυλών HX στο βοηθητικό qubit, ώστε να το μετατρέψουμε από $|0\rangle$ σε $|-\rangle$ (αφού $\mathbf{X}|0\rangle = |1\rangle$ και $\mathbf{H}|1\rangle = |-\rangle$, ενότητα 3.13):



Έτσι η συνολική κατάσταση μετά από αυτό το πρώτο βήμα είναι $|\psi\rangle \otimes |-\rangle$. Από εδώ και πέρα εφαρμόζουμε K φορές την επανάληψη του Grover $\hat{G} = \hat{\Gamma}\hat{O}$ πάνω στο qubit-δείκτη, χρησιμοποιώντας κάθε φορά

το ίδιο βοηθητικό qubit ως ενδιάμεσο βήμα μέσα στον $\hat{O}$: όπως δείξαμε στην ενότητα 5.2, το βοηθητικό qubit επιστρέφει ακριβώς στο $|-\rangle$ μετά από κάθε κλήση του μαντείου, οπότε μπορεί να ξαναχρησιμοποιηθεί απεριόριστες φορές χωρίς καμία επιπλέον προετοιμασία. Στο τέλος των K επαναλήψεων, το βοηθητικό qubit παραμένει στο $|-\rangle$ (μπορούμε, αν θέλουμε, να το επαναφέρουμε στο $|0\rangle$ εφαρμόζοντας ξανά XH , αν και αυτό δεν είναι απαραίτητο), ενώ το qubit-δείκτη βρίσκεται πλέον στην κατάσταση $\hat{G}^K |\psi\rangle$ που υπολογίσαμε στην ενότητα 5.3.

5.5 Πολυπλοκότητα του αλγορίθμου

Ο συμβολισμός $O(\cdot)$

Πριν υπολογίσουμε πόσες επαναλήψεις K χρειάζεται ο αλγόριθμος του Grover, ας ορίσουμε με ακρίβεια τον συμβολισμό *big-O*, που χρησιμοποιούμε ήδη ανεπίσημα από την ενότητα 5.1 για να περιγράψουμε την πολυπλοκότητα ενός αλγορίθμου, δηλαδή το πώς μεγαλώνει το «κόστος» του (π.χ. το πλήθος των ερωτήσεων σε ένα μαντείο, ή ο χρόνος εκτέλεσης) καθώς μεγαλώνει το μέγεθος N του προβλήματος.

Λέμε ότι μία συνάρτηση $g(N)$ είναι $O(h(N))$, και γράφουμε $g(N) = O(h(N))$, αν υπάρχουν μία σταθερά $c > 0$ και ένα N_0 τέτοια ώστε

$$|g(N)| \leq c |h(N)| \quad \text{για κάθε } N \geq N_0.$$

Διαισθητικά, το $g(N) = O(h(N))$ σημαίνει ότι το g δεν μεγαλώνει *πιο γρήγορα* από το h , αγνοώντας πολλαπλασιαστικές σταθερές και ό,τι συμβαίνει για μικρά N : μας ενδιαφέρει μόνο η *ασυμπτωτική* συμπεριφορά, για πολύ μεγάλα N .

Παράδειγμα 5.1: Ο συμβολισμός $O(\cdot)$

Ας δείξουμε ότι $g(N) = 3N^2 + 5N + 7$ είναι $O(N^2)$. Χρειαζόμαστε μία σταθερά c και ένα N_0 τέτοια ώστε $3N^2 + 5N + 7 \leq cN^2$ για κάθε $N \geq N_0$. Για $N \geq 1$ ισχύει $N \leq N^2$ και $7 \leq 7N^2$, οπότε

$$3N^2 + 5N + 7 \leq 3N^2 + 5N^2 + 7N^2 = 15N^2,$$

δηλαδή η ανισότητα ικανοποιείται με $c = 15$ και $N_0 = 1$. Αντίθετα, $g(N) = 3N^2 + 5N + 7$ δεν είναι $O(N)$: όσο μεγάλη κι αν επιλέξουμε τη σταθερά c , ο όρος $3N^2$ ξεπερνάει τελικά το cN για αρκετά μεγάλο N (συγκεκριμένα για $N > c/3$), οπότε καμία σταθερά c δεν μπορεί να δουλέψει για όλα τα αρκετά μεγάλα N .

