Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 8η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2026

Περιεχόμενα

1 Αναζήτηση και μαντείο

2 Διάχυση και επανάληψη

3 Κόστος και παραδείγματα

Το πρόβλημα της αναζήτησης

- Έχουμε N στοιχεία $x_0, \ldots, x_{N-1}$ και ψάχνουμε εκείνα που ικανοποιούν μία ιδιότητα. Το πρόβλημα περιγράφεται από μία συνάρτηση στους δείκτες

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

- Το σύνολο είναι *μη ταξινομημένο*: δεν υπάρχει δομή που να μας καθοδηγεί. Μπορούμε μόνο να υπολογίσουμε το $f(i)$ για όποιο i επιλέξουμε
- Μοντέλο *μαύρου κουτιού* (μαντείο): το f είναι δεδομένο και μετράμε το πλήθος των ερωτήσεων στο μαντείο
- Γραμμική αναζήτηση: N ερωτήσεις στη χειρότερη περίπτωση, περίπου $N/2$ κατά μέσο όρο. Κανένας κλασικός αλγόριθμος δεν κάνει καλύτερα από $O(N)$
- Η δυαδική αναζήτηση, $O(\log N)$, χρειάζεται ταξινομημένο σύνολο

Ο συμβολισμός $O(\cdot)$

- Μας ενδιαφέρει πώς μεγαλώνει το κόστος όταν το N γίνεται μεγάλο, όχι οι σταθερές. Ένας αλγόριθμος με $3N$ βήματα και ένας με $100N$ μεγαλώνουν με τον ίδιο τρόπο
- Η $g(N)$ είναι $O(h(N))$ αν υπάρχουν $c > 0$ και N_0 ώστε

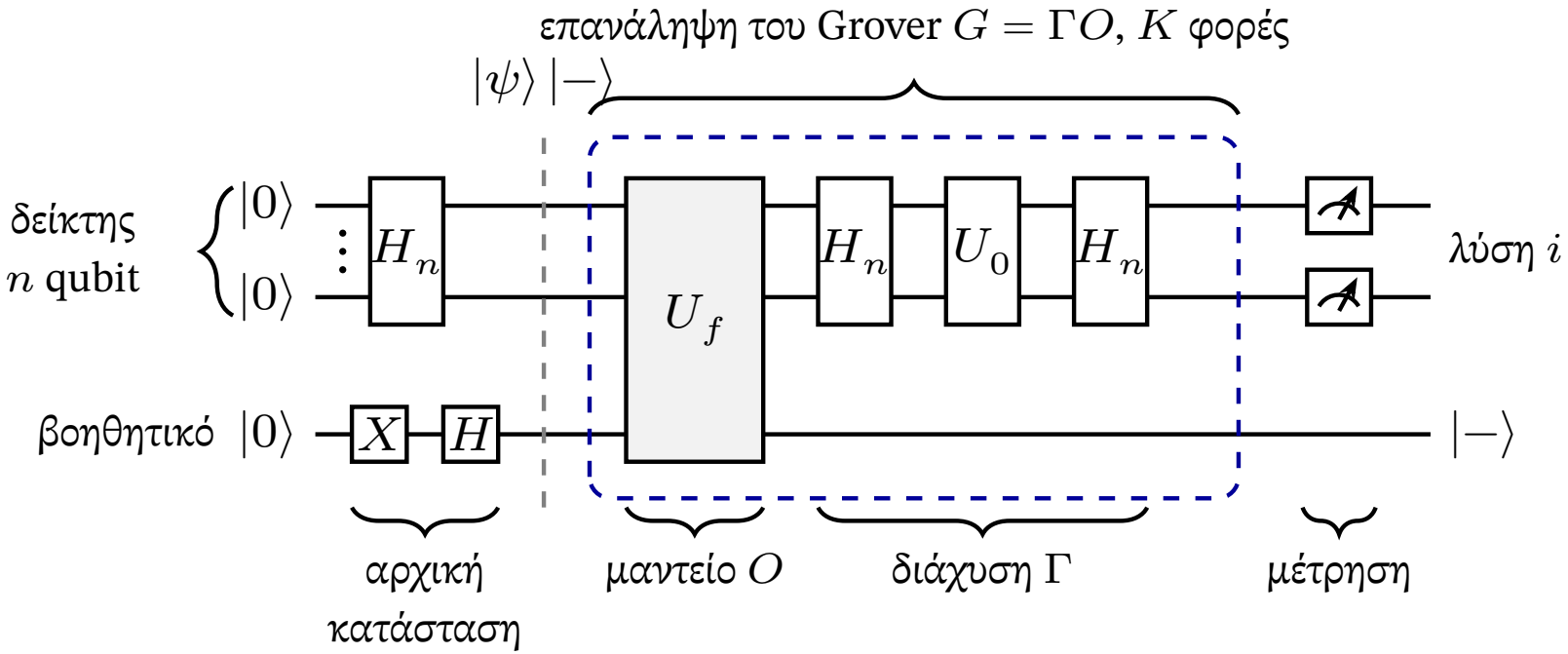
$$|g(N)| \leq c\,|h(N)|, \qquad N \geq N_0$$

