

6 Κβαντική Παραγοντοποίηση: Ο Αλγόριθμος του Shor

6.1 Επισκόπηση

Στην προηγούμενη ενότητα είδαμε τον πρώτο μεγάλο κβαντικό αλγόριθμο, αυτόν του Grover: μία τετραγωνική επιτάχυνση στην αναζήτηση μέσα σε ένα μη ταξινομημένο σύνολο δεδομένων. Πρόκειται για μια εντυπωσιακή, αλλά εντέλει μέτρια, βελτίωση — ο αριθμός των ερωτήσεων στο μαντείο πέφτει από N σε $\sqrt{N}$, παραμένοντας πάντως εκθετικός στο πλήθος των qubit. Το φυσικό ερώτημα που ακολουθεί είναι αν υπάρχει κάποιο υπολογιστικό πρόβλημα όπου ο κβαντικός υπολογιστής προσφέρει *εκθετική* επιτάχυνση, δηλαδή πολυωνυμικό αλγόριθμο εκεί όπου κάθε κλασικός αλγόριθμος χρειάζεται εκθετικό χρόνο.

Η απάντηση είναι θετική, και το πρόβλημα είναι από τα πιο σημαντικά στην πληροφορική: η *παραγοντοποίηση* μεγάλων αριθμών, δηλαδή η αναζήτηση των πρώτων παραγόντων ενός σύνθετου αριθμού n . Η ασφάλεια του ευρέως διαδεδομένου κρυπτοσυστήματος RSA βασίζεται ακριβώς στο ότι η παραγοντοποίηση θεωρείται —κλασικά— υπολογιστικά απαγορευτικά δαπανηρή για αριθμούς εκατοντάδων ψηφίων. Ο Peter Shor το 1994 έδειξε ότι ένας κβαντικός υπολογιστής μπορεί να παραγοντοποιήσει έναν αριθμό L ψηφίων (δυαδικών) σε χρόνο πολυωνυμικό στο L , της τάξης των L^3 στοιχειωδών πυλών, εκεί όπου οι καλύτεροι γνωστοί κλασικοί αλγόριθμοι απαιτούν χρόνο υποεκθετικό αλλά όχι πολυωνυμικό. Ήταν το αποτέλεσμα που έστρεψε την προσοχή όλου του κόσμου της πληροφορικής στην κβαντική υπολογιστική.

Η πορεία που θα ακολουθήσουμε είναι μεγάλη, αλλά κάθε βήμα της είναι από μόνο του ένα όμορφο κομμάτι κβαντικής υπολογιστικής. Πρώτα θα δούμε γιατί η παραγοντοποίηση είναι σημαντική και πόσο καλά μπορούμε να την κάνουμε κλασικά (ενότητα 6.2). Στη συνέχεια θα μελετήσουμε τον *κβαντικό μετασχηματισμό Fourier* (QFT), την κβαντική αναλογία του κλασικού μετασχηματισμού Fourier, και θα δούμε ότι υλοποιείται με πολύ οικονομικά κυκλώματα (ενότητα 6.3). Ο QFT θα μας δώσει αμέσως μία σημαντική υπορουτίνα, την *εκτίμηση φάσης* μιας μοναδιαίας πύλης (ενότητα 6.4). Το κεντρικό μαθηματικό αντικείμενο του αλγορίθμου του Shor είναι η *τάξη* r ενός αριθμού x modulo n , δηλαδή το μικρότερο θετικό ακέραιο με $x^r \equiv 1 \pmod{n}$. Στην ενότητα 6.5 θα δούμε ότι η εκτίμηση φάσης, εφαρμοσμένη σε μία κατάλληλα ορισμένη πύλη U_x , υπολογίζει την τάξη αυτή αποδοτικά. Στην ενότητα 6.6 θα δείξουμε ότι, αν έχουμε τη διάθεση της τάξης ως μαύρο κουτί, η παραγοντοποίηση ανάγεται σε αυτήν με καθαρά κλασικά βήματα. Τέλος, στην ενότητα 6.7 θα συναρμολογήσουμε όλα τα κομμάτια στον πλήρη αλγόριθμο του Shor και θα υπολογίσουμε την πολυπλοκότητά του.

6.2 Το πρόβλημα της παραγοντοποίησης και η κλασική πολυπλοκότητα

Το σημείο εκκίνησης είναι το *θεμελιώδες θεώρημα της αριθμητικής*: κάθε ακέραιος $n \geq 2$ γράφεται με μοναδικό τρόπο ως γινόμενο δυνάμεων πρώτων αριθμών,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}, \quad (6.1)$$

με πρώτους αριθμούς $p_1 < p_2 < \cdots < p_m$ και θετικούς εκθέτες a_i . Η ύπαρξη μιας τέτοιας αναπαράστασης είναι προφανής (διαιρούμε διαρκώς με πρώτους μέχρι να φτάσουμε στο 1)· η ουσία του θεωρήματος είναι η *μοναδικότητα*. Η παραγοντοποίηση είναι, με άλλα λόγια, ένα καλά ορισμένο υπολογιστικό πρόβλημα: δοθέντος του n , βρες τους πρώτους $p_1, \dots, p_m$ και τους εκθέτες $a_1, \dots, a_m$ της σχέσης (6.1).

Πριν μιλήσουμε για την πολυπλοκότητα, μια σημαντική σύμβαση: το «μέγεθος» της εισόδου δεν είναι ο αριθμός n αλλά το πλήθος L των δυαδικών ψηφίων του, $2^{L-1} \leq n < 2^L$. Ένας αλγόριθμος θεωρείται αποδοτικός αν ο χρόνος του είναι πολυώνυμο στο L — στο μήκος της εισόδου, όπως συνηθίζεται παντού στην πληροφορική — και όχι στο ίδιο το n , που είναι εκθετικά μεγαλύτερο. Αυτή η παρατήρηση από μόνη της εξηγεί γιατί η «βίαιη» προσέγγιση δεν είναι επιλογή: κάθε αλγόριθμος που δοκιμάζει ένας προς έναν τους υποψήφιους παράγοντες είναι υποχρεωτικά εκθετικός στο L .

Γιατί να μας νοιάζει η παραγοντοποίηση; Ο κυριότερος πρακτικός λόγος είναι η κρυπτογραφία. Στο κρυπτοσύστημα RSA, δύο πρώτοι αριθμοί p, q εκατοντάδων ψηφίων διαλέγονται και παραμένουν μυστικοί, και το γινόμενό τους $n = pq$ δημοσιεύεται ως δημόσιο κλειδί: οποιοσδήποτε μπορεί να κρυπτογραφήσει μηνύματα με τη βοήθεια του n , αλλά η αποκρυπτογράφηση χωρίς τη γνώση των p, q φαίνεται να απαιτεί την παραγοντοποίηση του n . Οι «προκλήσεις» (challenges) RSA είναι προκαθορισμένοι σύνθετοι αριθμοί, δημοσιευμένοι με σκοπό να μετρηθεί η πρόοδος των κλασικών αλγορίθμων: ο μεγαλύτερος που έχει μέχρι σήμερα

παραγοντοποιηθεί, ο RSA-250 με 829 δυαδικά ψηφία (250 δεκαδικά), έπεσε στις αρχές του 2020, μετά από υπολογιστική εργασία της τάξης των 2.700 πυρήνα-ετών. Το RSA-2048 (2.048 δυαδικά ψηφία), που χρησιμοποιείται πραγματικά σε εφαρμογές, βρίσκεται πολύ μακριά από κάθε κλασική δυνατότητα — όπως θα δούμε σε ένα λεπτό.