Με αυτόν τον ορισμό, η γραμμική αναζήτηση της ενότητας 5.1 είναι $O(N)$: το πλήθος των ερωτήσεων στη χειρότερη περίπτωση είναι ακριβώς $N \leq 1 \cdot N$ για κάθε $N \geq 1$.

Ο αριθμός επαναλήψεων του Grover

Από την ενότητα 5.3 γνωρίζουμε ότι $\sin(\theta/2) = \sqrt{M/N}$. Θα υποθέσουμε εδώ ότι οι λύσεις είναι σχετικά σπάνιες, $M \ll N$, οπότε το θ είναι μία μικρή γωνία. Χρησιμοποιώντας την προσέγγιση $\sin x \approx x$ για μικρά x ,

$$\sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \approx \frac{\theta}{2} \implies \theta \approx 2\sqrt{\frac{M}{N}}.$$

Θέλουμε να βρούμε το K για το οποίο η γωνία $(2K+1)\theta/2$ του $\hat{G}^K |\psi\rangle$ (ενότητα 5.3) πλησιάζει όσο γίνεται το $\pi/2$, αφού εκεί $\cos(\pi/2) = 0$ και $\sin(\pi/2) = 1$, δηλαδή $\hat{G}^K |\psi\rangle \approx |\psi_1\rangle$: η κατάσταση ταυτίζεται (με πολύ μεγάλη ακρίβεια) με την ομοιόμορφη υπέρθεση των λύσεων. Θέτοντας

$$\frac{2K+1}{2} \theta \approx \frac{\pi}{2} \implies K \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{\frac{N}{M}} - \frac{1}{2} < \frac{\pi}{4} \sqrt{\frac{N}{M}}.$$

Καταλήγουμε λοιπόν στο εξής θεμελιώδες αποτέλεσμα.

Αποτέλεσμα 5.1: Πολυπλοκότητα του αλγορίθμου του Grover

Για αναζήτηση μέσα σε N στοιχεία με $M \ll N$ λύσεις, ο αλγόριθμος του Grover εντοπίζει μία λύση (με πιθανότητα πολύ κοντά στο 1) μετά από

$$K \approx \frac{\pi}{4} \sqrt{\frac{N}{M}}$$

κλήσεις του μαντείου. Ειδικότερα, για μία μόνο λύση ($M = 1$), $K \approx \frac{\pi}{4} \sqrt{N} = O(\sqrt{N})$: τετραγωνική επιτάχυνση σε σχέση με την κλασική πολυπλοκότητα $O(N)$ της ενότητας 5.1.

Παράδειγμα 5.2: Αναζήτηση σε 8 στοιχεία με μία λύση

Ας δούμε αριθμητικά την περίπτωση $N = 8$ ($n = 3$ qubit), με μία λύση, έστω τον δείκτη $i = 5$. Εδώ $\theta = 2 \arcsin(1/\sqrt{8}) \approx 0.7227$ rad, οπότε

$$K \approx \frac{\pi}{4} \sqrt{8} - \frac{1}{2} \approx 1.72,$$

δηλαδή στρογγυλοποιούμε σε $K = 2$ επαναλήψεις. Υπολογίζοντας ακριβώς (χωρίς την προσέγγιση μικρής γωνίας) την πιθανότητα $|\langle 5 | \hat{G}^k | \psi \rangle|^2$ μετά από $k = 1, 2$ επαναλήψεις, βρίσκουμε