- Παράδειγμα: η $g(N) = 3N^2 + 5N + 7$ είναι $O(N^2)$. Για $N \geq 1$ ισχύει $N \leq N^2$ και $1 \leq N^2$, άρα

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

  δηλαδή $c = 15$, $N_0 = 1$
- Δεν είναι $O(N)$: θα έπρεπε $3N \leq c$ για κάθε μεγάλο N, που είναι αδύνατο
- Η γραμμική αναζήτηση είναι $O(N)$

Ο αλγόριθμος του Grover: επισκόπηση



- $N = 2^n$. Αρχική κατάσταση: ομοιόμορφη υπέρθεση όλων των δεικτών. Μετά K φορές η επανάληψη G (μαντείο και διάχυση) και τέλος μέτρηση
- Αποτέλεσμα: $O(\sqrt{N})$ ερωτήσεις στο μαντείο αντί για $O(N)$

Το κβαντικό μαντείο

- Κωδικοποιούμε τον δείκτη με n bit, $i = 2^{n-1}q_1 + \cdots + 2^0 q_n$, και γράφουμε $|i\rangle = |q_1\rangle \otimes \cdots \otimes |q_n\rangle$ (qubit-δείκτης)
- Η απεικόνιση $|i\rangle \to |f(i)\rangle$ δεν είναι αντιστρέψιμη, αφού πολλά i δίνουν το ίδιο $f(i)$
- Όπως στο κβαντικό AND, προσθέτουμε ένα βοηθητικό qubit $|q\rangle$ και ορίζουμε το μαντείο

$$U_f |i\rangle |q\rangle = |i\rangle |q \oplus f(i)\rangle$$

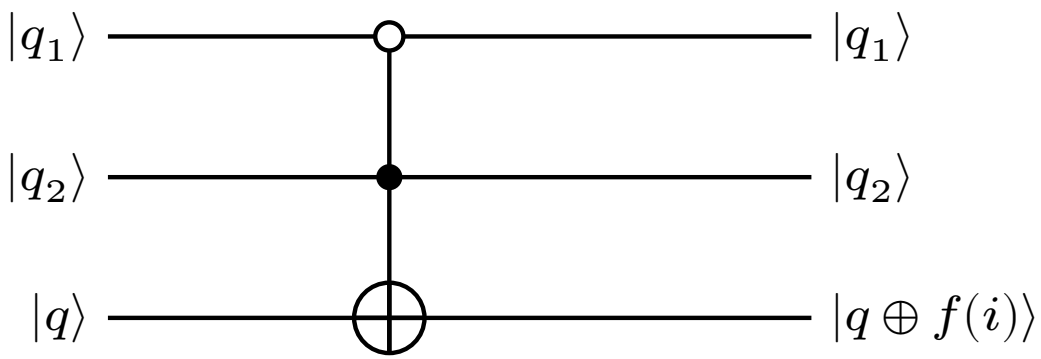
- Το $\oplus$ είναι πρόσθεση modulo 2 (XOR), bit προς bit. Το XOR με j αντιστρέφει όσα bit έχουν 1 στο j. Π.χ. για $n = 2$ και $j = 01$:

$$|00\rangle \to |01\rangle\,,\ |01\rangle \to |00\rangle\,,\ |10\rangle \to |11\rangle\,,\ |11\rangle \to |10\rangle$$

  που υλοποιείται με μία X στο δεύτερο qubit
- Στο μαντείο ο δείκτης δεν αλλάζει, ενώ το βοηθητικό qubit γίνεται $q \oplus f(i)$

Παράδειγμα: μαντείο για $N = 4$, λύση $i = 1$

- $f(1) = 1$ και $f(0) = f(2) = f(3) = 0$. Στα bit, $i = 1$ σημαίνει $q_1 q_2 = 01$
- Θέλουμε X στο βοηθητικό qubit ακριβώς όταν $q_1 = 0$ και $q_2 = 1$: Toffoli με *αρνητικό* έλεγχο στο q_1 (άσπρος κύκλος)