Ο απλούστερος κλασικός αλγόριθμος είναι η *διαίρεση δοκιμής* (trial division): δοκιμάζουμε διαδοχικά τους πρώτους 2, 3, 5, 7, ... μέχρι να βρούμε έναν που διαιρεί το n . αρκεί να φτάσουμε μέχρι το $\sqrt{n}$, γιατί αν το n έχει παράγοντα μεγαλύτερο του $\sqrt{n}$ έχει οπωσδήποτε και έναν μικρότερο. Στη χειρότερη περίπτωση (n γινόμενο δύο αντίστοιχων πρώτων) χρειάζονται της τάξης $\sqrt{n} = 2^{L/2}$ διαιρέσεις.

Παράδειγμα 6.1: Η ηλικία του σύμπαντος δεν αρκεί

Έστω n ένας αριθμός RSA-2048, δηλαδή $n \approx 2^{2048}$. Η διαίρεση δοκιμής χρειάζεται έως $\sqrt{n} = 2^{1024} \approx 1,8 \cdot 10^{308}$ διαιρέσεις. Ας υποθέσουμε, γενναιόδωρα, έναν υπολογιστή που εκτελεί 10^9 διαιρέσεις ανά δευτερόλεπτο. Ο χρόνος που χρειάζεται είναι

$$\frac{1,8 \cdot 10^{308}}{10^9 \text{ διαιρέσεις/s}} = 1,8 \cdot 10^{299} \text{ s} \approx 5,7 \cdot 10^{291} \text{ χρόνια.}$$

Η ηλικία του σύμπαντος είναι περίπου $1,4 \cdot 10^{10}$ χρόνια. Θα χρειαζόμασταν περίπου 10^{281} «ηλικίες σύμπαντος» — και μιλάμε για τον πιο αργό από τους κλασικούς αλγορίθμους. (Οι ταχύτεροι που ακολουθούν βελτιώνουν δραστικά την εικόνα, αλλά, όπως θα δούμε, όχι αρκετά.)

Η διαίρεση δοκιμής δεν είναι φυσικά το τέλος της κλασικής ιστορίας. Καλύτεροι αλγόριθμοι υπάρχουν: η μέθοδος ρ του Pollard βρίσκει παράγοντα σε χρόνο περίπου $n^{1/4} = 2^{L/4}$ (πάλι εκθετικό στο L), και ευφρέστερες μέθοδοι — η μέθοδος ελλειπτικών καμπυλών του Lenstra, το quadratic sieve κ.ά. — βελτιώνουν σταδιακά τον εκθέτη. Το πραγματικό όριο της κλασικής τέχνης είναι ο *γενικευμένος αλγόριθμος sieve αριθμικού πεδίου* (general number field sieve, GNFS), ο αλγόριθμος με τον οποίο παραγοντοποιήθηκε ο RSA-250, με χρόνο εκτέλεσης της μορφής

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

για κάποια σταθερά c — βλ. την εμβάθυνση 6.1 για το τι ακριβώς σημαίνει αυτή η έκφραση. Η κλασική «κλίμακα δυσκολίας» συνοψίζεται λοιπόν ως εξής:

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

Εμβάθυνση 6.1: Πολυωνυμικοί, υποεκθετικοί και εκθετικοί χρόνοι

Τρεις είναι οι κατηγορίες χρόνου εκτέλεσης που εμφανίζονται σε αυτό το κεφάλαιο, και αξίζει να τις δούμε συγκριτικά ως συναρτήσεις του μήκους εισόδου L :

- **Πολυωνυμικός**, $O(L^k)$ για σταθερό k : διπλασιάζοντας το L , ο χρόνος πολλαπλασιάζεται με σταθερό παράγοντα. Αυτή είναι η κατηγορία των «πρακτικά εφικτών» αλγορίθμων.
- **Εκθετικός**, $O(2^{cL})$: διπλασιάζοντας το L , ο χρόνος *τετραγωνίζεται*. Καμία ελπίδα πρακτικής εφαρμογής για μεγάλα L .
- **Υποεκθετικός**, της μορφής $\exp(O(L^\alpha (\log L)^\beta))$ με $0 < \alpha < 1$: κάπου ενδιάμεσα. Για μικρά και μεσαία L συμπεριφέρεται σχετικά διαχειρίσιμα, αλλά καθώς το L μεγαλώνει, η συνάρτηση $L^{1/3}(\log L)^{2/3}$ στο εκθετικό μεγαλώνει *χωρίς όριο*, οπότε τελικά κάθε υποεκθετικός αλγόριθμος χάνεται μπροστά σε οποιονδήποτε πολυωνυμικό.

Το εντυπωσιακό του αλγορίθμου του Shor δεν είναι απλώς ότι είναι ταχύτερος από τον GNFS — είναι ότι ανήκει σε *διαφορετική κατηγορία συνολικά*, εκθέτοντας το ότι η κλασική δυσκολία της παραγοντο-

ποίησης δεν είναι εγγενής ιδιότητα του προβλήματος αλλά ιδιότητα των κλασικών υπολογιστών.

Μία τελευταία, ενδιαφέρουσα παρατήρηση για την κλασική εικόνα. Το πρόβλημα του ελέγχου αν ένας αριθμός είναι πρώτος — πρόβλημα φαινομενικά «συγγενές» της παραγοντοποίησης — λύνεται κλασικά σε πολυωνυμικό χρόνο: ο πιθανοτικός αλγόριθμος Miller–Rabin (1980) το κάνει γρήγορα και με αυθαίρετα μικρή πιθανότητα λάθους, και από το 2002 υπάρχει και ντετερμινιστικός πολυωνυμικός αλγόριθμος (AKS). Η δυσκολία λοιπόν δεν κρύβεται στο «πρώτο ή σύνθετο;» αλλά στο «πώς μου λένε τους παράγοντες;». Αυτή η ασυμμετρία είναι και η καρδιά του RSA: εύκολο να φτιάξεις ένα δύσκολο-να-χαλάσεις $n = pq$ (διαλέγεις τυχαία μεγάλους πρώτους, κάτι που ελέγχεται γρήγορα), δύσκολο να το αντιστρέψεις χωρίς την ιδιωτική γνώση των p, q .

Δεν είναι γνωστός κανένας πολυωνυμικός κλασικός αλγόριθμος παραγοντοποίησης, ούτε και είναι γνωστό ότι κάτι τέτοιο αποκλείεται θεωρητικά — η παραγοντοποίηση δεν είναι ούτε αποδεδειγμένα «δύσκολη» πρόβλημα (όπως τα NP-hard προβλήματα, για τα οποία πιστεύουμε αλλά δεν αποδεικνύουμε δυσκολία), ούτε αποδεδειγμένα εύκολη. Είναι, με την τεχνική ορολογία, ένα πρόβλημα στην κλάση NP που πιστεύουμε εκτεταμένα ότι δεν είναι ούτε NP-complete ούτε πολυωνυμικό: παραμονεύει σε ένα ενδιαφέρον «ενδιάμεσο». Ο αλγόριθμος του Shor έδειξε ότι, όποια κι αν είναι η κλασική της μοίρα, κβαντικά η παραγοντοποίηση είναι εύκολη — και αυτό άλλαξε για πάντα το τοπίο.

