Κβαντικοί Υπολογιστές και Αλγόριθμοι

Διάλεξη 9η

Θωμάς Καμαλάκης

Χαροκόπειο Πανεπιστήμιο Αθηνών

2026

Περιεχόμενα

1. Πολυπλοκότητα και παραγοντοποίηση
2. Θεωρία αριθμών και επισκόπηση του Shor
3. Ο QFT και η εκτίμηση φάσης
4. Εύρεση της τάξης και ο αλγόριθμος του Shor

Τι κερδίζουμε με τον Grover

- Αν κάθε υποψήφια λύση παριστάνεται με L qubit, τότε $N = 2^L$
- Ο Grover χρειάζεται
$$\sqrt{N} = 2^{L/2}$$
κλήσεις του μαντείου, αντί για $N = 2^L$ της κλασικής αναζήτησης
- Το πλήθος των κλήσεων παραμένει εκθετικό ως προς το L: απλώς ο εκθέτης είναι μικρότερος
- Υπάρχουν προβλήματα όπου η κβαντική επιτάχυνση είναι πολύ μεγαλύτερη; Ναι, και το πιο γνωστό παράδειγμα είναι ο *αλγόριθμος του Shor* (1994)
- Λύνει το πρόβλημα της *παραγοντοποίησης*: δίνεται ένας φυσικός αριθμός n και ζητάμε να τον γράψουμε ως γινόμενο πρώτων αριθμών

Μέγεθος εισόδου και αποδοτικός αλγόριθμος

- Ως μέγεθος της εισόδου δεν παίρνουμε τον αριθμό n, αλλά το πλήθος L των δυαδικών ψηφίων του
- Ο n έχει L ψηφία όταν

$$2^{L-1} \leq n < 2^L$$

- Ένας αλγόριθμος λέγεται *αποδοτικός* όταν ο χρόνος του είναι πολυώνυμο του L, όπως $O(L^3)$
- Ένας αλγόριθμος που κάνει n βήματα είναι *εκθετικός* ως προς το L, γιατί

$$n \geq 2^{L-1}$$

και κάθε επιπλέον bit διπλασιάζει τον χρόνο

Προβλήματα απόφασης

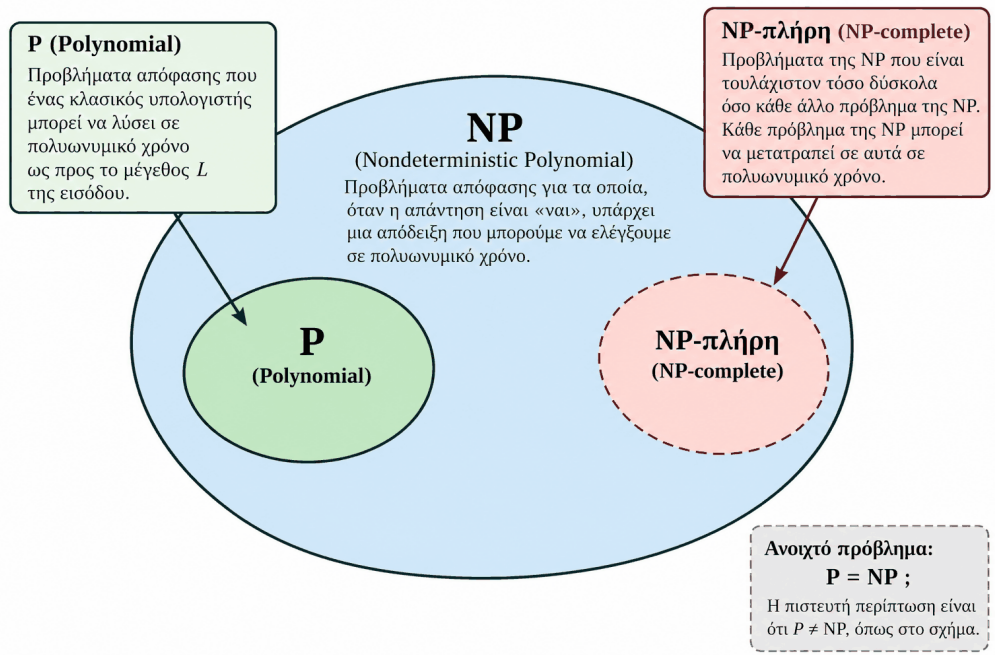
- Οι κλάσεις πολυπλοκότητας αφορούν *προβλήματα απόφασης*: ερωτήματα με απάντηση «ναι» ή «όχι»
- Η παραγοντοποίηση γίνεται πρόβλημα απόφασης αν ρωτήσουμε: «έχει ο n έναν παράγοντα μικρότερο από k;»
- Με επαναλαμβανόμενες ερωτήσεις αυτού του τύπου μπορούμε να βρούμε και τους ίδιους τους παράγοντες

Οι κλάσεις P και NP

- Η κλάση *P* (polynomial) περιέχει τα προβλήματα απόφασης που λύνονται από κλασικό υπολογιστή σε πολυωνυμικό χρόνο ως προς το L. Παράδειγμα: ο έλεγχος αν ένας αριθμός είναι πρώτος (αλγόριθμος AKS, 2002)
- Η κλάση *NP* (nondeterministic polynomial) περιέχει τα προβλήματα απόφασης για τα οποία, όταν η απάντηση είναι «ναι», υπάρχει απόδειξη που ελέγχεται σε πολυωνυμικό χρόνο
- Το «NP» δεν σημαίνει «όχι πολυωνυμικό»
- Για την παραγοντοποίηση η απόδειξη είναι ο παράγοντας d: με μία διαίρεση ελέγχουμε αν διαιρεί τον n. Η εύρεσή του είναι δύσκολη, ο έλεγχός του εύκολος
- Κάθε πρόβλημα της P ανήκει στην NP. Το αν ισχύει και το αντίστροφο, δηλαδή αν $\mathrm{P} = \mathrm{NP}$, είναι το πιο γνωστό ανοιχτό πρόβλημα της πληροφορικής

NP-πλήρη προβλήματα

- Ένα πρόβλημα είναι *NP-πλήρες* όταν ανήκει στην NP και κάθε πρόβλημα της NP μετατρέπεται σε αυτό σε πολυωνυμικό χρόνο
- Πολυωνυμικός αλγόριθμος για ένα NP-πλήρες πρόβλημα θα έλυνε όλη την NP. Παράδειγμα: το SAT
- Η παραγοντοποίηση ανήκει στην NP. Πιστεύεται ότι δεν είναι ούτε στην P ούτε NP-πλήρης
- Ο Shor δείχνει ότι κβαντικά είναι εύκολη



Κλασικοί αλγόριθμοι παραγοντοποίησης

- *Διαίρεση δοκιμής*: δοκιμάζουμε τους πρώτους $2, 3, 5, \ldots$ μέχρι το $\sqrt{n}$. Στη χειρότερη περίπτωση χρειάζονται περίπου $\sqrt{n} = 2^{L/2}$ διαιρέσεις
- Η μέθοδος ρ του Pollard χρειάζεται περίπου $n^{1/4} = 2^{L/4}$, πάλι εκθετικός χρόνος
- Ο καλύτερος γνωστός αλγόριθμος είναι ο *general number field sieve* (GNFS), με χρόνο

$$\exp\left(c\, L^{1/3} (\log L)^{2/3}\right)$$

που είναι υποεκθετικός, αλλά όχι πολυωνυμικός

Αλγόριθμος	Χρόνος	Χαρακτηρισμός
Διαίρεση δοκιμής	$O(2^{L/2})$	εκθετικός
Μέθοδος ρ του Pollard	$O(2^{L/4})$	εκθετικός
GNFS	$\exp\left(O(L^{1/3}(\log L)^{2/3})\right)$	υποεκθετικός
Shor (κβαντικός)	$O(L^3)$	πολυωνυμικός

Η ηλικία του σύμπαντος δεν αρκεί

- Αριθμός RSA-2048: $n \approx 2^{2048}$. Η διαίρεση δοκιμής χρειάζεται έως

$$\sqrt{n} = 2^{1024} \approx 1{,}8 \cdot 10^{308}$$

διαιρέσεις

- Με 10^9 διαιρέσεις το δευτερόλεπτο ο χρόνος είναι

$$1{,}8 \cdot 10^{299}\ \text{s} \approx 5{,}7 \cdot 10^{291}\ \text{χρόνια}$$

- Η ηλικία του σύμπαντος είναι περίπου $1{,}4 \cdot 10^{10}$ χρόνια. Χρειαζόμαστε περίπου 10^{281} φορές την ηλικία του σύμπαντος
- Ο μεγαλύτερος αριθμός που έχει παραγοντοποιηθεί, ο RSA-250 με 829 δυαδικά ψηφία, έπεσε το 2020 με περίπου 2.700 πυρήνα-έτη υπολογισμών