$$k = 1 : 78.13\%, \quad k = 2 : 94.53\%,$$

δηλαδή ήδη μετά από μόλις 2 κλήσεις του μαντείου (αντί για κατά μέσο όρο 4–5 κλήσεις που θα χρειαζόταν η κλασική γραμμική αναζήτηση σε 8 στοιχεία) η πιθανότητα να μετρήσουμε τη σωστή λύση είναι ήδη πάνω από 94%. Ένα script που επιβεβαιώνει αριθμητικά αυτό το παράδειγμα, χτίζοντας ρητά τους πίνακες $\hat{H}_n, \hat{U}_0, \hat{O}, \hat{G}$ με τη βοήθεια της qulib2.py, βρίσκεται στο αρχείο python/ex_grover_search.py:

```
import functools
import operator as pyop

import numpy as np

from qulib2 import Gate, GateH, QuantumState

np.set_printoptions(precision=4, suppress=True)

n = 3
N = 2 ** n
solution = 5

Hn = functools.reduce(pyop.pow, [GateH()] * n)

O_mat = np.eye(N)
O_mat[solution, solution] = -1
O = Gate(U=O_mat)

U0_mat = -np.eye(N)
U0_mat[0, 0] = 1
U0 = Gate(U=U0_mat)

Gamma = Hn @ U0 @ Hn
G = Gamma @ O

psi = Hn @ QuantumState(n)

theta = 2 * np.arcsin(1 / np.sqrt(N))
K = round(np.pi / 4 * np.sqrt(N) - 0.5)
```

```
print(f"N={N} στοιχεία, μιά λύση (i={solution}), theta={theta:.4f} rad, βέλτιστο K={K}")

state = psi
for k in range(1, K + 1):
    state = G @ state
    prob = abs(state.a[solution]) ** 2
    print(f"μετά από {k} επαναλήψεις: Πμέτρηση( |{solution}>) = {prob:.4f}")
```

Για να εκτιμήσουμε πόσο δραματική είναι η επιτάχυνση καθώς μεγαλώνει το N , ας δούμε ένα μεγαλύτερο παράδειγμα: για $N = 2^{10} = 1024$ στοιχεία με μία λύση, η κλασική γραμμική αναζήτηση χρειάζεται κατά μέσο όρο περίπου 512 ερωτήσεις, ενώ ο αλγόριθμος του Grover χρειάζεται μόνο $K \approx \frac{\pi}{4} \sqrt{1024} - \frac{1}{2} \approx 24.6$, δηλαδή στρογγυλά 25 κλήσεις του μαντείου: περισσότερες από 20 φορές λιγότερες.

Εμβάθυνση 5.1: Είναι βέλτιστος ο αλγόριθμος του Grover;

Θα μπορούσε κανείς να αναρωτηθεί αν υπάρχει κάποιος ακόμα πιο γρήγορος κβαντικός αλγόριθμος για το ίδιο πρόβλημα, που να λύνει την αναζήτηση σε, ας πούμε, $O(\log N)$ ή $O(1)$ κλήσεις του μαντείου. Η απάντηση είναι όχι: οι Bennett, Bernstein, Brassard και Vazirani απέδειξαν το 1997 ότι *κάθε* κβαντικός αλγόριθμος που λύνει το πρόβλημα της μη ταξινομημένης αναζήτησης, χρησιμοποιώντας το μαντείο ως μαύρο κουτί, χρειάζεται τουλάχιστον $\Omega(\sqrt{N})$ κλήσεις (το σύμβολο Ω είναι το «κάτω φράγμα» ανάλογο του O). Ο αλγόριθμος του Grover είναι λοιπόν *βέλτιστος*, μέχρι σταθερό πολλαπλασιαστικό παράγοντα: καμία κβαντική μέθοδος δεν μπορεί να κάνει καλύτερα από τετραγωνική επιτάχυνση για αυτό το πρόβλημα. Δεν θα παρουσιάσουμε εδώ την απόδειξη αυτού του κάτω φράγματος, που είναι αρκετά πιο τεχνική από όσα έχουμε δει μέχρι τώρα.