6.3 Ο κβαντικός μετασχηματισμός Fourier

Ο κλασικός μετασχηματισμός Fourier (DFT) παίρνει ένα διάνυσμα N μιγαδικών αριθμών $(x_0, x_1, \dots, x_{N-1})$ και μας δίνει τις «συχνότητές» του, δηλαδή το νέο διάνυσμα $(y_0, \dots, y_{N-1})$ με

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

Είναι ένα από τα πιο χρήσιμα εργαλεία όλων των εφαρμοσμένων μαθηματικών, και ο ταχύτερος κλασικός αλγόριθμος για τον υπολογισμό του, ο ταχύς μετασχηματισμός Fourier (FFT), χρειάζεται $O(N \log N)$ αριθμητικές πράξεις αντί για τις N^2 του αφελούς υπολογισμού.

Η κβαντική εκδοχή λειτουργεί σε καταστάσεις αντί για διανύσματα δεδομένων. Έστω μητρώο n qubit, δηλαδή χώρος Hilbert διάστασης $N = 2^n$ με βάση τα $|p\rangle$, $p = 0, 1, \dots, N-1$, και έστω μια κατάσταση $|\psi\rangle = \sum_p x_p |p\rangle$ με κανονικοποιημένους συντελεστές. Ο κβαντικός μετασχηματισμός Fourier (QFT) είναι η μοναδιαία πύλη F_N που δρα στις καταστάσεις βάσης ως εξής:

$$\hat{F}_N |p\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j2\pi kp/N} |k\rangle, \quad p = 0, 1, \dots, N-1. \quad (6.2)$$

Ο πίνακας της στη βάση αυτή έχει στοιχεία

$$f_{kp} = \langle k | \hat{F}_N | p \rangle = \frac{e^{j2\pi kp/N}}{\sqrt{N}},$$

δηλαδή, γραμμένος ως πίνακας, είναι ο πίνακας του κλασικού DFT διαιρεμένος με $\sqrt{N}$ — μια κανονικοποίηση που είναι αναγκαία για μοναδιαιότητα, όπως θα δούμε σε ένα λεπτό. Τον πίνακα αυτόν έχουμε ήδη συναντήσει: για $n = 2$ qubit είναι ο $\mathcal{M}$ με στοιχεία $u_{pq} = \frac{1}{2}j^{pq}$ που αναλύσαμε σε διεπίπεδους πίνακες στο παράδειγμα 4.11 της ενότητας 4.6, με επαλήθευση σε Python στο `ex_two_level_QFT4.py`.

Παράδειγμα 6.2: Ο QFT ενός qubit είναι η πύλη Hadamard

Για $n = 1$ qubit ($N = 2$) ο ορισμός (6.2) δίνει

$$\hat{F}_2 |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \hat{F}_2 |1\rangle = \frac{|0\rangle + e^{j\pi} |1\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

αφού $e^{j2\pi kp/2} = e^{j\pi kp} = (-1)^{kp}$. Ο πίνακας είναι άρα

$$F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

δηλαδή η γνωστή μας πύλη Hadamard H (ενότητα 3.13). Ο QFT είναι επομένως μια φυσική γενίκευση της Hadamard σε πολλά qubit.

Αποτέλεσμα 6.1: Ο QFT είναι μοναδιαίος

Ο πίνακας με στοιχεία $f_{kp} = e^{j2\pi kp/N} / \sqrt{N}$ είναι μοναδιαίος για κάθε N .

Απόδειξη. Αρκεί να ελέγξουμε ότι οι στήλες του πίνακα είναι ορθοκανονικές (ενότητα 1.11):

$$\sum_{k=0}^{N-1} f_{kp}^* f_{kq} = \frac{1}{N} \sum_{k=0}^{N-1} e^{j2\pi k(q-p)/N}.$$

Για $p = q$ το άθροισμα είναι $N/N = 1$. Για $p \neq q$ θέτουμε $\omega = e^{j2\pi(q-p)/N}$: πρόκειται για N -οστή ρίζα της μονάδας διαφορετική του 1, με $\omega^N = e^{j2\pi(q-p)} = 1$, οπότε η γεωμετρική σειρά μηδενίζεται:

$$\sum_{k=0}^{N-1} \omega^k = \frac{\omega^N - 1}{\omega - 1} = 0.$$

Άρα οι στήλες είναι ορθοκανονικές και ο πίνακας μοναδιαίος. ■

Μία πρώτη, βιαστική σκέψη θα ήταν: «θαύμα! ο QFT υπολογίζει όλες τις N συντελεστές Fourier της κατάστασης $|\psi\rangle$ ταυτόχρονα, με ένα μόνο κύκλωμα — ας τις διαβάσουμε». Η σκέψη σκοντάφτει στο γνωστό εμπόδιο της μέτρησης: αν μετρήσουμε το μητρώο, θα πάρουμε ένα μόνο αποτέλεσμα k , με πιθανότητα $|y_k|^2$, όπου y_k ο k -ος συντελεστής Fourier της $|\psi\rangle$. Όλα τα υπόλοιπα χάνονται στην κατάρρευση. Ο QFT δεν είναι, επομένως, μια «γρήγορη μηχανή DFT». Η πραγματική του δύναμη είναι αλλού: σε κυκλώματα όπου η φασματική πληροφορία κωδικοποιείται στη φάση μιας επικάλυψης και ξαναδιαβάζεται με τον αντίστροφο QFT — ακριβώς το σχήμα που θα κατασκευάσουμε στην ενότητα 6.4.

Παρ' όλα αυτά, η κατασκευή αποδοτικών κυκλωμάτων για τον QFT είναι εντυπωσιακή από μόνη της. Ο κλασικός FFT πάνω σε $N = 2^n$ αριθμούς χρειάζεται $O(N \log N) = O(2^n n)$ πράξεις — εκθετικό πλήθος στο n . Θα δούμε ότι ο QFT υλοποιείται με μόλις $O(n^2)$ πύλες.

Ο τύπος γινομένου

Το κλειδί για την οικονομική υλοποίηση είναι ένας κλειστός τύπος για τη δράση του $\hat{F}_N$ σε κατάσταση βάσης, που αποκαλύπτει ότι το αποτέλεσμα είναι γινόμενο καταστάσεων μεμονωμένων qubit — χωρίς καθόλου επικάλυψη. Γράφουμε τον ακέραιο p σε δυαδική μορφή $p = p_1 p_2 \cdots p_n$ (με το p_1 ως πιο σημαντικό ψηφίο), δηλαδή

$$p = \sum_{\mu=1}^n p_\mu 2^{n-\mu},$$

και εισάγουμε τον συμβολισμό των δυαδικών κλασμάτων:

$$0.b_1 b_2 \cdots b_m := \frac{b_1}{2} + \frac{b_2}{4} + \cdots + \frac{b_m}{2^m}.$$

Παράδειγμα: $0.101 = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$. Ο συμβολισμός είναι συμβατός με τη συνήθη δυαδική αναπαράσταση: το $p/2^n$ γράφεται $0.p_1 p_2 \cdots p_n$.