- Ισοδύναμα: μία X στο q_1 πριν, μία Toffoli με δύο κανονικούς ελέγχους, και μία X στο q_1 μετά
- Για μεγαλύτερο n το κύκλωμα έχει την ίδια μορφή, με n ελέγχους, μαύρους ή άσπρους ανάλογα με τα bit του i

Ανάδραση φάσης

- Προετοιμάζουμε το βοηθητικό qubit στην $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Αν $f(i) = 0$ δεν αλλάζει τίποτα: $U_f |i\rangle |-\rangle = |i\rangle |-\rangle$. Αν $f(i) = 1$ το βοηθητικό qubit αντιστρέφεται:

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

- Και στις δύο περιπτώσεις $U_f |i\rangle |-\rangle = (-1)^{f(i)} |i\rangle |-\rangle$
- Το βοηθητικό qubit μένει στο $|-\rangle$ μετά από κάθε κλήση, και η μόνη αλλαγή είναι μία *φάση* στον δείκτη (ανάδραση φάσης, phase kickback)

Ο τελεστής φάσης του μαντείου

Μπορούμε να ξεχάσουμε το βοηθητικό qubit και να δουλεύουμε με τον O που δρα μόνο στον δείκτη:

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

Ο O αλλάζει το πρόσημο ακριβώς των λύσεων

Ο O για το παράδειγμα $N = 4$

- Για λύση το $i = 1$:

$$O\left|00\right\rangle = +\left|00\right\rangle,\ O\left|01\right\rangle = -\left|01\right\rangle,\ O\left|10\right\rangle = +\left|10\right\rangle,\ O\left|11\right\rangle = +\left|11\right\rangle$$

- Ο O δεν ανακατεύει τις καταστάσεις βάσης, άρα ο πίνακάς του είναι διαγώνιος με στοιχεία $(-1)^{f(i)}$:

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

Ο μετασχηματισμός H_n

- Ο $H_n = H \otimes \cdots \otimes H$ (n φορές) είναι μία Hadamard σε κάθε qubit του δείκτη
- Για $n = 2$, με βάση $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

$$\mathbf{H}_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

- Στην $|0 \cdots 0\rangle$ δίνει την ομοιόμορφη υπέρθεση: κάθε $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ και το γινόμενο περιέχει κάθε ακολουθία n bit με συντελεστή $+1$

$$|\psi\rangle = H_n |0 \cdots 0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

- Επειδή $H^2 = I$ και $\mathbf{H}^{\mathrm{T}} = \mathbf{H}$, ισχύει

$$H_n^2 = I, \qquad H_n^{\mathrm{T}} = H_n$$

Η επιλεκτική αλλαγή φάσης U_0

- Ο U_0 αφήνει την $|0\cdots 0\rangle$ ως έχει και αλλάζει το πρόσημο όλων των άλλων καταστάσεων βάσης:

$$U_0 |b\rangle = \begin{cases} |0\rangle, & b = 0 \\ -|b\rangle, & b \neq 0 \end{cases}$$

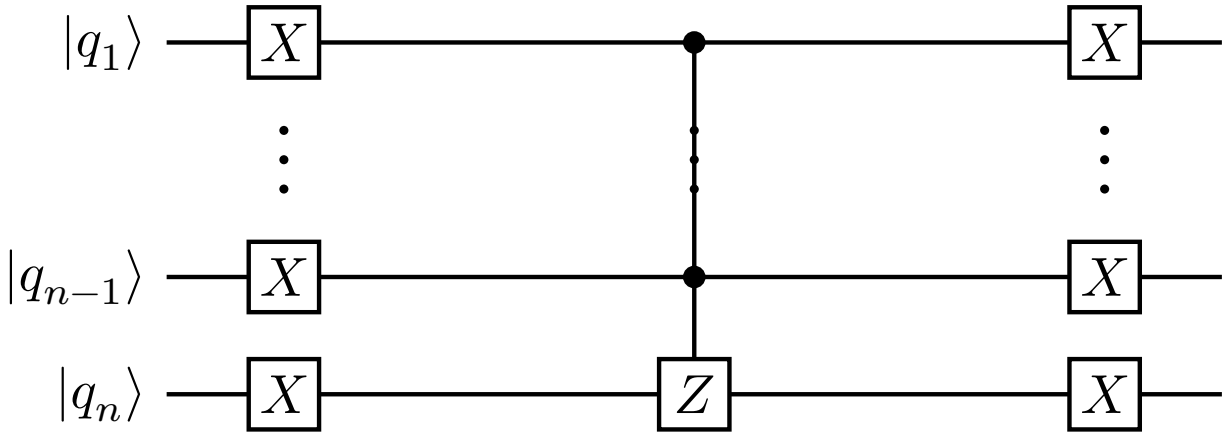
- Για $n = 2$ είναι διαγώνιος:

$$\mathbf{U}_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = 2|0\rangle\langle 0| - \mathbf{I}$$