Συγκεντρώνοντας όλα τα βήματα των ενότητων 5.2–5.5, ο πλήρης αλγόριθμος του Grover είναι ο εξής:

1. Ξεκινάμε από την κατάσταση $|0 \cdots 0\rangle \otimes |0\rangle$ (n qubit-δείκτη, ένα βοηθητικό qubit).
2. Εφαρμόζουμε $\hat{H}_n$ στο qubit-δείκτη και HX στο βοηθητικό qubit, παίρνοντας την κατάσταση $|\psi\rangle \otimes |-\rangle$ (ενότητα 5.4).
3. Επαναλαμβάνουμε $K \approx \frac{\pi}{4} \sqrt{N/M}$ φορές την επανάληψη του Grover $\hat{G} = \hat{\Gamma}\hat{O}$ πάνω στο qubit-δείκτη (ενότητα 5.3), όπου κάθε εφαρμογή του $\hat{O}$ γίνεται μέσω μίας κλήσης του μαντείου $\hat{U}_f$ πάνω στο ζεύγος qubit-δείκτη/βοηθητικό qubit (ενότητα 5.2).
4. Μετράμε το qubit-δείκτη στην υπολογιστική βάση: με πιθανότητα πολύ κοντά στο 1, το αποτέλεσμα είναι ένας δείκτης i με $f(i) = 1$, δηλαδή μία λύση του προβλήματος.

Σύνοψη Ενότητας

Σε αυτό το κεφάλαιο μελετήσαμε τον πρώτο μας κβαντικό αλγόριθμο, τον αλγόριθμο αναζήτησης του Grover. Συνοπτικά:

- Διατυπώσαμε το πρόβλημα της μη ταξινομημένης αναζήτησης μέσω μίας συνάρτησης $f(i) \in \{0, 1\}$, και θυμηθήκαμε ότι κάθε κλασικός αλγόριθμος χρειάζεται $O(N)$ ερωτήσεις στη χειρότερη περίπτωση.
- Ορίσαμε το κβαντικό «μαντείο» $\hat{U}_f |i\rangle |q\rangle = |i\rangle |q \oplus f(i)\rangle$ και δείξαμε, μέσω ανάδρασης φάσης με το βοηθητικό qubit στην κατάσταση $|-\rangle$, ότι ισοδυναμεί με έναν τελεστή φάσης $\hat{O} |i\rangle = (-1)^{f(i)} |i\rangle$ πάνω στο qubit-δείκτη.
- Κατασκευάσαμε τον τελεστή διάχυσης $\hat{\Gamma} = \hat{H}_n \hat{U}_0 \hat{H}_n = 2 |\psi\rangle \langle \psi| - \hat{I}$ και τον τελεστή επανάληψης του Grover $\hat{G} = \hat{\Gamma}\hat{O}$, και δείξαμε γεωμετρικά ότι δρα ως στροφή κατά γωνία θ (με $\sin(\theta/2) = \sqrt{M/N}$) μέσα στο επίπεδο που παράγουν οι καταστάσεις $|\psi_0\rangle, |\psi_1\rangle$ (μη λύσεις/λύσεις).
- Είδαμε πώς κατασκευάζεται η αρχική κατάσταση $|\psi\rangle \otimes |-\rangle$ με τη βοήθεια των $\hat{H}_n$ και HX .
- Ορίσαμε αυστηρά τον συμβολισμό $O(\cdot)$ και υπολογίσαμε τον βέλτιστο αριθμό επαναλήψεων $K \approx$

$\frac{\pi}{4}\sqrt{N/M}$, καταλήγοντας στην τετραγωνική επιτάχυνση $O(\sqrt{N})$ του αλγορίθμου του Grover σε σχέση με την κλασική $O(N)$ πολυπλοκότητα, μία επιτάχυνση που είναι μάλιστα αποδεδειγμένα βέλτιστη.