Γιατί μας ενδιαφέρει: το RSA

- Το *RSA* (Rivest, Shamir, Adleman, 1977) είναι το πιο διαδεδομένο σύστημα κρυπτογράφησης δημόσιου κλειδιού
- Χρησιμοποιείται στο HTTPS, στα ψηφιακά πιστοποιητικά, στις ψηφιακές υπογραφές, στο SSH και στο ηλεκτρονικό ταχυδρομείο
- Ο παραλήπτης επιλέγει δύο μεγάλους μυστικούς πρώτους p, q και δημοσιεύει το $n = pq$ ως δημόσιο κλειδί
- Ο αποστολέας κρυπτογραφεί με το n. Ο παραλήπτης αποκρυπτογραφεί γιατί ξέρει τα p, q
- Όποιος παρακολουθεί το κανάλι βλέπει μόνο το n και το κρυπτογραφημένο μήνυμα. Για να διαβάσει το μήνυμα φαίνεται να χρειάζεται την παραγοντοποίηση του n
- Ο έλεγχος αν ένας αριθμός είναι πρώτος είναι εύκολος (Miller–Rabin, AKS), η παραγοντοποίηση δύσκολη. Αυτή η ασυμμετρία είναι η καρδιά του RSA

Απειλή

Ένας κβαντικός υπολογιστής που εκτελεί τον αλγόριθμο του Shor θα έσπαγε την ασφάλεια του RSA

Διαιρετότητα και πρώτοι αριθμοί

- Το $a \neq 0$ *διαιρεί* το b, και γράφουμε $a \mid b$, όταν $b = k \cdot a$ για κάποιον ακέραιο k. Για παράδειγμα $3 \mid 21$, ενώ $4 \nmid 21$
- Ένας ακέραιος $p \geq 2$ είναι *πρώτος* όταν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο εαυτός του. Ένας ακέραιος $n \geq 2$ που δεν είναι πρώτος είναι *σύνθετος*
- Κάθε $n \geq 2$ γράφεται με μοναδικό τρόπο ως γινόμενο δυνάμεων πρώτων. Για παράδειγμα $21 = 3 \cdot 7$
- Ο *μέγιστος κοινός διαιρέτης* $\gcd(a, b)$ είναι ο μεγαλύτερος ακέραιος που διαιρεί και το a και το b. Τα a, b είναι *σχετικά πρώτα* όταν $\gcd(a, b) = 1$
- Παραδείγματα: $\gcd(6, 21) = 3$, $\gcd(4, 21) = 1$

Πράξεις modulo n και αλγόριθμος του Ευκλείδη

- Το $\mathrm{mod}(a, n)$ είναι το υπόλοιπο της διαίρεσης του a με το n
- Οι x, y είναι ίσοι modulo n, και γράφουμε $x = y \bmod n$, όταν $\mathrm{mod}(x, n) = \mathrm{mod}(y, n)$, δηλαδή όταν το n διαιρεί τη διαφορά $x - y$
- Οι πράξεις modulo n γίνονται σε πολυωνυμικό χρόνο ως προς το L
- Ο *αλγόριθμος του Ευκλείδη* υπολογίζει τον μέγιστο κοινό διαιρέτη με τη σχέση

$$\gcd(a, b) = \gcd(b, \mathrm{mod}(a, b))$$

σε $O(L)$ βήματα

- Ο $\gcd(a, b)$ γράφεται ως $au + bv$ με ακέραιους u, v
- Αν $\gcd(a, b) = 1$ και $b \mid ac$, τότε $b \mid c$. Αν $\gcd(x, n) = 1$, το x έχει *αντίστροφο* modulo n

Η συνάρτηση και το θεώρημα του Euler

- Οι αριθμοί από το 1 έως το $n-1$ που είναι σχετικά πρώτοι με το n σχηματίζουν το σύνολο $\mathbb{Z}_n^*$, με $\phi(n)$ στοιχεία
- Για $n = pq$, με p, q πρώτους,

$$\phi(n) = (p-1)(q-1)$$

  Για παράδειγμα $\phi(21) = 12$
- *Θεώρημα του Euler*: για κάθε x με $\gcd(x, n) = 1$ ισχύει

$$\mathrm{mod}(x^{\phi(n)}, n) = 1$$

- Το κινέζικο θεώρημα υπολοίπων: αν $\gcd(m_1, m_2) = 1$ και $n = m_1 m_2$, η απεικόνιση $x \mapsto (\mathrm{mod}(x, m_1), \mathrm{mod}(x, m_2))$ είναι ένα προς ένα, και αντιστοιχίζει το $\mathbb{Z}_n^*$ στα ζεύγη από $\mathbb{Z}_{m_1}^*$ και $\mathbb{Z}_{m_2}^*$

Η τάξη

- Η *τάξη* r του x modulo n είναι ο μικρότερος θετικός ακέραιος με

$$\mathrm{mod}(x^r, n) = 1$$

- Αν $\mathrm{mod}(x^s, n) = 1$, τότε $r \mid s$. Ειδικότερα $r \mid \phi(n)$
- Παράδειγμα: η τάξη του 2 modulo 21 είναι $r = 6$, που διαιρεί το $\phi(21) = 12$
- Για κάθε πρώτο p το $\mathbb{Z}_p^*$ έχει *γεννήτορα* g: κάθε στοιχείο του γράφεται ως $\mathrm{mod}(g^k, p)$ με μοναδικό k από το 1 έως το $p - 1$
- Δεν είναι γνωστός κλασικός αλγόριθμος που να βρίσκει την τάξη σε πολυωνυμικό χρόνο. Αυτό το βήμα θα το αναλάβει ο κβαντικός υπολογιστής

Από την τάξη στους παράγοντες

- Αν $\mathrm{mod}(w^2, n) = 1$ και $1 < w < n - 1$, το w είναι *μη τετριμμένη ρίζα της μονάδας*, και οι $\gcd(w - 1, n)$, $\gcd(w + 1, n)$ είναι παράγοντες του n
- Αν η τάξη r του x είναι άρτια, ο αριθμός