- Η σχέση $U_0 = 2|0\rangle\langle 0| - I$ ισχύει για κάθε n: για $|0\rangle$ δίνει $2|0\rangle - |0\rangle = |0\rangle$ και για $b \neq 0$ δίνει $-|b\rangle$, αφού $\langle 0|b\rangle = 0$

Το κύκλωμα του U_0

- Η $C_{n-1}(Z)$ αλλάζει το πρόσημο μόνο της $|1\cdots 1\rangle$. Για να το κάνουμε στην $|0\cdots 0\rangle$, βάζουμε X σε κάθε qubit πριν και μετά



- Το κύκλωμα υλοποιεί τον $I - 2|0\rangle\langle 0| = -U_0$, δηλαδή τον U_0 με καθολική φάση -1, που δεν έχει φυσική συνέπεια

Ο τελεστής διάχυσης

- Ορίζουμε $\Gamma = H_n U_0 H_n$. Θα δείξουμε ότι

$$\Gamma = 2 |\psi\rangle \langle\psi| - I$$

- Με $U_0 = 2 |0\rangle \langle 0| - I$ και $H_n^2 = I$:

$$\Gamma = 2H_n |0\rangle \langle 0| H_n - H_n H_n = 2H_n |0\rangle \langle 0| H_n - I$$

- Ισχύει $H_n |0\rangle = |\psi\rangle$, και από τη συμμετρία $H_n^{\mathrm{T}} = H_n$ είναι $\langle 0| H_n = \langle\psi|$. Άρα

$$\Gamma = 2 |\psi\rangle \langle\psi| - I$$

- Σε τυχαία κατάσταση $|\omega\rangle$:

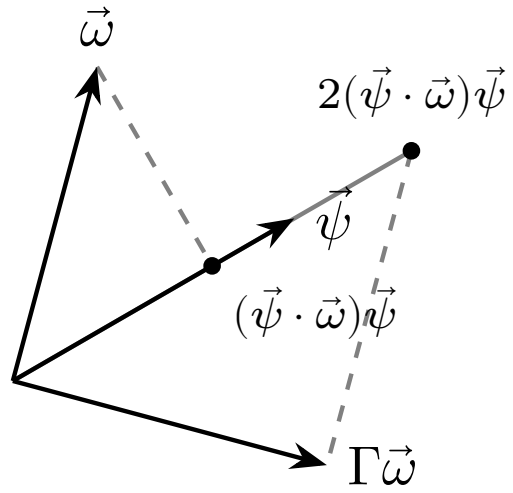
$$\Gamma |\omega\rangle = 2 |\psi\rangle \langle\psi|\omega\rangle - |\omega\rangle$$

Ο Γ είναι ανάκλαση

- Αναλύουμε $|\phi\rangle = \langle\psi|\phi\rangle\,|\psi\rangle + |\omega\rangle$, με $\langle\psi|\omega\rangle = 0$
- $\Gamma\,|\psi\rangle = |\psi\rangle$ και $\Gamma\,|\omega\rangle = -\,|\omega\rangle$, άρα

$$\Gamma\,|\phi\rangle = \langle\psi|\phi\rangle\,|\psi\rangle - |\omega\rangle$$

- Κρατά το κομμάτι πάνω στην $|\psi\rangle$ και αντιστρέφει το κάθετο: ανάκλαση ως προς την ευθεία της $|\psi\rangle$. Διατηρεί το μέτρο



Ο Γ για $n = 2$ και η ανάκλαση γύρω από τον μέσο όρο

- Με $|\psi\rangle = \frac{1}{2}(1,1,1,1)^{\mathrm{T}}$ ο $2|\psi\rangle\langle\psi| - \mathbf{I}$ δίνει (όπως και ο $\mathbf{H}_2\mathbf{U}_0\mathbf{H}_2$)

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

- Αν μ ο μέσος όρος των πλατών a_i μιας κατάστασης, τότε Γ αντικαθιστά κάθε a_i με $2\mu - a_i$: αναστρέφει τα πλάτη γύρω από τον μέσο όρο