Ξεκινάμε από τον ορισμό (6.2) και αναπτύσσουμε τον εκθέτη. Με $k = \sum_{\mu} k_{\mu} 2^{n-\mu}$:

$$\frac{kp}{N} = \frac{kp}{2^n} = \sum_{\mu=1}^n k_{\mu} \frac{p}{2^{\mu}}, \quad \text{οπότε} \quad e^{j2\pi kp/N} = \prod_{\mu=1}^n e^{j2\pi k_{\mu} p/2^{\mu}}.$$

Το πλεονέκτημα είναι προφανές: ο εκθέτης διασπάστηκε σε άθροισμα όρων, καθένας από τους οποίους εξαρτάται από ένα μόνο δυαδικό ψηφίο k_{μ} του k . Το άθροισμα πάνω στα k διασπάται επομένως σε γινόμενο αθροισμάτων πάνω στα επιμέρους ψηφία:

$$\hat{F}_N |p\rangle = \frac{1}{\sqrt{N}} \sum_{k_1, \dots, k_n \in \{0,1\}} \prod_{\mu=1}^n e^{j2\pi k_{\mu} p/2^{\mu}} |k_1 k_2 \dots k_n\rangle = \bigotimes_{\mu=1}^n \frac{|0\rangle + e^{j2\pi p/2^{\mu}} |1\rangle}{\sqrt{2}}.$$

Μένει να απλοποιήσουμε τις φάσεις. Για κάθε μ , μόνο το κλασματικό μέρος του $p/2^{\mu}$ συμβάλλει, αφού $e^{j2\pi m} = 1$ για κάθε ακέραιο m :

$$e^{j2\pi p/2^{\mu}} = e^{j2\pi \{p/2^{\mu}\}},$$

όπου με $\{x\}$ συμβολίζουμε το κλασματικό μέρος. Το κλάσμα $\{p/2^{\mu}\}$ διαβάζεται απευθείας από τα δυαδικά ψηφία του p : μετατοπίζοντας το δυαδικό σημείο $p_1 p_2 \dots p_n$ κατά μ θέσεις αριστερά, δεξιά του σημείου μένουν τα τελευταία μ ψηφία του p , δηλαδή $\{p/2^{\mu}\} = 0.p_{n-\mu+1} p_{n-\mu+2} \dots p_n$. Καταλήγουμε στον τύπο γινόμενου:

Αποτέλεσμα 6.2: Ο τύπος γινόμενου του QFT

$$\hat{F}_N |p_1 p_2 \dots p_n\rangle = \frac{|0\rangle + e^{j2\pi 0.p_n} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{j2\pi 0.p_{n-1} p_n} |1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + e^{j2\pi 0.p_1 p_2 \dots p_n} |1\rangle}{\sqrt{2}}. \quad (6.3)$$

Ιδού η μεγάλη έκπληξη: το $\hat{F}_N |p\rangle$ είναι γινόμενο καταστάσεων, μία για κάθε qubit — η δράση του QFT σε κατάσταση βάσης δεν δημιουργεί κανέναν εμπλογισμό. Το πρώτο qubit της εξόδου φέρει φάση που εξαρτάται μόνο από το τελευταίο ψηφίο p_n της εισόδου, το δεύτερο από τα δύο τελευταία, και ούτω καθεξής, μέχρι το τελευταίο qubit, που φέρει φάση εξαρτώμενη από όλα τα ψηφία.

Παράδειγμα 6.3: Επαλήθευση του τύπου γινόμενου για $N = 4$

Παίρνουμε $p = 2 = |10\rangle$, δηλαδή $p_1 = 1, p_2 = 0$. Ο τύπος (6.3) δίνει

$$\hat{F}_4 |10\rangle = \frac{|0\rangle + e^{j2\pi 0.0} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{j2\pi 0.10} |1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2},$$

αφού $0.p_2 = 0.0 = 0$ και $0.p_1 p_2 = 0.10 = \frac{1}{2}$, με $e^{j2\pi/2} = e^{j\pi} = -1$. Πράγματι, η τρίτη στήλη του πίνακα $\mathcal{M}$ του παραδείγματος 4.11 είναι $\frac{1}{2}(1, -1, 1, -1)^T$ — δηλαδή ακριβώς οι συντελεστές που υπολογίσαμε, με τη σειρά $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Το κύκλωμα

Ο τύπος (6.3) υλοποιείται άμεσα με ένα κύκλωμα από τρεις τύπους πυλών:

1. Μία H στο qubit 1 δίνει $|p_1\rangle \rightarrow (|0\rangle + e^{j\pi p_1} |1\rangle)/\sqrt{2} = (|0\rangle + e^{j2\pi 0.p_1} |1\rangle)/\sqrt{2}$, δηλαδή το σωστό πρώτο δυαδικό ψηφίο της φάσης του πρώτου qubit.
2. Η φάση εμπλουτίζεται με ελεγχόμενες πύλες φάσης. Ορίζουμε

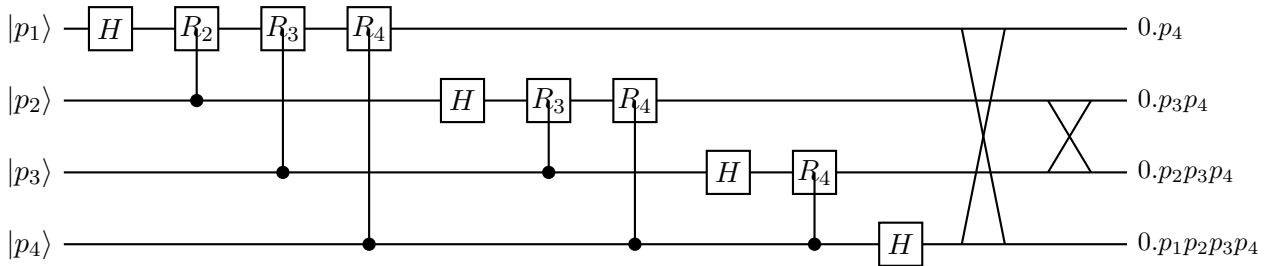
$$\mathbf{R}_{\nu} = \begin{bmatrix} 1 & 0 \\ 0 & e^{j2\pi/2^{\nu}} \end{bmatrix}, \quad \nu = 2, 3, \dots, n,$$

και εφαρμόζουμε την ελεγχόμενη πύλη $\hat{C}_1^1(\hat{R}_{\nu})$ (ενότητα 4.1) με qubit-έλεγχο το ν και qubit-στόχο το 1: αν $p_{\nu} = 1$, το $|1\rangle$ του πρώτου qubit πολλαπλασιάζεται με $e^{j2\pi/2^{\nu}} = e^{j2\pi 0.0\dots 01}$, όπου το 1

βρίσκεται στη ν -οστή θέση μετά το δυαδικό σημείο. Μετά από όλες αυτές τις πύλες το qubit 1 έχει φάση $0.p_1 + 0.0p_2 + 0.00p_3 + \dots = 0.p_1p_2 \dots p_n$, όπως θέλουμε για το τελευταίο qubit της εξόδου στον τύπο (6.3).

3. Γενικά, στο qubit μ εφαρμόζουμε πρώτα μία H και κατόπιν $\hat{C}_1^1(\hat{R}_\nu)$ για όλα τα $\nu > \mu$, με έλεγχο το qubit ν : το qubit μ καταλήγει με φάση $0.p_\mu p_{\mu+1} \dots p_n$.

Υπάρχει όμως μια λεπτομέρεια: κατά τον τύπο (6.3), το qubit μ της εξόδου πρέπει να φέρει τη φάση $0.p_{n-\mu+1} \dots p_n$, ενώ το κύκλωμα τοποθετεί στο σύρμα μ τη φάση $0.p_\mu \dots p_n$ — δηλαδή τη φάση του qubit $n - \mu + 1$. Η λύση είναι απλή: στο τέλος αντιστρέφουμε τη σειρά των qubit με $\lfloor n/2 \rfloor$ πύλες SWAP (τα qubit $1 \leftrightarrow n, 2 \leftrightarrow n-1$ κ.ο.κ.). Το πλήρες κύκλωμα για $n = 4$ qubit:



Αποτέλεσμα 6.3: Η πολυπλοκότητα του QFT

Ο QFT σε n qubit ($N = 2^n$) υλοποιείται με n πύλες H , $\binom{n}{2} = n(n-1)/2$ ελεγχόμενες πύλες $\hat{C}_1^1(\hat{R}_\nu)$ και $\lfloor n/2 \rfloor$ πύλες SWAP — συνολικά $O(n^2)$ πύλες. Ο κλασικός FFT πάνω στα N συντελεστές απαιτεί $O(N \log N) = O(2^n n)$ πράξεις. Επειδή $n = \log_2 N$, η διαφορά είναι εκθετική: $O(n^2)$ έναντι $O(2^n n)$.