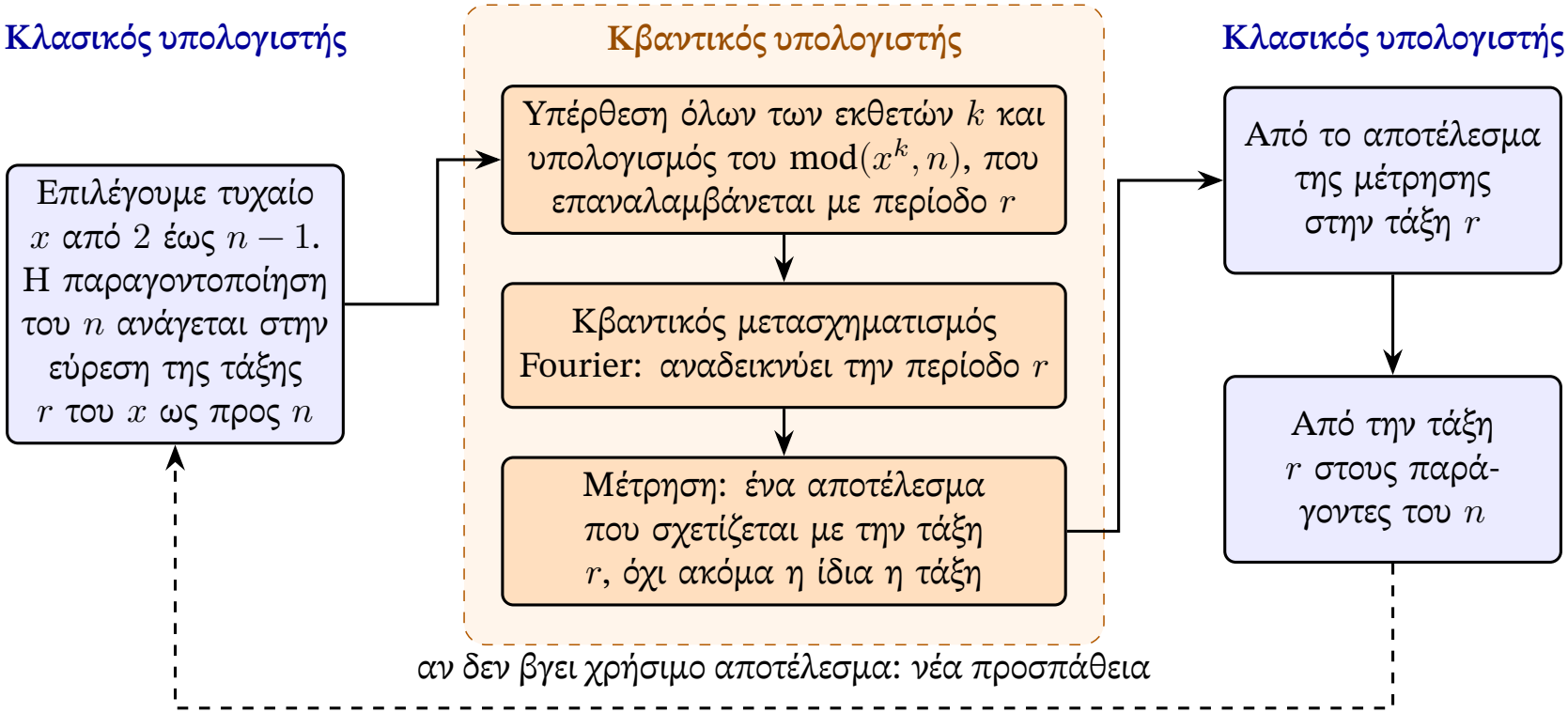
$$w = \mathrm{mod}(x^{r/2}, n)$$

  είναι ρίζα της μονάδας, και είναι μη τετριμμένη εκτός αν $w = n - 1$
- Παράδειγμα: $x = 2, n = 21, r = 6$. Βρίσκουμε $w = 8$ και τους παράγοντες $\gcd(7, 21) = 7$ και $\gcd(9, 21) = 3$
- Για $n = pq$, με p, q διαφορετικούς περιττούς πρώτους, ένα τυχαίο $x \in \mathbb{Z}_n^*$ έχει άρτια τάξη και $w \neq n - 1$ με πιθανότητα τουλάχιστον $1/2$
- Αν μπορούμε να βρούμε την τάξη, βρίσκουμε τους παράγοντες του n με λίγες προσπάθειες

Η γενική ιδέα

- Θέλουμε να παραγοντοποιήσουμε έναν σύνθετο αριθμό n. Επιλέγουμε τυχαία x από το 2 έως το $n-1$
- Αν $\gcd(x,n) > 1$, ο αλγόριθμος του Ευκλείδη μας έχει ήδη δώσει έναν παράγοντα
- Διαφορετικά $x \in \mathbb{Z}_n^*$ και ζητάμε την τάξη r του x modulo n
- Από την τάξη βρίσκουμε, με πιθανότητα τουλάχιστον $1/2$, έναν παράγοντα του n με λίγες κλασικές πράξεις. Η παραγοντοποίηση ανάγεται στην εύρεση της τάξης
- Η εύρεση της τάξης είναι δύσκολη για κλασικό υπολογιστή. Αυτό το βήμα αναλαμβάνει ο κβαντικός υπολογιστής
- Όλα τα υπόλοιπα βήματα είναι απλές πράξεις που ο κλασικός υπολογιστής κάνει γρήγορα
- Ο κβαντικός υπολογιστής βρίσκει την τάξη με την *εκτίμηση φάσης*, που στηρίζεται στον *κβαντικό μετασχηματισμό Fourier*. Αυτά θα δούμε στη συνέχεια

Καταμερισμός εργασίας



Η εύρεση της τάξης γίνεται στον κβαντικό υπολογιστή (πορτοκαλί περιοχή). Η προετοιμασία και η επεξεργασία του αποτελέσματος γίνονται κλασικά

Ο διακριτός μετασχηματισμός Fourier

- Η παραγοντοποίηση σε κβαντικό υπολογιστή συνδέεται άμεσα με τον μετασχηματισμό Fourier και ιδιαίτερα με την κβαντική του εκδοχή
- Ο κλασικός *DFT* παίρνει N μιγαδικούς αριθμούς $x_0, \ldots, x_{N-1}$ και δίνει $y_0, \ldots, y_{N-1}$ με

$$y_k = \sum_{p=0}^{N-1} x_p \, e^{j2\pi kp/N}$$

- Ο άμεσος υπολογισμός χρειάζεται N^2 πράξεις (διπλός βρόχος `for`)
- Ο *FFT* τον υπολογίζει σε $O(N \log N)$ πράξεις

Ο κβαντικός μετασχηματισμός Fourier

- Η είσοδος είναι n qubit στη βάση $|p\rangle$, με $p = 0, \ldots, N-1$ και $N = 2^n$
- Ο *QFT* $\hat{F}$ ορίζεται στις καταστάσεις βάσης ως

$$\hat{F}\,|p\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j2\pi kp/N}\,|k\rangle$$

- Είναι γραμμικός, άρα περιγράφεται από πίνακα $\mathbf{F}$ με στοιχεία

$$f_{kp} = \frac{1}{\sqrt{N}} e^{j2\pi kp/N}$$

- Είναι ο πίνακας του DFT διαιρεμένος με $\sqrt{N}$. Τον έχουμε ήδη συναντήσει για $n = 2$, στη διάσπαση σε διεπίπεδους πίνακες

Ο πίνακας F είναι μοναδιαίος

- Θέλουμε $\mathbf{F}\mathbf{F}^{\mathrm{T}} = \mathbf{I}_N$. Το στοιχείο c_{pq} του γινομένου είναι

$$c_{pq} = \frac{1}{N} \sum_{k=0}^{N-1} e^{j2\pi k(p-q)/N}$$

- Αν $p = q$, κάθε όρος είναι 1 και $c_{pp} = 1$
- Αν $p \neq q$, με $\omega = e^{j2\pi(p-q)/N} \neq 1$ και $\omega^N = 1$, το άθροισμα είναι γεωμετρική σειρά

$$1 + \omega + \cdots + \omega^{N-1} = \frac{\omega^N - 1}{\omega - 1} = 0$$

- Άρα οι στήλες είναι ορθοκανονικές και ο $\mathbf{F}$ είναι μοναδιαίος για κάθε n
- Ο παράγοντας $1/\sqrt{N}$ είναι αναγκαίος: χωρίς αυτόν θα παίρναμε $N\mathbf{I}_N$, ο πίνακας δεν θα διατηρούσε την πιθανότητα και δεν θα ήταν κβαντική πύλη

Παραδείγματα: $N = 2$ και $N = 4$

- Για $n = 1$ έχουμε $e^{j\pi kp} = (-1)^{kp}$ και

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

  δηλαδή η πύλη Hadamard. Ο QFT είναι η φυσική γενίκευσή της σε πολλά qubit

- Για $n = 2$ ισχύει $e^{j2\pi/4} = j$, άρα

$$\mathbf{F}_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}$$

- Οι στήλες είναι κάθετες. Για παράδειγμα

$$\langle \psi_0 | \psi_2 \rangle = \frac{1}{4}(1 - 1 + 1 - 1) = 0$$

Δράση σε τυχαία κατάσταση

- Για $|\psi\rangle = \sum_p x_p |p\rangle$ η γραμμικότητα δίνει

$$\hat{F}|\psi\rangle = \sum_{k=0}^{N-1} \tilde{y}_k |k\rangle, \qquad \tilde{y}_k = \frac{1}{\sqrt{N}} \sum_{p=0}^{N-1} x_p \, e^{j2\pi kp/N}$$

- Το πλάτος του $|k\rangle$ είναι ο DFT των πλατών της εισόδου, διαιρεμένος με $\sqrt{N}$
- Παράδειγμα $N = 4$: για $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ βρίσκουμε

$$\hat{F}|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+j}{2\sqrt{2}}|1\rangle + \frac{1-j}{2\sqrt{2}}|3\rangle$$

- Οι πιθανότητες είναι $\frac{1}{2}$, $\frac{1}{4}$, 0, $\frac{1}{4}$ και έχουν άθροισμα 1

Προσοχή

Ο QFT δεν είναι γρήγορη μηχανή υπολογισμού DFT: η μέτρηση δίνει ένα μόνο $|k\rangle$ και η υπόλοιπη πληροφορία χάνεται. Η δύναμή του φαίνεται όταν η πληροφορία είναι κωδικοποιημένη στη φάση (εκτίμηση φάσης)

Δυαδικά κλάσματα

- Γράφουμε $p = p_1 p_2 \cdots p_n$ στο δυαδικό, με το p_1 ως πιο σημαντικό ψηφίο
$$p = p_1 2^{n-1} + p_2 2^{n-2} + \cdots + p_n$$
- Το *δυαδικό κλάσμα* ορίζεται ως
$$0.b_1 b_2 \cdots b_m = \frac{b_1}{2} + \frac{b_2}{4} + \cdots + \frac{b_m}{2^m}$$
- Παράδειγμα: $0.101 = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$
- Ισχύει
$$\frac{p}{2^n} = 0.p_1 p_2 \cdots p_n$$