Ο τελεστής διάχυσης

$\Gamma = H_n U_0 H_n = 2|\psi\rangle\langle\psi| - I$ είναι ανάκλαση ως προς την ομοιόμορφη υπέρθεση $|\psi\rangle$

Ο χώρος αναζήτησης

- Η επανάληψη του Grover είναι $G = \Gamma O$. Χωρίζουμε τους δείκτες σε λύσεις $S_1 = \{i : f(i) = 1\}$ (M στοιχεία) και μη λύσεις $S_0 = \{i : f(i) = 0\}$ ($N - M$ στοιχεία)
- Ορίζουμε

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

- Είναι κανονικοποιημένες, $\langle \psi_1 | \psi_1 \rangle = \frac{1}{M} \cdot M = 1$, και ορθογώνιες, $\langle \psi_0 | \psi_1 \rangle = 0$, αφού τα S_0, S_1 δεν έχουν κοινά στοιχεία
- Για το παράδειγμα $N = 4$, $M = 1$:

$$|\psi_1\rangle = |01\rangle \,, \qquad |\psi_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle)$$

Η αρχική κατάσταση στο επίπεδο

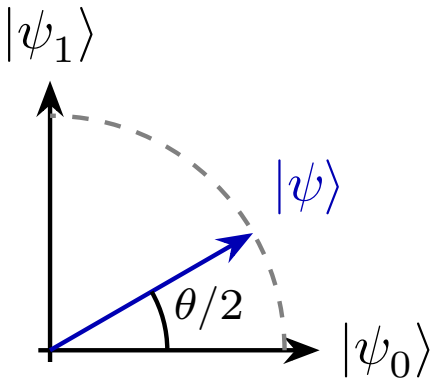
- Χωρίζοντας το άθροισμα της $|\psi\rangle$ στα S_0 και S_1:

$$|\psi\rangle = \sqrt{\tfrac{N-M}{N}}\,|\psi_0\rangle + \sqrt{\tfrac{M}{N}}\,|\psi_1\rangle$$

- Ορίζουμε γωνία θ με $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$, οπότε

$$|\psi\rangle = \cos\tfrac{\theta}{2}\,|\psi_0\rangle + \sin\tfrac{\theta}{2}\,|\psi_1\rangle$$

- Για $M \ll N$ η $|\psi\rangle$ είναι μακριά από τις λύσεις
- Παράδειγμα $N = 4$, $M = 1$: $\theta = \frac{\pi}{3}$ και $|\psi\rangle = \frac{\sqrt{3}}{2}\,|\psi_0\rangle + \frac{1}{2}\,|\psi_1\rangle$



Οι O και Γ μένουν στο επίπεδο

- Το μαντείο αφήνει τις μη λύσεις και αλλάζει το πρόσημο των λύσεων:

$$O\left|\psi_0\right\rangle = \left|\psi_0\right\rangle, \qquad O\left|\psi_1\right\rangle = -\left|\psi_1\right\rangle$$

Άρα για $\left|\phi\right\rangle = \alpha\left|\psi_0\right\rangle + \beta\left|\psi_1\right\rangle$ είναι $O\left|\phi\right\rangle = \alpha\left|\psi_0\right\rangle - \beta\left|\psi_1\right\rangle$: ανάκλαση ως προς τον άξονα $\left|\psi_0\right\rangle$

- Με $c = \cos\frac{\theta}{2}$, $s = \sin\frac{\theta}{2}$ έχουμε $\langle\psi|\phi\rangle = c\alpha + s\beta$ και

$$\Gamma\left|\phi\right\rangle = \left[(2c^2-1)\alpha + 2cs\,\beta\right]\left|\psi_0\right\rangle + \left[2cs\,\alpha + (2s^2-1)\beta\right]\left|\psi_1\right\rangle$$

που είναι πάλι συνδυασμός των $\left|\psi_0\right\rangle, \left|\psi_1\right\rangle$ (ανάκλαση ως προς την $\left|\psi\right\rangle$)