Μία δευτερεύουσα παρατήρηση: οι γωνίες των περιστροφών R_ν μικραίνουν εκθετικά με το ν : για μεγάλα ν η πύλη είναι πρακτικά η ταυτότητα. Μπορεί να αποδειχθεί ότι παραλείποντας όλες τις R_ν με ν πάνω από μια τάξη $\log n$, το κύκλωμα προσεγγίζει τον QFT με αυθαίρετα μικρό σφάλμα χρησιμοποιώντας μόνο $O(n \log n)$ πύλες. Για τις ανάγκες μας δεν θα χρειαστούμε αυτή τη βελτιστοποίηση — το $O(n^2)$ είναι ήδη εκθετικά καλύτερο από οτιδήποτε κλασικό.

Παράδειγμα 6.4: Ο QFT σε Python

Το παρακάτω πρόγραμμα κατασκευάζει το κύκλωμα του QFT για $n = 3$ qubit από τις στοιχειώδεις πύλες του qulib2.py (μία H και ελεγχόμενες R_ν ανά qubit, και στο τέλος τις SWAP, καθεμία υλοποιημένη με τρεις CNOT) και συγκρίνει το γινόμενο με τον ακριβή πίνακα (6.2) για $N = 8$: κατόπιν επαληθεύει και τον τύπο γινομένου (6.3) στη βάση |101>:

```
import functools
import operator as op

import numpy as np

from qulib2 import ControlledGate, Gate, GateH, GateX, I, QuantumState

np.set_printoptions(precision=3, suppress=True)

n = 3
N = 2 ** n

# Ηπύληφάσης R_nu = diag(1, e^{j \pi 2 / 2^{nu}}), nu = 2, 3, ...
def R(nu):
    return Gate(U=np.diag([1.0, np.exp(2j * np.pi / 2 ** nu)]))

# Ενσωμάτωση 1-qubit πύλης g στο qubit mu (theta = αριστερό) μητρώου n qubit
def single(mu, g):
```

```

    return I(mu) ** g ** I(n - 1 - mu)

# CNOT σεμνηρώ n qubit: control, target = δείκτες qubit
def CNOT(control, target):
    rest = [q for q in range(n) if q not in (control, target)]
    return ControlledGate(n, through=rest, control=[control], target=[target], gate=GateX())

# SWAP δύο qubit μέσω τριών CNOT
def swap(q1, q2):
    return CNOT(q1, q2) @ CNOT(q2, q1) @ CNOT(q1, q2)

# Κατασκευή του κυκλώματος QFT: στο qubit mu πρώτα μία H και κατόπιν
# ελεγχόμενες Rnu με έλεγχο κάθε qubit nu στα δεξιά του (nu > mu).
circuit = I(n)
for mu in range(n):
    circuit = single(mu, GateH()) @ circuit
    for nu in range(mu + 1, n):
        rest = [q for q in range(n) if q not in (mu, nu)]
        CR = ControlledGate(n, through=rest, control=[nu], target=[mu], gate=R(nu - mu + 1))
        circuit = CR @ circuit

# Τέλος αντιστρέφουμε τη σειρά των qubit με floor(n/2) πύλες SWAP
for mu in range(n // 2):
    circuit = swap(mu, n - 1 - mu) @ circuit

# Ο ακριβής πίνακας του QFT:  $f_{\{kp\}} = e^{j \pi^2 k p / N} / \sqrt{N}$ 
F = np.array([[np.exp(2j * np.pi * k * p / N) / np.sqrt(N) for p in range(N)]
              for k in range(N)])

print("Κύκλωμα (H + ελεγχόμενες R + SWAP) == QFT_8;", np.allclose(circuit.calc_U(), F))
print("μέγιστη απόκλιση:", np.max(np.abs(circuit.calc_U() - F)))

# Επαλήθευση του τύπου γινόμενου για την κατάσταση εισόδου  $|p\rangle = |101\rangle$  ( $p = 5$ ):
# το qubit 0 φέρει φάση  $\theta.p_2 = 0.1$ , το qubit 1 φάση  $\theta.p_1 p_2 = 0.01$ ,
# το qubit 2 φάση  $\theta.p_0 p_1 p_2 = 0.101 = 5/8$ .
psi_in = QuantumState({"101": 1.0})
state_out = circuit @ psi_in
print("απόσκοπη έξοδος του κυκλώματος για |101>:")
print(state_out.a)

# Ο τύπος γινόμενου:  $(|\theta\rangle + e^{j\pi} |1\rangle) / \sqrt{2} \otimes (|\theta\rangle + e^{j\pi/2} |1\rangle) / \sqrt{2} \otimes (|\theta\rangle + e^{j\pi/4} |1\rangle) / \sqrt{2}$ 
phase = [np.exp(2j * np.pi * 0.5), np.exp(2j * np.pi * 0.25), np.exp(2j * np.pi * 0.625)]
product = functools.reduce(pyop.pow, [QuantumState([1, ph]) for ph in phase])
print("κτάση από τον τύπο γινόμενου:")
print(product.a)
print("συμφωνούν;", np.allclose(state_out.a, product.a))

```

Η έξοδος επιβεβαιώνει ότι το γινόμενο των πυλών του κυκλώματος ισούται με τον πίνακα F_8 (μέγιστη απόκλιση της τάξης 10^{-15} , δηλαδή στο όριο της αριθμητικής ακρίβειας) και ότι η κατάσταση εξόδου για $|101\rangle$ συμπίπτει με το γινόμενο των μονοqubit καταστάσεων με φάσεις $0.p_3 = 0.1$, $0.p_2 p_3 = 0.01$ και $0.p_1 p_2 p_3 = 0.101 = 5/8$.

Ο αντίστροφος QFT

Καθώς το κύκλωμα του QFT αποτελείται από μοναδιαίες πύλες, ο αντίστροφός του προκύπτει απλά τρέχοντας το κύκλωμα αντίστροφα στον χρόνο: διαβάζουμε το διάγραμμα από δεξιά προς τα αριστερά, αντικαθιστώντας κάθε πύλη με την αντίστροφή της (ενότητα 1.10), δηλαδή κάθε $\hat{C}_1^1(\hat{R}_\nu)$ με $\hat{C}_1^1(\hat{R}_\nu^{-1})$ με

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

Σε πίνακες: $\mathbf{F}_N^{-1} = \mathbf{F}_N^\dagger$, και επειδή ο πίνακας είναι συμμετρικός ($f_{kp} = f_{pk}$), η αντιστροφή ισοδυναμεί με συζυγία όλων των στοιχείων του. Σημειώνουμε ότι στην εφαρμογή που ακολουθεί (εκτίμηση φάσης) θα χρειαστούμε ακριβώς τον αντίστροφο QFT — αυτή η «κατεύθυνση» του μετασχηματισμού είναι που μετατρέπει τη φασική κωδικοποίηση σε διακριτή μέτρηση.