Από το άθροισμα στο γινόμενο

- Γράφουμε και το $k = k_1 \cdots k_n$ στο δυαδικό. Τότε

$$\frac{kp}{2^n} = \sum_{\mu=1}^{n} k_\mu \frac{p}{2^\mu}$$

- Το εκθετικό αθροίσματος είναι γινόμενο εκθετικών

$$e^{j2\pi kp/N} = \prod_{\mu=1}^{n} e^{j2\pi k_\mu p/2^\mu}$$

Από το άθροισμα στο γινόμενο (συνέχεια)

- Αθροίζουμε ανεξάρτητα ως προς κάθε ψηφίο $k_\mu \in \{0, 1\}$ αντί για το k από το 0 έως το $N - 1$. Το αποτέλεσμα είναι τανυστικό γινόμενο

$$\hat{F}\,|p\rangle = \frac{1}{\sqrt{N}} \bigotimes_{\mu=1}^{n} \sum_{k_\mu=0}^{1} e^{j2\pi k_\mu p/2^\mu} \left|k_\mu\right\rangle$$

- Αφού κάθε άθροισμα έχει δύο όρους, και το $1/\sqrt{N}$ μοιράζεται ως $1/\sqrt{2}$ σε κάθε παράγοντα,

$$\hat{F}\,|p\rangle = \bigotimes_{\mu=1}^{n} \frac{|0\rangle + e^{j2\pi p/2^\mu}\,|1\rangle}{\sqrt{2}}$$

Μόνο το κλασματικό μέρος μετράει

- Γράφουμε $p/2^\mu = m + \{p/2^\mu\}$, με m ακέραιο και $\{\cdot\}$ το κλασματικό μέρος
- Επειδή $e^{j2\pi m} = 1$, το ακέραιο μέρος δεν παίζει ρόλο στο εκθετικό
- Από την αναπαράσταση του p, οι όροι με $p_i 2^{n-\mu-i}$ και $n - \mu - i \geq 0$ είναι ακέραιοι. Έτσι το κλασματικό μέρος προκύπτει από τα μ τελευταία ψηφία του p:

$$\left\{ \frac{p}{2^\mu} \right\} = 0.p_{n-\mu+1} p_{n-\mu+2} \cdots p_n$$

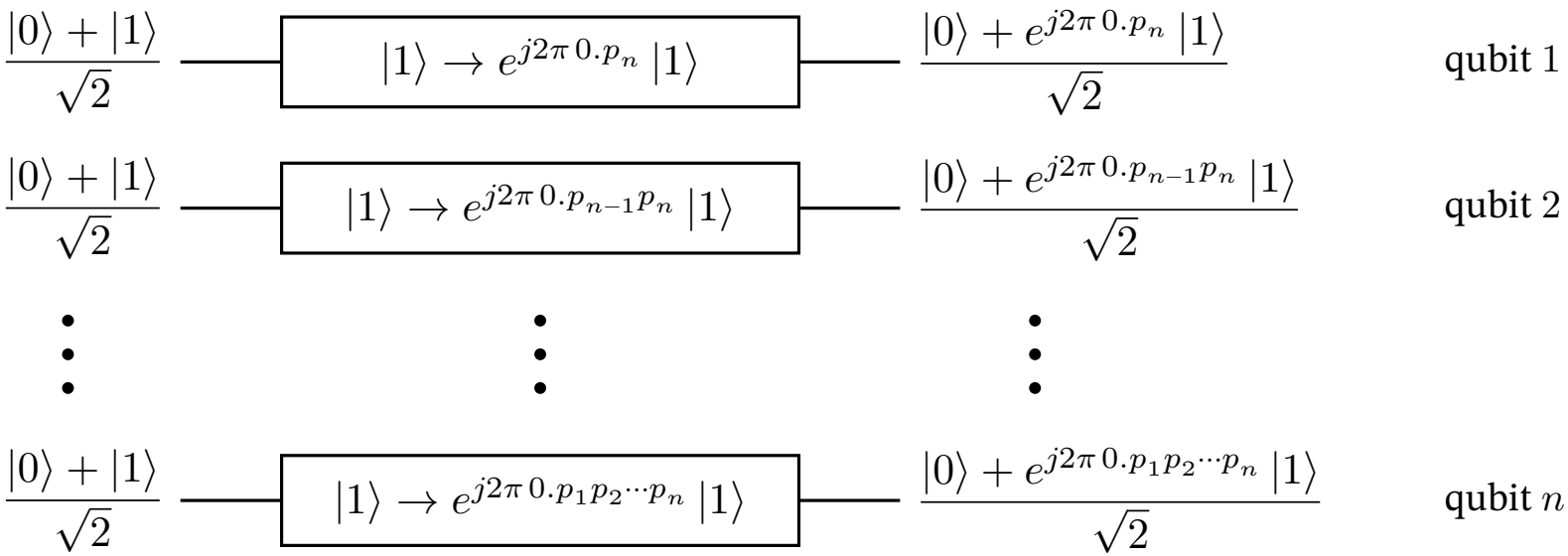
Ο τύπος γινομένου του QFT

Τύπος γινομένου

$$\hat{F}\left|p_1 \cdots p_n\right\rangle = \bigotimes_{\mu=1}^{n} \frac{\left|0\right\rangle + e^{j2\pi\, 0.p_{n-\mu+1}\cdots p_n}\left|1\right\rangle}{\sqrt{2}}$$

- Το $\hat{F}\left|p\right\rangle$ είναι γινόμενο καταστάσεων, μία για κάθε qubit: δεν υπάρχει εμπλοκή
- Κάθε qubit μ της εξόδου είναι η κατάσταση $(\left|0\right\rangle + \left|1\right\rangle)/\sqrt{2}$ με το $\left|1\right\rangle$ πολλαπλασιασμένο με μία φάση
- Το πρώτο qubit έχει φάση που εξαρτάται μόνο από το p_n, το δεύτερο από τα $p_{n-1}p_n$ και ούτω καθεξής, μέχρι το τελευταίο που εξαρτάται από όλα τα ψηφία

Η ερμηνεία του τύπου



Κάθε qubit περνάει από ένα κουτί που αφήνει το $|0\rangle$ όπως είναι και κάνει ολίσθηση φάσης στο $|1\rangle$. Η γωνία εξαρτάται από τα ψηφία του p

Παράδειγμα: $N = 4, p = 2$

- $p = 2 = |10\rangle$, με $p_1 = 1, p_2 = 0$. Οι φάσεις είναι $0.p_2 = 0.0 = 0$ και $0.p_1p_2 = 0.10 = \frac{1}{2}$
- Άρα $e^{j2\pi \cdot 0} = 1$ και $e^{j\pi} = -1$, και

$$\hat{F}_4 |10\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Πολλαπλασιάζοντας

$$\hat{F}_4 |10\rangle = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

- Είναι η τρίτη στήλη του $\mathbf{F}_4$, $\frac{1}{2}(1, -1, 1, -1)^{\mathrm{T}}$

Το κύκλωμα του QFT: πύλη H

- Στο qubit 1, που είναι στην $|p_1\rangle$, εφαρμόζουμε μια πύλη H. Επειδή $e^{j\pi p_1} = (-1)^{p_1}$,

$$H|p_1\rangle = \frac{|0\rangle + e^{j\pi p_1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{j2\pi\, 0.p_1}|1\rangle}{\sqrt{2}}$$

- Η H δίνει στο qubit 1 το πρώτο δυαδικό ψηφίο της φάσης $0.p_1p_2\cdots p_n$ που θέλουμε
- Για τα υπόλοιπα ψηφία χρειαζόμαστε ελεγχόμενες πύλες φάσης. Για $\nu = 2, \ldots, n$ ορίζουμε

$$\mathbf{R}_\nu = \begin{bmatrix} 1 & 0 \\ 0 & e^{j2\pi/2^\nu} \end{bmatrix}$$

Το κύκλωμα του QFT: ελεγχόμενες πύλες φάσης

- Εφαρμόζουμε την $\hat{C}_1^1(\hat{R}_\nu)$ με έλεγχο το qubit ν και στόχο το qubit 1
- Αν $p_\nu = 0$, δεν γίνεται τίποτα. Αν $p_\nu = 1$, το $|1\rangle$ του qubit 1 πολλαπλασιάζεται με $e^{j2\pi/2^\nu}$. Και στις δύο περιπτώσεις