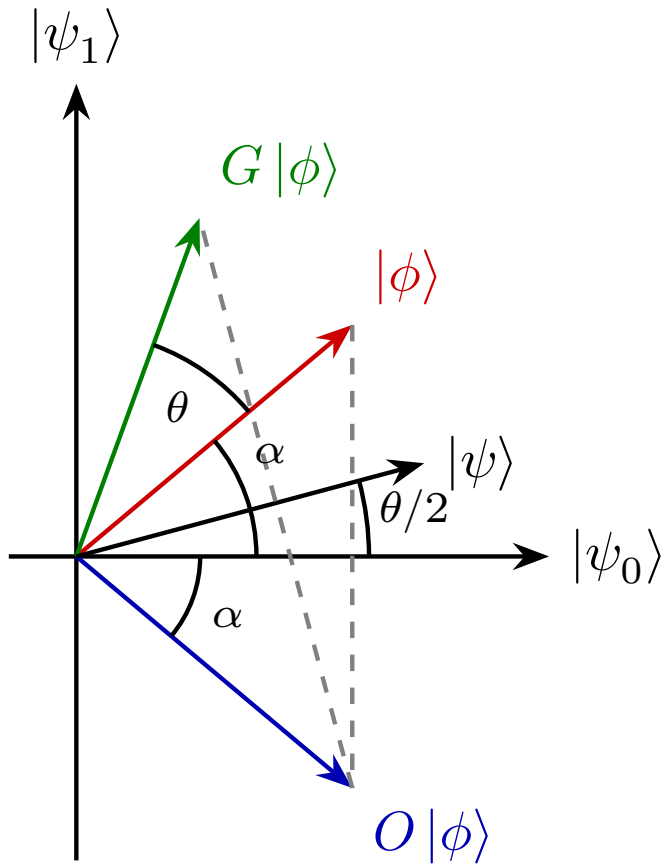
- Άρα και ο $G = \Gamma O$ απεικονίζει το επίπεδο στον εαυτό του: μπορούμε να αγνοήσουμε τις άλλες $N-2$ διαστάσεις

Δύο ανακλάσεις κάνουν στροφή

- Έστω $|\phi\rangle$ σε γωνία α από τον $|\psi_0\rangle$
- Ο O την στέλνει σε γωνία $-\alpha$
- Η $|\psi\rangle$ είναι σε γωνία $\theta/2$, και το $O|\phi\rangle$ απέχει από αυτήν $\theta/2+\alpha$. Ο Γ το στέλνει στην άλλη πλευρά, σε γωνία

$$\frac{\theta}{2}+\left(\frac{\theta}{2}+\alpha\right)=\alpha+\theta$$

- Ο G στρέφει κάθε κατάσταση κατά θ προς το $|\psi_1\rangle$



Οι πίνακες στο επίπεδο

- Με βάση $|\psi_0\rangle, |\psi_1\rangle$ και τις ταυτότητες $2c^2 - 1 = \cos\theta$, $2s^2 - 1 = -\cos\theta$, $2cs = \sin\theta$:

$$\Gamma = 2\begin{bmatrix} c^2 & cs \\ cs & s^2 \end{bmatrix} - \mathbf{I} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}, \qquad \mathbf{O} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

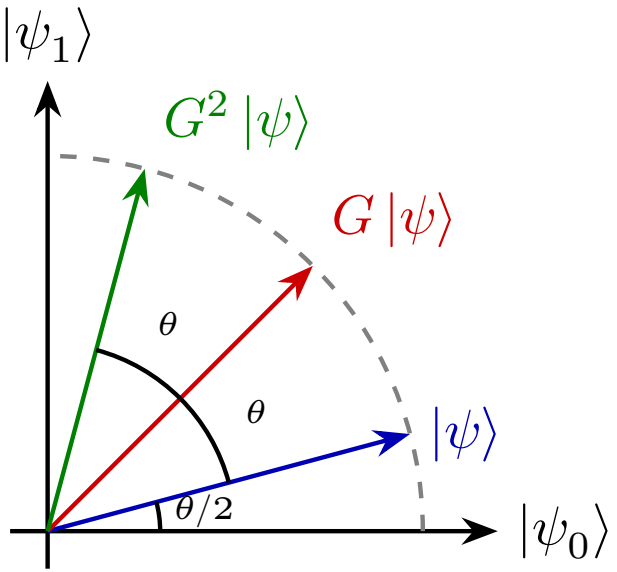
- Ο πίνακας της επανάληψης είναι το γινόμενο $\mathbf{G} = \Gamma\mathbf{O}$ (πρώτα O, μετά Γ):

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

- Είναι ο πίνακας στροφής κατά θ: στο διάνυσμα $(r\cos\varphi, r\sin\varphi)$ δίνει $(r\cos(\varphi+\theta), r\sin(\varphi+\theta))$