6.4 Εκτίμηση φάσης

Το δεύτερο δομικό στοιχείο του αλγορίθμου του Shor είναι μια γενική και πολύ κομψή τεχνική, την οποία αποκαλούμε *εκτίμηση φάσης* (phase estimation). Έστω U μια οποιαδήποτε μοναδιαία πύλη που δρα σε κάποιο μητρώο, και έστω $|u\rangle$ μια ιδιοκατάστασή της με ιδιοτιμή μονάδιου μέτρου,

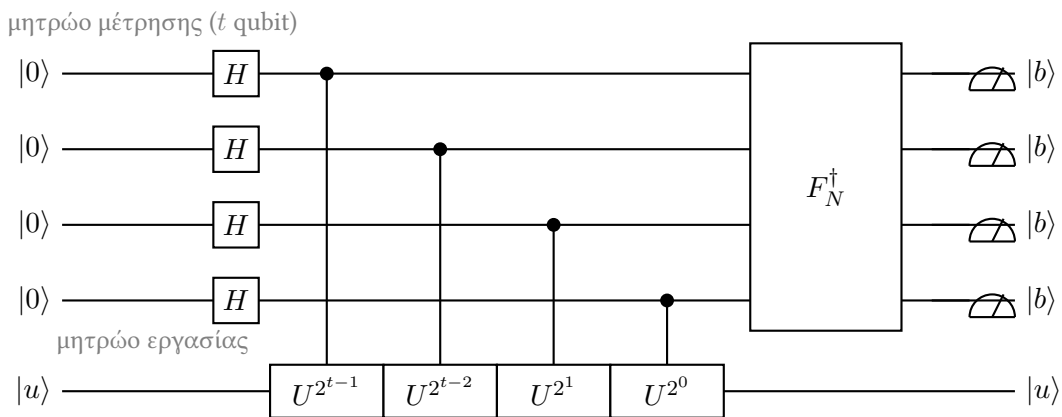
$$\hat{U} |u\rangle = e^{j2\pi\varphi} |u\rangle, \quad 0 \leq \varphi < 1. \quad (6.4)$$

(Θυμίζουμε ότι όλες οι ιδιοτιμές μοναδιαίων πυλών έχουν μονάδινο μέτρο — ενότητα 1.11· γράφουμε την ιδιοτιμή ως $e^{j2\pi\varphi}$ με τη «φάση» φ να κλιμακώνεται στο $[0, 1)$.) Το ερώτημα της εκτίμησης φάσης είναι: υποθέτοντας ότι μπορούμε να ετοιμάσουμε το $|u\rangle$ και να υλοποιήσουμε την $\hat{U}$ σε κύκλωμα, πόσο ακριβώς μπορούμε να μάθουμε τον αριθμό φ ;

Ας μη φαίνεται το πρόβλημα αφηρημένο: στον αλγόριθμο του Shor, η πύλη U θα είναι ο πολλαπλασιασμός επί x modulo n και η φάση $\varphi = s/r$ θα κρύβει την άγνωστη τάξη r του x — θα το δούμε αναλυτικά στην επόμενη ενότητα. Εδώ θα αναπτύξουμε την τεχνική γενικά, ως μαύρο κουτί.

Το κύκλωμα

Χρησιμοποιούμε δύο μητρώα: το πρώτο, που θα αποκαλούμε *μητρώο μέτρησης*, έχει t qubit και ξεκινά από το $|00 \dots 0\rangle$ · το δεύτερο, το *μητρώο εργασίας*, φιλοξενεί την ιδιοκατάσταση $|u\rangle$. Το κύκλωμα έχει τρεις φάσεις:



1. *Επικάλυψη στο μητρώο μέτρησης.* Εφαρμόζουμε H σε κάθε qubit μέτρησης (ενότητα 1.13):

$$|00 \dots 0\rangle |u\rangle \xrightarrow{\hat{H}^{\otimes t}} \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} |q\rangle |u\rangle, \quad N = 2^t.$$

2. *Ελεγχόμενες δυνάμεις της $\hat{U}$.* Το qubit μέτρησης βάρους 2^k ελέγχει την πύλη U^{2^k} , που δρα στο μητρώο εργασίας. Εδώ δρα το φαινόμενο της *αναπήδησης φάσης* (phase kickback), που συναντήσαμε ήδη στο

μαντείο του Grover (ενότητα 5.2): όταν η πύλη U^{2^k} δράσει πάνω στην ιδιοκατάσταση $|u\rangle$, το αποτέλεσμα δεν είναι μια μεταβολή του μητρώου εργασίας αλλά ένας παράγοντας φάσης που «πηδάει» πίσω στο qubit-έλεγχο:

$$|q\rangle |u\rangle \xrightarrow{\text{ελεγχόμενες } \hat{U}^{2^k}} e^{j2\pi q\varphi} |q\rangle |u\rangle.$$

Πράγματι, το qubit βάρους 2^k , αν είναι στην κατάσταση $|1\rangle$, πολλαπλασιάζει την κατάσταση με $e^{j2\pi\varphi 2^k}$. το γινόμενο των παραγόντων πάνω σε όλα τα qubit δίνει $e^{j2\pi\varphi \sum_k q_k 2^k} = e^{j2\pi q\varphi}$, αφού $\sum_k q_k 2^k = q$.

3. *Ανάγνωση με αντίστροφο QFT.* Η κατάσταση του μητρώου μέτρησης είναι πια

$$\frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{j2\pi q\varphi} |q\rangle = \hat{F}_N |N\varphi\rangle, \quad (6.5)$$

όπου το $N\varphi$ εννοούμε ως «κλασματικό δείκτη»: η σχέση προκύπτει απευθείας από τον ορισμό (6.2) (η στήλη « $N\varphi$ » του πίνακα έχει ακριβώς αυτούς τους συντελεστές). Εφαρμόζουμε τον αντίστροφο QFT $F_N^\dagger$ στο μητρώο μέτρησης και μετράμε: παίρνουμε έναν ακέραιο $b \in \{0, \dots, N-1\}$, με ελπίδα ότι $b/N \approx \varphi$.

Αξίζει να τονιστεί ένα σημείο: σε όλη τη διαδικασία το μητρώο εργασίας *παραμένει ακριβώς* στην ιδιοκατάσταση $|u\rangle$ — δεν εμπλέκεται ποτέ με το μητρώο μέτρησης. Αυτό είναι αποτέλεσμα του ότι το $|u\rangle$ είναι ιδιοκατάσταση: η επίδραση της $\hat{U}$ σε αυτό είναι καθαρά ένας αριθμός (φάση), όχι μια νέα κατάσταση.

Η ακριβής περίπτωση

Πότε λειτουργεί το κύκλωμα τέλεια; Όταν η φάση είναι ακριβώς πολλαπλάσιο του $1/N$, δηλαδή $\varphi = b/N$ για κάποιον ακέραιο $b \in \{0, 1, \dots, N-1\}$. Τότε η κατάσταση (6.5) γίνεται

$$\frac{1}{\sqrt{N}} \sum_q e^{j2\pi qb/N} |q\rangle = \hat{F}_N |b\rangle$$

— σύγκριση με τον ορισμό (6.2): πρόκειται ακριβώς για τη στήλη b του QFT. Ο αντίστροφος QFT την μετατρέπει στο $|b\rangle$ με βεβαιότητα:

Αποτέλεσμα 6.4: Εκτίμηση ακριβούς φάσης

Αν $\varphi = b/N$ με b ακέραιο στο $\{0, \dots, N-1\}$, η μέτρηση στο τέλος του κυκλώματος εκτίμησης φάσης δίνει πάντα το b , και συνεπώς ανακτά τη φάση ακριβώς: $\varphi = b/N$.