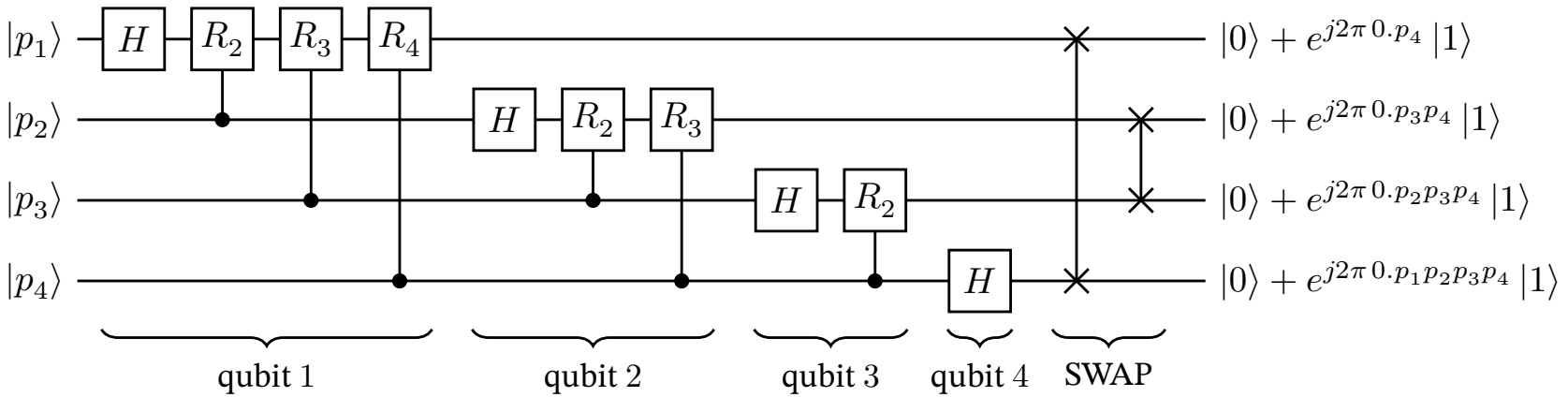
$$e^{j2\pi\, 0.p_1}\, e^{j2\pi p_\nu/2^\nu} = e^{j2\pi\,(0.p_1 + 0.0\cdots 0p_\nu)}$$

- Η πύλη προσθέτει το ψηφίο p_ν ακριβώς στη θέση ν της φάσης, ενώ το qubit-έλεγχος μένει αμετάβλητο
- Μετά από όλες τις πύλες, το qubit 1 έχει φάση

$$0.p_1 + 0.0p_2 + 0.00p_3 + \cdots = 0.p_1p_2\cdots p_n$$

- Γενικά, στο qubit μ εφαρμόζουμε μια H και μετά την $\hat{C}_1^1(\hat{R}_{\nu-\mu+1})$ για κάθε $\nu > \mu$. Το qubit μ καταλήγει με φάση $0.p_\mu p_{\mu+1}\cdots p_n$

Το πλήρες κύκλωμα του QFT



Το κύκλωμα βάζει στο σύρμα μ τη φάση $0.p_\mu \cdots p_n$, ενώ ο τύπος γινομένου τη θέλει στο qubit $n - \mu + 1$. Γι' αυτό στο τέλος αντιστρέφουμε τη σειρά των qubit με $\lfloor n/2 \rfloor$ πύλες SWAP

Πολυπλοκότητα του QFT

- Ο QFT σε n qubit υλοποιείται με n πύλες H, $n(n-1)/2$ ελεγχόμενες πύλες $\hat{C}_1^1(\hat{R}_\nu)$ και $\lfloor n/2 \rfloor$ πύλες SWAP
- Συνολικά
$$n + \frac{n(n-1)}{2} + \left\lfloor \frac{n}{2} \right\rfloor = O(n^2)$$
- Ο κλασικός FFT χρειάζεται
$$O(N \log_2 N) = O(2^n n)$$
πράξεις. Η διαφορά είναι εκθετική
- Αφού το κύκλωμα αποτελείται από μοναδιαίες πύλες, ο *αντίστροφος QFT* προκύπτει διαβάζοντάς το από δεξιά προς τα αριστερά, με $\hat{R}_\nu^{-1}$ στη θέση της $\hat{R}_\nu$. Ισχύει $\mathbf{F}^{-1} = \mathbf{F}^{\mathrm{T}}$

Παράδειγμα: το κύκλωμα για $n = 3$

- Επτά πύλες: H, R_2, R_3 στο qubit 1, H, R_2 στο qubit 2, H στο qubit 3 και SWAP των qubit $1, 3$
- Μετά τις πρώτες τρεις πύλες, το qubit 1 έχει φάση $0.p_1p_2p_3$. Μετά τις επόμενες δύο, το qubit 2 έχει $0.p_2p_3$, και μετά την H του qubit 3 έχουμε

$$\frac{|0\rangle + e^{j2\pi\, 0.p_1p_2p_3}\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{j2\pi\, 0.p_2p_3}\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{j2\pi\, 0.p_3}\,|1\rangle}{\sqrt{2}}$$

- Οι φάσεις είναι σωστές, αλλά σε αντίστροφη σειρά. Η SWAP ανταλλάσσει τα qubit 1 και 3 και παίρνουμε ακριβώς τον τύπο γινομένου, δηλαδή $\hat{F}_8\,|p_1p_2p_3\rangle$
- Για την είσοδο $|101\rangle$ οι φάσεις είναι $0.1 = \frac{1}{2}$, $0.01 = \frac{1}{4}$ και $0.101 = \frac{5}{8}$, άρα

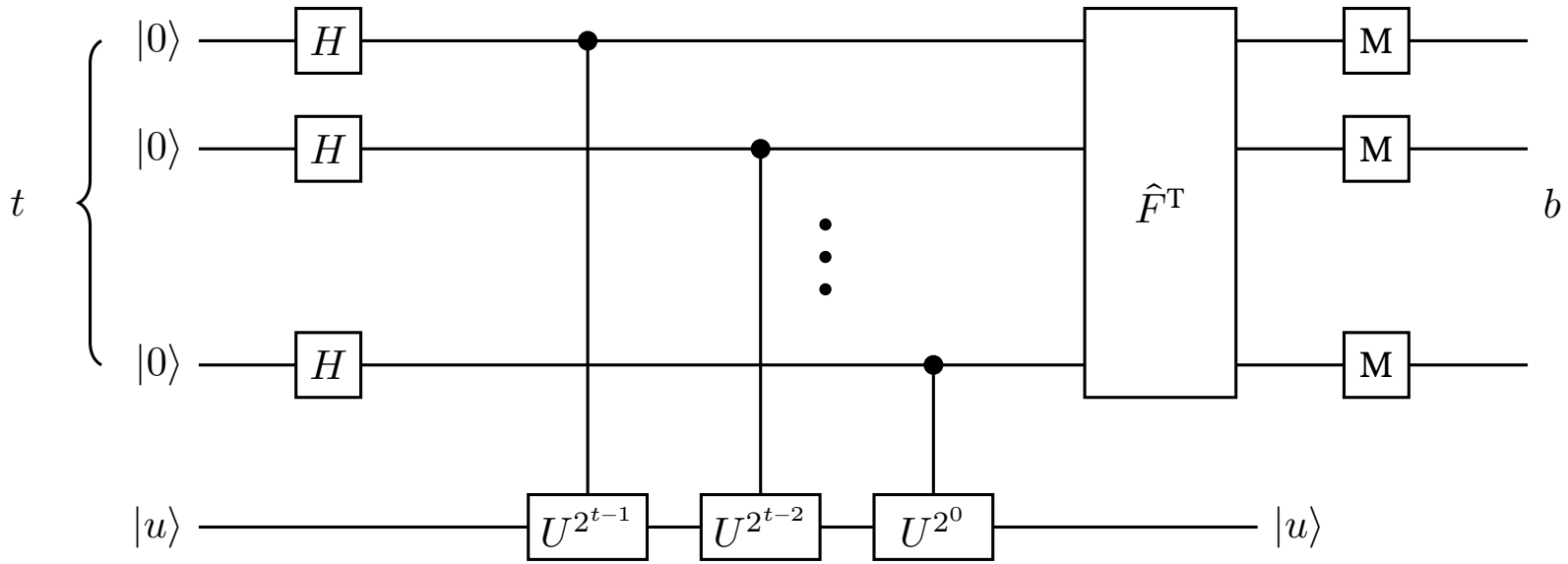
$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + j\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{j5\pi/4}\,|1\rangle}{\sqrt{2}}$$