Μετά από k επαναλήψεις

- Η αρχική γωνία είναι $\theta/2$ και κάθε επανάληψη προσθέτει θ
- Μετά από k επαναλήψεις η γωνία είναι $\frac{(2k+1)\theta}{2}$
- Το πλάτος του $|\psi_1\rangle$ αυξάνει σε κάθε επανάληψη, όσο η γωνία δεν ξεπερνά το $\pi/2$



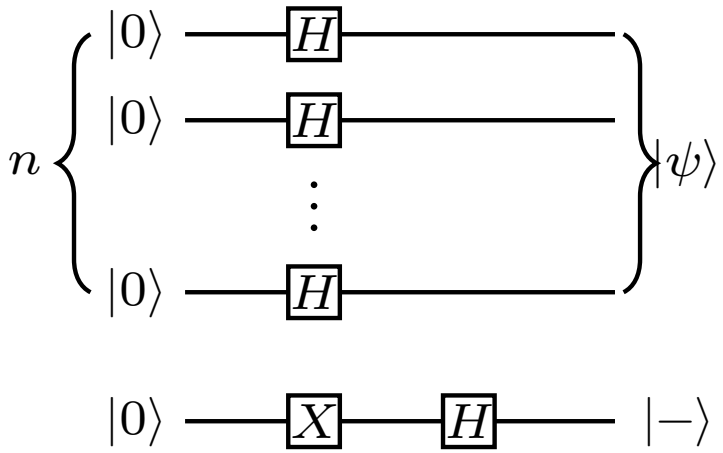
$$G^k|\psi\rangle = \cos\tfrac{(2k+1)\theta}{2}|\psi_0\rangle + \sin\tfrac{(2k+1)\theta}{2}|\psi_1\rangle$$

Η επανάληψη του Grover

Ο $G = \Gamma O$ είναι στροφή κατά θ προς τις λύσεις μέσα στο επίπεδο των $|\psi_0\rangle, |\psi_1\rangle$

Αρχική κατάσταση και βήματα

1. n qubit δείκτη στην $|0\cdots 0\rangle$ και ένα βοηθητικό στην $|0\rangle$
2. H_n στον δείκτη, και X, H στο βοηθητικό: παίρνουμε $|\psi\rangle\,|-\rangle$
3. K φορές $G = \Gamma O$: μία κλήση του μαντείου και η διάχυση. Το βοηθητικό qubit μένει στο $|-\rangle$
4. Μέτρηση του δείκτη: λύση με πιθανότητα $\sin^2 \frac{(2K+1)\theta}{2}$



Πόσες επαναλήψεις χρειάζονται

- Θέλουμε $\sin\frac{(2K+1)\theta}{2} \approx 1$, δηλαδή $\frac{(2K+1)\theta}{2} = \frac{\pi}{2}$, άρα

$$K = \frac{\pi}{2\theta} - \frac{1}{2}$$

- Για $M \ll N$ η γωνία $\theta/2$ είναι μικρή και $\sin x \approx x$. Άρα

$$\frac{\theta}{2} \approx \sqrt{\frac{M}{N}}, \qquad \theta \approx 2\sqrt{\frac{M}{N}}$$

- Αντικαθιστώντας και αγνοώντας το $\frac{1}{2}$ (αμελητέο για μεγάλο N):

Πολυπλοκότητα του Grover

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

Για μία λύση, $K \approx \frac{\pi}{4}\sqrt{N} = O(\sqrt{N})$ κλήσεις του μαντείου, δηλαδή τετραγωνική επιτάχυνση σε σχέση με το κλασικό $O(N)$

Παράδειγμα: αναζήτηση σε $N = 1024$ στοιχεία

- $M = 1$. Η κλασική γραμμική αναζήτηση χρειάζεται κατά μέσο όρο περίπου 512 ερωτήσεις
- Για τον Grover: $\sin \frac{\theta}{2} = \frac{1}{32}$, άρα $\theta \approx \frac{1}{16}$ και

$$K \approx \frac{\pi}{2\theta} - \frac{1}{2} = 8\pi - \frac{1}{2} \approx 24.6$$

- Παίρνουμε $K = 25$, και η πιθανότητα επιτυχίας είναι

$$\sin^2 \frac{51\,\theta}{2} \approx 0.9995$$

- Μόνο 25 κλήσεις του μαντείου αντί για περίπου 512: πάνω από 20 φορές λιγότερες

Βέλτιστος αλγόριθμος

Κάθε κβαντικός αλγόριθμος για μη ταξινομημένη αναζήτηση με μαντείο χρειάζεται $\Omega(\sqrt{N})$ κλήσεις (Bennett, Bernstein, Brassard, Vazirani, 1997). Ο Grover είναι βέλτιστος, μέχρι σταθερά