Η γενική περίπτωση

Τι γίνεται όταν το φ δεν είναι πολλαπλάσιο του $1/N$; Γράφουμε

$$\varphi = \frac{b + \varepsilon}{N}, \quad \text{με } b = \text{τον πλησιέστερο ακέραιο στο } N\varphi, \quad |\varepsilon| \leq \frac{1}{2},$$

και ελπίζουμε ότι η μέτρηση θα δει τον κοντινό ακέραιο b . Η ανάλυση (εμβάθυνση 6.2) δίνει ένα αποτέλεσμα εντυπωσιακά καλό:

Αποτέλεσμα 6.5: Πιθανότητα εκτίμησης φάσης

Η πιθανότητα η μέτρηση να δώσει τον πλησιέστερο ακέραιο b στο $N\varphi$ ικανοποιεί

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

ανεξαρτήτως του πλήθους t των qubit μέτρησης και της ίδιας της φάσης φ . Επιπλέον, η πιθανότητα συγκεντρώνεται σε λίγους ακέραιους κοντά στο $N\varphi$: η μέτρηση δίνει «σχεδόν σωστή» απάντηση με μεγάλη πιθανότητα και πολύ λάθος απάντηση με αμελητέα.

Η σταθερά $4/\pi^2 \approx 40\%$ μοιάζει μετρία, αλλά για τον σκοπό μας αρκεί περίσσια: όπως θα δούμε στην ενότητα 6.5, οι αποτυχίες της εκτίμησης φάσης *ανιχνεύονται* σε ένα απλό κλασικό βήμα επαλήθευσης, οπότε αρκεί να επαναλάβουμε τη διαδικασία έναν μικρό, τυχαίο αριθμό φορών. Επιπλέον, τρέχοντας το κύκλωμα με t qubit, το σφάλμα της εκτίμησης είναι το πολύ $1/(2N) = 2^{-t-1}$ στη φάση $\varphi = b/N$.

Εμβάθυνση 6.2: Η πιθανότητα του πλησιέστερου ακέραιου

Μετά τον αντίστροφο QFT, ο συντελεστής της κατάστασης βάσης $|b\rangle$ στο μητρώο μέτρησης είναι

$$\alpha_b = \langle b | \hat{F}_N^\dagger \hat{F}_N | N\varphi \rangle \quad \text{όπου η «στήλη } N\varphi \text{» της (6.5),}$$

δηλαδή, με τους πίνακες του QFT και του αντίστροφου του,

$$\alpha_b = \frac{1}{N} \sum_{q=0}^{N-1} e^{j2\pi q(\varphi-b/N)} = \frac{1}{N} \sum_{q=0}^{N-1} \omega^q, \quad \omega = e^{j2\pi(\varphi-b/N)} = e^{j2\pi\varepsilon/N}.$$

Πρόκειται πάλι για γεωμετρική σειρά, όπως στην απόδειξη του αποτελέσματος 6.1· εδώ όμως το $\omega^N = e^{j2\pi\varepsilon} \neq 1$ (αφού $|\varepsilon| \leq 1/2$ και, εκτός της ειδικής περίπτωσης $\varepsilon = 0$, δεν μηδενίζεται), οπότε

$$\alpha_b = \frac{1}{N} \frac{\omega^N - 1}{\omega - 1} = \frac{1}{N} \frac{e^{j2\pi\varepsilon} - e^{-j2\pi\varepsilon}}{e^{j2\pi\varepsilon/N} - e^{-j2\pi\varepsilon/N}} = \frac{1}{N} \frac{2j \sin(\pi\varepsilon)}{2j \sin(\pi\varepsilon/N)},$$

και συνεπώς

$$P(b) = |\alpha_b|^2 = \frac{\sin^2(\pi\varepsilon)}{N^2 \sin^2(\pi\varepsilon/N)}.$$

Το κλάσμα αυτό έχει το όριο 1 όταν $\varepsilon \rightarrow 0$ (συμφωνώντας με το αποτέλεσμα 6.4) και, για το φράγμα από κάτω, χρησιμοποιούμε δύο κλασικές ανισότητες της $\sin$: για $|x| \leq 1/2$ ισχύει $|\sin(\pi x)| \geq 2|x|$ (η $\sin$ μένει πάνω από τη χορδή της στο $[0, \pi/2]$) και πάντα $|\sin(\pi x)| \leq \pi|x|$. Με $x = \varepsilon$ στην πρώτη και $x = \varepsilon/N$ στη δεύτερη:

$$P(b) = \frac{\sin^2(\pi\varepsilon)}{N^2 \sin^2(\pi\varepsilon/N)} \geq \frac{4\varepsilon^2}{N^2 \pi^2 \varepsilon^2 / N^2} = \frac{4}{\pi^2}.$$

(Στην περίπτωση $\varepsilon = 0$ έχουμε $P(b) = 1$.) Η ανάλυση δείχνει επίσης ότι για ακέραιους b' μακριά από το $N\varphi$ ο παρονομαστής $\sin^2(\pi\varepsilon'/N)$ μεγαλώνει και η πιθανότητα πέφτει απότομα – η κατανομή του αποτελέσματος συγκεντρώνεται γύρω από το $N\varphi$.

Πόσα qubit μέτρησης χρειαζόμαστε;

Στην εφαρμογή μας η φάση θα είναι κλάσμα της μορφής $\varphi = s/r$ με παρονομαστή $r < n < 2^L$. Θα θέλαμε το σφάλμα $|b/N - s/r|$ να είναι αρκετά μικρό ώστε το κλάσμα s/r να είναι *απομονώσιμο* από την ακέραια μέτρηση b με καθαρά κλασικά μέσα (συνεχή κλάσματα – επόμενη ενότητα). Το κρίσιμο κατώφλι, όπως θα δούμε, είναι το $1/(2r^2)$. Επειδή το σφάλμα είναι το πολύ $1/(2N)$, αρκεί $1/(2N) \leq 1/(2r^2)$, δηλαδή $N \geq r^2$. και επειδή $r < 2^L$ είναι αρκετό να πάρουμε

Αποτέλεσμα 6.6: Επιλογή του πλήθους qubit μέτρησης

Αν η φάση είναι $\varphi = s/r$ με $0 < r \leq 2^L$, τότε η εκτίμηση φάσης με

$$t = 2L + 1$$

qubit μέτρησης δίνει, με πιθανότητα τουλάχιστον $4/\pi^2$, έναν ακέραιο b με

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

Μία τεχνική, αλλά σημαντική παρατήρηση για την πρακτικότητα του κυκλώματος: οι ελεγχόμενες πύλες

U^{2^k} δεν απαιτούν 2^k διαδοχικές εφαρμογές της U . Πρώτον, ισχύει $\hat{U}^{2^k} = (\hat{U}^{2^{k-1}})^2$, οπότε οι δυνάμεις οικοδομούνται με επαναλαμβανόμενη τετράγωνιση: $\hat{U}^2, \hat{U}^4, \hat{U}^8, \dots$ — μόνο $t - 1$ σύνθετες πύλες. Δεύτερον, και σημαντικότερο, στην εφαρμογή μας η πύλη U_x έχει τόσο ειδική δομή ώστε η «δύναμη» της να μπορεί να υλοποιηθεί απευθείας με πολυωνυμικό κόστος — το αναλύουμε στην εμφάνιση 6.4.