- Ο συντελεστής του $|k_1\,k_2\,k_3\rangle$ είναι $(-1)^{k_1}\,j^{k_2}\,e^{j5\pi k_3/4}/\sqrt{8} = e^{j5\pi k/4}/\sqrt{8}$, δηλαδή η στήλη $p = 5$ του $\mathbf{F}_8$

Εκτίμηση φάσης: το πρόβλημα

- Έστω $\hat{U}$ μοναδιαία πύλη και $|u\rangle$ ιδιοκατάστασή της. Η ιδιοτιμή έχει μέτρο 1:
$$\hat{U}|u\rangle = e^{j2\pi\varphi}|u\rangle, \qquad 0 \leq \varphi < 1$$
- Αν μπορούμε να ετοιμάσουμε την $|u\rangle$ και να υλοποιήσουμε την $\hat{U}$ σε κύκλωμα, πόσο καλά μπορούμε να βρούμε το φ;
- Στον Shor το $\hat{U}$ επιλέγεται ώστε η φάση να σχετίζεται με την τάξη r
- Χρησιμοποιούμε δύο μητρώα: το *μητρώο μέτρησης* με t qubit, και το *μητρώο εργασίας* που περιέχει την $|u\rangle$. Θέτουμε $N = 2^t$

Το κύκλωμα της εκτίμησης φάσης



Τρία βήματα: H σε όλα τα qubit μέτρησης, ελεγχόμενες πύλες $\hat{U}^{2^k}$ στο μητρώο εργασίας, αντίστροφος QFT στο μητρώο μέτρησης και μέτρηση

Βήματα 1 και 2: η φάση κωδικοποιείται

- Οι H δίνουν ομοιόμορφη επικάλυψη $\frac{1}{\sqrt{N}} \sum_q |q\rangle |u\rangle$
- Το qubit q_k έχει βάρος 2^k στο q και ελέγχει την $\hat{U}^{2^k}$. Αφού $\hat{U}^{2^k} |u\rangle = e^{j2\pi\varphi 2^k} |u\rangle$, ισχύει

$$|q_k\rangle |u\rangle \to e^{j2\pi\varphi\, q_k 2^k} |q_k\rangle |u\rangle$$

- Η φάση «πηδάει» στο qubit-έλεγχο. Οι φάσεις όλων των qubit πολλαπλασιάζονται και, αφού $\sum_k q_k 2^k = q$, το μητρώο μέτρησης γίνεται

$$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{j2\pi q\varphi} |q\rangle$$

- Το μητρώο εργασίας μένει στην $|u\rangle$: δεν δημιουργείται εμπλοκή, επειδή η $|u\rangle$ είναι ιδιοκατάσταση
- Όλα τα πλάτη έχουν το ίδιο μέτρο και διαφέρουν μόνο στη φάση $e^{j2\pi q\varphi}$

Βήμα 3: ο αντίστροφος QFT

- Ο $\hat{F}^{\mathrm{T}}$ δρα ως $\hat{F}^{\mathrm{T}}\left|q\right\rangle = \frac{1}{\sqrt{N}} \sum_k e^{-j2\pi kq/N} \left|k\right\rangle$
- Εφαρμόζοντάς τον στην $\left|\psi_{\mathrm{in}}\right\rangle$,

$$\left|\psi_{\mathrm{out}}\right\rangle = \sum_{k=0}^{N-1} \alpha_k \left|k\right\rangle, \qquad \alpha_k = \frac{1}{N} \sum_{q=0}^{N-1} \omega^q$$

όπου

$$\omega = e^{j2\pi(\varphi - k/N)}$$

- Η μέτρηση του μητρώου δίνει τον ακέραιο b με πιθανότητα $|\alpha_b|^2$
- Ο αντίστροφος QFT μετατρέπει τις φάσεις σε μέτρα πλατών. Θα δούμε γιατί το b/N είναι καλή εκτίμηση του φ

Ακριβής φάση

- Αν $\varphi = \lambda/N$ με λ ακέραιο, τότε $|\psi_{\text{in}}\rangle = \hat{F}\,|\lambda\rangle$ και

$$|\psi_{\text{out}}\rangle = \hat{F}^{\text{T}}\hat{F}\,|\lambda\rangle = |\lambda\rangle$$

- Ισοδύναμα, $\alpha_\lambda = 1$ και, αν $k \neq \lambda$, η γεωμετρική σειρά δίνει $\alpha_k = 0$
- Η μέτρηση δίνει πάντα $b = \lambda$, και βρίσκουμε τη φάση ακριβώς: $\varphi = b/N$
- Παράδειγμα: $t = 3$, $N = 8$, $\varphi = 5/8$. Τότε $|\psi_{\text{in}}\rangle = \hat{F}_8\,|5\rangle$, η μέτρηση δίνει $b = 5$ και $b/N = 5/8 = \varphi$

Φάση που δεν είναι πολλαπλάσιο του $1/N$

- Γράφουμε $\varphi = (\lambda + \varepsilon)/N$, με λ τον πλησιέστερο ακέραιο στο $N\varphi$ και $|\varepsilon| \leq \frac{1}{2}$
- Από τη γεωμετρική σειρά, η πιθανότητα να μετρήσουμε $b = \lambda$ είναι

$$P(\lambda) = \frac{\sin^2(\pi\varepsilon)}{N^2 \sin^2(\pi\varepsilon/N)}$$

- Με τις ανισότητες $|\sin \pi x| \geq 2|x|$ για $|x| \leq \frac{1}{2}$ και $|\sin \pi x| \leq \pi|x|$ προκύπτει

$$P(\lambda) \geq \frac{4}{\pi^2} \approx 0{,}405$$

  ανεξάρτητα από το t και το φ
- Η πιθανότητα συγκεντρώνεται σε λίγους ακέραιους κοντά στο $N\varphi$
- Το 40% αρκεί: οι αποτυχίες ανιχνεύονται με κλασικό έλεγχο, οπότε επαναλαμβάνουμε

Παράδειγμα: $\varphi = 2/3, t = 3$

- $N = 8, N\varphi = 16/3 \approx 5{,}33$, άρα $\lambda = 5$ και $\varepsilon = 1/3$
- Οι πιθανότητες $|\alpha_k|^2$ για $k = 0, \ldots, 7$ είναι

$$0{,}0156,\ 0{,}0119,\ 0{,}0126,\ 0{,}0186,\ 0{,}0469,\ 0{,}6878,\ 0{,}1749,\ 0{,}0316$$

- Ο τύπος δίνει $P(5) = \dfrac{3/4}{64\sin^2(\pi/24)} \approx 0{,}6878$, πάνω από το $4/\pi^2$
- Η μέτρηση δίνει $b = 5$ ή $b = 6$ με πιθανότητα $0{,}6878 + 0{,}1749 \approx 0{,}86$
- Περισσότερα qubit μέτρησης δεν αυξάνουν την πιθανότητα επιτυχίας. Αυξάνουν την ακρίβεια της εκτίμησης b/N

Πόσα qubit μέτρησης χρειαζόμαστε

- Στον Shor η φάση είναι κλάσμα $\varphi = s/r$ με $r < n < 2^L$
- Θέλουμε $|b/N - s/r| < 1/(2r^2)$, ώστε να ανακτήσουμε το s/r με συνεχή κλάσματα. Το σφάλμα είναι το πολύ $1/(2N)$, άρα αρκεί $N \geq r^2$. Αφού $r < 2^L$, αρκεί $N \geq 2^{2L}$

Επιλογή του t

Με $t = 2L + 1$ qubit μέτρησης, με πιθανότητα τουλάχιστον $4/\pi^2$ παίρνουμε b με

$$\left| \frac{b}{N} - \frac{s}{r} \right| \leq \frac{1}{2N} < \frac{1}{2r^2}$$

- Οι $\hat{U}^{2^k}$ δεν απαιτούν 2^k εφαρμογές της $\hat{U}$: προκύπτουν με διαδοχικούς τετραγωνισμούς, και στον Shor υλοποιούνται απευθείας

Ο τελεστής $\hat{U}_x$

- Μητρώο εργασίας με L qubit, $2^L \geq n$, και $x \in \mathbb{Z}_n^*$. Ορίζουμε

$$\hat{U}_x |y\rangle = \begin{cases} |\mathrm{mod}(xy, n)\rangle, & y < n \\ |y\rangle, & y \geq n \end{cases}$$