Παράδειγμα $N = 4$: μία επανάληψη

- Λύση ο $i = 1$. Αρχικά $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- Το μαντείο αλλάζει το πρόσημο της λύσης:

$$O|\psi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

- Τα πλάτη είναι $a_0 = a_2 = a_3 = \frac{1}{2}$, $a_1 = -\frac{1}{2}$, με μέσο όρο $\mu = \frac{1}{4}$ και $2\mu = \frac{1}{2}$
- Ο Γ αντικαθιστά $a_i \to 2\mu - a_i$:

$$a_0 = a_2 = a_3 \to \frac{1}{2} - \frac{1}{2} = 0, \qquad a_1 \to \frac{1}{2} + \frac{1}{2} = 1$$

- Άρα

$$G|\psi\rangle = |01\rangle$$

και η λύση βρίσκεται με πιθανότητα 1 με μία κλήση του μαντείου (κλασικά: 2 με 3 ερωτήσεις κατά μέσο όρο)

Παράδειγμα $N = 4$: η γεωμετρία

- $\theta = \frac{\pi}{3}$. Μετά από $k = 1$ επανάληψη η γωνία είναι

$$\frac{2k+1}{2}\theta = \frac{3}{2} \cdot \frac{\pi}{3} = \frac{\pi}{2}$$

  δηλαδή η κατάσταση έχει στραφεί ακριβώς πάνω στο $|\psi_1\rangle$

- Αν κάναμε και δεύτερη επανάληψη ($k = 2$), η γωνία θα ήταν $\frac{5}{2} \cdot \frac{\pi}{3} = \frac{5\pi}{6}$ και η πιθανότητα

$$\sin^2 \frac{5\pi}{6} = \frac{1}{4}$$

- Περισσότερες επαναλήψεις δεν σημαίνουν καλύτερο αποτέλεσμα: η κατάσταση περνά πάνω από το $|\psi_1\rangle$ και η πιθανότητα μειώνεται. Πρέπει να σταματήσουμε στη σωστή στιγμή

Παράδειγμα $N = 8$: λύση ο $i = 5$

- $\sin \frac{\theta}{2} = \sqrt{\frac{1}{8}}$, άρα $\theta = 2 \arcsin \frac{1}{\sqrt{8}} \approx 0.7227$ rad
- Αριθμός επαναλήψεων: $K \approx \frac{\pi}{4}\sqrt{8} - \frac{1}{2} \approx 1.72$, άρα $K = 2$
- Πιθανότητα επιτυχίας $\sin^2 \frac{(2k+1)\theta}{2}$:

k	1	2	3
πιθανότητα	0.7813	0.9453	0.33

- Με 2 κλήσεις του μαντείου βρίσκουμε τη λύση με πιθανότητα 94.53%. Κλασικά χρειάζονται κατά μέσο όρο 4 με 5 κλήσεις
- Για $k = 3$ η γωνία $\frac{7\theta}{2} \approx 2.53$ ξεπερνά το $\frac{\pi}{2} \approx 1.57$ και η πιθανότητα πέφτει στο 0.33

Σύνοψη

- Μη ταξινομημένη αναζήτηση με συνάρτηση $f(i) \in \{0, 1\}$: κλασικά $O(N)$ ερωτήσεις
- Μαντείο U_f. Με το βοηθητικό qubit στο $|-\rangle$ δρα στον δείκτη ως $O|i\rangle = (-1)^{f(i)}|i\rangle$
- Διάχυση $\Gamma = H_n U_0 H_n = 2|\psi\rangle\langle\psi| - I$: ανάκλαση ως προς την ομοιόμορφη υπέρθεση
- Επανάληψη $G = \Gamma O$: στροφή κατά θ, με $\sin\frac{\theta}{2} = \sqrt{M/N}$, προς το $|\psi_1\rangle$ στο επίπεδο λύσεων-μη λύσεων
- Αλγόριθμος: $|\psi\rangle|-\rangle$, $K \approx \frac{\pi}{4}\sqrt{N/M}$ επαναλήψεις του G, μέτρηση του δείκτη
- $O(\sqrt{N})$ κλήσεις του μαντείου, τετραγωνική επιτάχυνση, αποδεδειγμένα βέλτιστη
- Περισσότερες επαναλήψεις από το K δεν βοηθούν, όπως φάνηκε στα παραδείγματα $N = 4$ και $N = 8$