- Ξεκινώντας από την $|1\rangle$ και εφαρμόζοντας τον $\hat{U}_x$ παίρνουμε διαδοχικά $|\mathrm{mod}(x, n)\rangle$, $|\mathrm{mod}(x^2, n)\rangle$, ..., και μετά από r εφαρμογές επιστρέφουμε στην $|1\rangle$
- Παράδειγμα: $n = 15$, $x = 2$, $L = 4$:

$$|1\rangle \to |2\rangle \to |4\rangle \to |8\rangle \to |1\rangle$$

άρα $r = 4$

- Ο πίνακας $\mathbf{U}_x$ είναι πίνακας μετάθεσης: ένα 1 σε κάθε γραμμή και στήλη. Κάθε πίνακας μετάθεσης είναι μοναδιαίος, $\mathbf{P}^{\mathrm{T}}\mathbf{P} = \mathbf{I}$
- Ισχύει $\hat{U}_x^a |y\rangle = |\mathrm{mod}(x^a y, n)\rangle$

Οι ιδιοκαταστάσεις του $\hat{U}_x$

- Αναζητούμε ιδιοκαταστάσεις στον χώρο που παράγουν οι $\left|\mathrm{mod}(x^k, n)\right\rangle$, $k = 0, \ldots, r-1$. Η συνθήκη ιδιοκατάστασης δίνει $e^{j2\pi\varphi r} = 1$, άρα $\varphi = s/r$ με $s = 0, \ldots, r-1$
- Για $s = 0, 1, \ldots, r-1$ ορίζουμε

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-j2\pi sk/r} \left|\mathrm{mod}(x^k, n)\right\rangle$$

- Κάθε $\left|u_s\right\rangle$ είναι ιδιοκατάσταση:

$$\hat{U}_x \left|u_s\right\rangle = e^{j2\pi s/r} \left|u_s\right\rangle$$

- Η τάξη r εμφανίζεται στον παρονομαστή της φάσης
- Παράδειγμα $n = 15, x = 2, r = 4$:

$$\left|u_1\right\rangle = \tfrac{1}{2}\left(\left|1\right\rangle - j\left|2\right\rangle - \left|4\right\rangle + j\left|8\right\rangle\right), \qquad \hat{U}_2 \left|u_1\right\rangle = j\left|u_1\right\rangle$$

Το $|1\rangle$ ως επικάλυψη ιδιοκαταστάσεων

- Πρόβλημα: ο ορισμός των $|u_s\rangle$ προϋποθέτει ότι ξέρουμε το r, που είναι αυτό που ψάχνουμε
- Λύση: δεν χρειαζόμαστε συγκεκριμένη ιδιοκατάσταση. Η απλή κατάσταση $|1\rangle$ είναι ισοβαρής επικάλυψη όλων

Το $|1\rangle$ ως επικάλυψη

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

- Απόδειξη: ο συντελεστής του $\left|\mathrm{mod}(x^k, n)\right\rangle$ είναι $\frac{1}{r}\sum_s e^{-j2\pi sk/r}$, που είναι 1 για $k = 0$ και 0 για $k = 1, \ldots, r-1$ (γεωμετρική σειρά)
- Παράδειγμα $n = 15$: $|u_0\rangle + |u_1\rangle + |u_2\rangle + |u_3\rangle = 2\,|1\rangle$

Το κύκλωμα βήμα-βήμα

- Αρχικά: μητρώο μέτρησης στην $|0 \cdots 0\rangle$ και μητρώο εργασίας στην $|1\rangle$. Μετά τις H,

$$|\phi_1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left(\frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} |q\rangle \right) |u_s\rangle$$

- Οι ελεγχόμενες πύλες εφαρμόζουν $\hat{U}_x^q$, και $\hat{U}_x^q |u_s\rangle = e^{j2\pi qs/r} |u_s\rangle$:

$$|\phi_2\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_{\text{in}}(s/r)\rangle |u_s\rangle$$

- Ο αντίστροφος QFT δρα στο μητρώο μέτρησης:

$$|\phi_3\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_{\text{out}}(s/r)\rangle |u_s\rangle$$

- Σαν r εκτιμήσεις φάσης παράλληλα. Η μέτρηση δίνει b με $b/N \approx s/r$ για τυχαίο s, με πιθανότητα $1/r$ το καθένα

Πότε αποτυγχάνει η μέτρηση

- Δεν ξέρουμε ούτε το s ούτε το r. Θα βρούμε s, r με $r < n$ ώστε το s/r να είναι κοντά στο b/N, με συνεχή κλάσματα
- Αν $s = 0$ (πιθανότητα $1/r$), παίρνουμε $b = 0$ και καμία πληροφορία
- Αν τα s και r έχουν κοινό διαιρέτη, το s/r απλοποιείται και βρίσκουμε μόνο διαιρέτη του r
- Και στις δύο περιπτώσεις επαναλαμβάνουμε το πείραμα

Παράδειγμα: $n = 15, x = 2, t = 3$

- $r = 4$, $N = 8$, φάσεις $s/4 = 0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$. Όλες είναι πολλαπλάσια του $1/8$, αφού $N \cdot s/4 = 2s$
- Άρα
$$|\phi_3\rangle = \frac{1}{2}\left(|0\rangle|u_0\rangle + |2\rangle|u_1\rangle + |4\rangle|u_2\rangle + |6\rangle|u_3\rangle\right)$$
και η μέτρηση δίνει $b = 0, 2, 4, 6$ με πιθανότητα $\frac{1}{4}$ το καθένα
- $b = 2$: $b/N = \frac{1}{4}$ και ο παρονομαστής δίνει $r = 4$. Ομοίως $b = 6$: $b/N = \frac{3}{4}$
- $b = 4$: $b/N = \frac{1}{2}$, βρίσκουμε μόνο τον διαιρέτη 2 του r. Ο έλεγχος $\mathrm{mod}(2^2, 15) = 4 \neq 1$ αποτυγχάνει και επαναλαμβάνουμε
- $b = 0$: καμία πληροφορία
- Με πιθανότητα $\frac{1}{2}$ βρίσκουμε την τάξη με την πρώτη προσπάθεια

Παράδειγμα: $n = 21, x = 2$

- $r = 6$, $L = 5$, $t = 11$, $N = 2048$. Το 6 δεν διαιρεί το 2048, άρα οι φάσεις $s/6$ δεν είναι πολλαπλάσια του $1/N$
- Η κορυφή για κάθε s βρίσκεται στον πλησιέστερο ακέραιο στο $N\, s/6$:

$$0,\ 341,\ 683,\ 1024,\ 1365,\ 1707$$

- Η μέτρηση δίνει b κοντά σε ένα από αυτά. Με συνεχή κλάσματα θα ανακτήσουμε το $s/6$ και την τάξη $r = 6$

Συνεχή κλάσματα

- Κάθε πραγματικός αριθμός z γράφεται ως *συνεχές κλάσμα*

$$z = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [a_0; a_1, a_2, ...]$$

με $a_0 = \lfloor z \rfloor$ και a_i θετικούς ακέραιους. Οι a_i βρίσκονται με διαδοχικές διαιρέσεις, όπως στον αλγόριθμο του Ευκλείδη

- Κόβοντας το ανάπτυγμα μετά τον όρο a_i παίρνουμε τη *συγκλίνουσα* p_i/q_i, με

$$p_i = a_i p_{i-1} + p_{i-2}, \qquad q_i = a_i q_{i-1} + q_{i-2}$$

και αρχικές τιμές $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$

Θεώρημα του Legendre

Αν $\gcd(p, q) = 1$ και $|z - p/q| < 1/(2q^2)$, τότε το p/q είναι συγκλίνουσα του z

Παράδειγμα: συνεχές κλάσμα του 167/256

- Διαδοχικές διαιρέσεις:

$$256 = 1 \cdot 167 + 89, \quad 167 = 1 \cdot 89 + 78, \quad 89 = 1 \cdot 78 + 11$$

$$78 = 7 \cdot 11 + 1, \quad 11 = 11 \cdot 1 + 0$$

- Άρα $\frac{167}{256} = [0; 1, 1, 1, 7, 11]$ και οι συγκλίνουσες είναι

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{15}{23}, \frac{167}{256}$$

- Παράδειγμα υπολογισμού: $p_4 = 7 \cdot 2 + 1 = 15$, $q_4 = 7 \cdot 3 + 2 = 23$
- Αν η πραγματική φάση ήταν $2/3$, η απόσταση $\frac{11}{768} \approx 0{,}014 < \frac{1}{18}$, και το $2/3$ βρίσκεται στις συγκλίνουσες
- Ποια είναι η σωστή; Δοκιμάζουμε κλασικά αν $\mathrm{mod}(x^q, n) = 1$ για τον παρονομαστή q κάθε συγκλίνουσας

Ανάκτηση της τάξης: $n = 21, b = 341$

- $N = 2048$. Οι διαιρέσεις:

$$2048 = 6 \cdot 341 + 2, \quad 341 = 170 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0$$

- Άρα $\frac{341}{2048} = [0; 6, 170, 2]$, με συγκλίνουσες

$$\frac{0}{1}, \frac{1}{6}, \frac{170}{1021}, \frac{341}{2048}$$

- Η $\frac{1}{6}$ έχει παρονομαστή $6 \leq n$ και $\mathrm{mod}(2^6, 21) = 1$: η τάξη είναι $r = 6$
- Το $b/N \approx 0{,}1665$ απέχει από το $1/6$ μόλις $0{,}0002$, πολύ λιγότερο από το κατώφλι $1/(2 \cdot 36) \approx 0{,}014$

Ο κβαντικός αλγόριθμος εύρεσης τάξης

Είσοδος: περιττός σύνθετος n και $x \in \mathbb{Z}_n^*$. Έξοδος: η τάξη r

1. $L = \lceil \log_2 n \rceil$, $t = 2L + 1$, $N = 2^t$. Μητρώο μέτρησης στην $|0 \cdots 0\rangle$, μητρώο εργασίας στην $|1\rangle$
2. Κύκλωμα εκτίμησης φάσης με $\hat{U} = \hat{U}_x$ και μέτρηση του b
3. Υπολογισμός των συγκλινουσών p_i/q_i του b/N
4. Για κάθε $q_i \leq n$, με αύξουσα σειρά, έλεγχος αν $\mathrm{mod}(x^{q_i}, n) = 1$
5. Αν κάποιο περάσει, είναι η τάξη. Διαφορετικά επιστρέφουμε στο βήμα 1

- Ο έλεγχος είναι σωστός: $\mathrm{mod}(x^q, n) = 1$ ακριβώς όταν $r \mid q$, άρα το πρώτο q_i που περνά είναι το r
- Αποτυχίες: κακό b (πιθανότητα το πολύ $1 - 4/\pi^2 \approx 0{,}6$), $s = 0$, ή s με κοινό διαιρέτη με το r. Όλες ανιχνεύονται και επαναλαμβάνουμε

Πόσο συχνά πετυχαίνει μια προσπάθεια

- Για $n = 21$, $x = 2$, $N = 2048$: 160 από τις 2048 τιμές του b οδηγούν στο σωστό $r = 6$ (7,8%)
- Η κατανομή του b όμως δεν είναι ομοιόμορφη: συγκεντρώνεται στις έξι κορυφές
- Οι πιθανότητες των καλών τιμών αθροίζονται σε περίπου $0{,}33$. Επιτυγχάνουν οι κορυφές των $s = 1$ και $s = 5$, τα μόνα σχετικά πρώτα με το 6, και κάθε s έχει πιθανότητα $1/6$, άρα $2/6 \approx 0{,}33$
- Περίπου μία στις τρεις προσπάθειες πετυχαίνει, και οι αποτυχίες ανιχνεύονται πάντα

Οι ελεγχόμενες πύλες $\hat{U}_x^{2^k}$

- Φαίνεται ότι η $\hat{U}_x^{2^k}$ απαιτεί 2^k εφαρμογές της $\hat{U}_x$, που θα ήταν καταστροφικό. Εκμεταλλευόμαστε τη δομή του τελεστή
- Οι $c_k = \mathrm{mod}(x^{2^k}, n)$ υπολογίζονται κλασικά με επαναλαμβανόμενο τετραγωνισμό, $c_k = \mathrm{mod}(c_{k-1}^2, n)$: μόνο k πολλαπλασιασμοί
- Η $\hat{U}_x^{2^k}$ είναι ο πολλαπλασιασμός επί τη σταθερά c_k modulo n, που υλοποιείται αντιστρέψιμα με κυκλώματα αριθμητικής κόστους $O(L^2)$
- Συνολικά $t = O(L)$ ελεγχόμενοι πολλαπλασιασμοί των $O(L^2)$ πυλών: $O(L^3)$ πύλες
- Παράδειγμα $n = 21, x = 2$:

$$c_0 = 2, \quad c_1 = 4, \quad c_2 = 16, \quad c_3 = \mathrm{mod}(256, 21) = 4, \ \ldots$$

και μετά εναλλάσσονται 4 και 16

Ο αλγόριθμος του Shor

Είσοδος: σύνθετος n με L bit. Έξοδος: μη τετριμμένος παράγοντας

1. *Κλασικοί έλεγχοι*: αν το n είναι άρτιο, επιστρέφουμε το 2. Αν είναι δύναμη πρώτου, βρίσκουμε τον παράγοντα με αναζήτηση ρίζας. Επιλέγουμε τυχαίο $x \in \{2, \ldots, n-2\}$ και αν $1 < \gcd(x, n) < n$ επιστρέφουμε το gcd
2. *Κβαντικό βήμα*: $t = 2L + 1$ qubit μέτρησης στην $|0 \cdots 0\rangle$ και L qubit εργασίας στην $|1\rangle$. H, ελεγχόμενες $\hat{U}_x^{2^k}$, αντίστροφος QFT, μέτρηση του b
3. *Κλασική επεξεργασία*: συγκλίνουσες του b/N και έλεγχος $\mathrm{mod}(x^q, n) = 1$. Αν βρούμε το r συνεχίζουμε, αλλιώς πίσω στο βήμα 2
4. *Από την τάξη στους παράγοντες*: αν το r είναι περιττό ή $\mathrm{mod}(x^{r/2}, n) = n - 1$, πίσω στο βήμα 1. Αλλιώς $w = \mathrm{mod}(x^{r/2}, n)$ και επιστρέφουμε $\gcd(w - 1, n)$, $\gcd(w + 1, n)$

Μόνο το βήμα 2 είναι κβαντικό

Κόστος του αλγορίθμου

- Οι ελεγχόμενοι πολλαπλασιασμοί: $t = 2L + 1$ το πλήθος, με $O(L^2)$ πύλες ο καθένας, άρα $O(L^3)$
- Ο αντίστροφος QFT σε $O(L)$ qubit κοστίζει $O(L^2)$ πύλες, αμελητέο μπροστά στο προηγούμενο
- Τα κλασικά βήματα (Ευκλείδης, συνεχή κλάσματα, δυνάμεις modulo) είναι πολυωνυμικά
- Συνολικά $O(L^3)$, ενώ ο GNFS έχει υποεκθετικό κόστος $\exp\big(O(L^{1/3}(\log L)^{2/3})\big)$
- Για RSA-2048: Shor περίπου 10^{10} πύλες, GNFS περίπου 10^{20} πράξεις
- Η πρακτική εφαρμογή απαιτεί κβαντικούς υπολογιστές με εκατομμύρια φυσικά qubit, λόγω διόρθωσης σφαλμάτων

Σύνοψη

- Η παραγοντοποίηση είναι κλασικά δύσκολη (υποεκθετικό κόστος). Ο Shor (1994) χρειάζεται $O(L^3)$ πύλες
- Ο QFT είναι μοναδιαία πύλη που στέλνει το $|p\rangle$ σε ισοβαρή επικάλυψη των $|k\rangle$ με φάσεις $e^{j2\pi kp/N}$. Ο τύπος γινομένου δίνει κύκλωμα με $O(n^2)$ πύλες, εκθετικά λιγότερες από τον FFT
- Η εκτίμηση φάσης (Hadamard, ελεγχόμενες $\hat{U}^{2^k}$, αντίστροφος QFT) δίνει b με $b/N \approx \varphi$. Με $t = 2L + 1$ qubit, το σφάλμα είναι αρκετά μικρό με πιθανότητα τουλάχιστον $4/\pi^2$
- Ο $\hat{U}_x$ έχει ιδιοτιμές $e^{j2\pi s/r}$ και το $|1\rangle$ είναι ισοβαρής επικάλυψη των ιδιοκαταστάσεών του. Έτσι η εκτίμηση φάσης με αρχική κατάσταση $|1\rangle$ δίνει $b \approx N\, s/r$ για τυχαίο s
- Τα συνεχή κλάσματα ανακτούν το s/r από το b/N και ένας κλασικός έλεγχος επιβεβαιώνει την τάξη
- Αν r άρτιο και $\mathrm{mod}(x^{r/2}, n) \neq n - 1$, οι $\gcd(x^{r/2} \pm 1, n)$ είναι παράγοντες του n. Το x είναι κατάλληλο με πιθανότητα τουλάχιστον $1/2$
- Μόνο η εκτίμηση φάσης είναι κβαντική. Οι αποτυχίες ανιχνεύονται και επαναλαμβάνονται