6.5 Η τάξη ενός αριθμού και η σύνδεσή της με την εκτίμηση φάσης

Φτάνουμε στο κεντρικό μαθηματικό αντικείμενο του αλγορίθμου του Shor. Σε αυτή την ενότητα θα ορίσουμε την *τάξη* ενός αριθμού modulo n , θα δούμε γιατί η εύρεσή της είναι κλασικά δύσκολη, και θα δείξουμε πώς ανάγεται στην εκτίμηση φάσης της προηγούμενης ενότητας — δηλαδή σε ένα αποδοτικό κβαντικό κύκλωμα. Η ύλη διασπάται σε δύο μέρη: πρώτα ένα επιτραχύ, αλλά αυστηρό, μάθημα θεωρίας αριθμών· κατόπιν η κβαντική κατασκευή.

Υπολογισμός modulo n

Γράφουμε $x \equiv y \pmod{n}$ (διαβάζεται « x σύγχρονό του y modulo n ») όταν το n διαιρεί τη διαφορά $x - y$, δηλαδή όταν τα x και y αφήνουν το ίδιο υπόλοιπο στη διαίρεση με το n . Παράδειγμα: $47 \equiv 2 \pmod{5}$, αφού $47 - 2 = 45 = 9 \cdot 5$. Ο συμβολισμός συνοδεύεται από την αντίστοιχη *πράξη*: με $xy \bmod n$ εννοούμε το υπόλοιπο του γινομένου xy στη διαίρεση με το n . π.χ. $7 \cdot 6 \bmod 15 = 42 \bmod 15 = 12$. Όλες οι πράξεις της ενότητας αυτής («πολλαπλασιασμός modulo n ») είναι στοιχειώδεις αριθμητικές πράξεις που εκτελούνται σε χρόνο πολυωνυμικό στο L .

Ο *μέγιστος κοινός διαιρέτης* $\gcd(a, b)$ δύο θετικών ακεραίων είναι, όπως γνωρίζουμε, ο μεγαλύτερος ακέραιος που διαιρεί και τους δύο. Υπολογίζεται αποδοτικά με τον *αλγόριθμο του Ευκλείδη*, που βασίζεται στην αναδρομή

$$\gcd(a, b) = \gcd(b, a \bmod b), \quad a \geq b > 0,$$

και σταματά όταν το δεύτερο όρισμα μηδενιστεί. Παράδειγμα:

$$\gcd(1071, 462) = \gcd(462, 147) = \gcd(147, 21) = \gcd(21, 0) = 21,$$

αφού $1071 = 2 \cdot 462 + 147$, $462 = 3 \cdot 147 + 21$, $147 = 7 \cdot 21 + 0$.

Αποτέλεσμα 6.7: Ο αλγόριθμος του Ευκλείδη είναι γρήγορος

Ο αλγόριθμος του Ευκλείδη τερματίζει σε $O(L)$ βήματα για εισόδους L δυαδικών ψηφίων. Συγκεκριμένα, μετά από δύο βήματα ο μικρότερος από τους δύο αριθμούς έχει τουλάχιστον μειωθεί στο μισό, οπότε το πλήθος των βημάτων είναι το πολύ $2L + 1$. (Πιο λεπτή ανάλυση δίνει το φράγμα του Lamé, $O(\log_\varphi a)$ βήματα με φ τον χρυσό αριθμό — αλλά το $O(L)$ μάς αρκεί.)

Δύο αριθμοί λέγονται *συνπαθείς* (coprime) όταν $\gcd(a, b) = 1$. Ο ορισμός κρύβει μια κρίσιμη ιδιότητα, που θα χρειαστούμε δύο φορές παρακάτω:

Εμφάνιση 6.3: Ο μέγιστος κοινός διαιρέτης ως γραμμικός συνδυασμός

Ισχυρισμός. Το $\gcd(a, b)$ είναι το μικρότερο θετικό στοιχείο του συνόλου $\{ax + by : x, y \in \mathbb{Z}\}$.

Απόδειξη. Έστω $s = ax_0 + by_0$ το μικρότερο θετικό τέτοιο στοιχείο (υπάρχει, αφού π.χ. $a \cdot 1 + b \cdot 0 = a > 0$). Κάθε κοινός διαιρέτης των a, b διαιρεί το s . Δείχνουμε ότι το s διαιρεί το a : γράφουμε τη διαίρεση με υπόλοιπο $a = qs + \rho$ με $0 \leq \rho < s$. τότε

$$\rho = a - qs = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$$

είναι κι αυτός γραμμικός συνδυασμός των a, b , και αφού $0 \leq \rho < s$ με το s ελάχιστο θετικό, πρέπει $\rho = 0$, δηλαδή $s \mid a$. Με τον ίδιο συλλογισμό $s \mid b$, οπότε το s είναι κοινός διαιρέτης που διαιρείται από κάθε κοινό διαιρέτη — άρα ο μέγιστος. ■

Συμπέρασμα (λόγος του Ευκλείδη). Αν $\gcd(a, b) = 1$ και $b \mid ac$, τότε $b \mid c$.

Απόδειξη. Από την ιδιότητα του γραμμικού συνδυασμού υπάρχουν x, y με $ax + by = 1$. πολλαπλασιάζοντας με c : $acx + bcy = c$. Το b διαιρεί και τον acx (γιατί $b \mid ac$) και το bcy , άρα διαιρεί το c . ■

Μία άμεση συνέπεια της ίδιας ιδιότητας: αν $\gcd(x, n) = 1$, υπάρχει ακέραιος y με $xy \equiv 1 \pmod{n}$ (ο «αντίστροφος» του x modulo n) – απλά λύνουμε το $xy + nw = 1$ του Bézout.

Η ομάδα $\mathbb{Z}_n^*$ και η συνάρτηση φ του Euler

Έστω n σύνθετος και περιττός. Το σύνολο

$$\mathbb{Z}_n^* = \{x \in \{1, 2, \dots, n-1\} : \gcd(x, n) = 1\}$$

είναι κλειστό ως προς τον πολλαπλασιασμό modulo n : αν $\gcd(x, n) = \gcd(y, n) = 1$, τότε και $\gcd(xy \bmod n, n) = 1$, γιατί κάθε πρώτος που διαιρεί το n δεν μπορεί να διαιρεί το γινόμενο xy . Με άλλα λόγια, το $\mathbb{Z}_n^*$ με τον πολλαπλασιασμό modulo n αποτελεί (αβελιανή) ομάδα: κάθε στοιχείο έχει αντίστροφο (πράγματι τον βρήκαμε παραπάνω). Το πλήθος των στοιχείων της ονομάζεται *συνάρτηση φ του Euler* και συμβολίζεται $\varphi(n)$. Αν $n = p_1^{a_1} \cdots p_m^{a_m}$ είναι η παραγοντοποίηση του n , τότε (χωρίς απόδειξη – είναι μια όμορφη άσκηση στοιχειώδους συνδυαστικής, βλ. και τα πρόσθετα κείμενα του μαθήματος)

$$\varphi(n) = \prod_{i=1}^m p_i^{a_i-1} (p_i - 1). \quad (6.6)$$

Παραδείγματα: $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ και $\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12$ – τα στοιχεία των $\mathbb{Z}_{15}^*$ και $\mathbb{Z}_{21}^*$ είναι οκτώ και δώδεκα αντίστοιχα.

Αποτέλεσμα 6.8: Θεώρημα του Euler

Για κάθε x με $\gcd(x, n) = 1$ ισχύει

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Απόδειξη. Θεωρούμε τον πολλαπλασιασμό επί x modulo n ως απεικόνιση του συνόλου $\mathbb{Z}_n^*$ στον εαυτό του: $y \mapsto xy \bmod n$. Η απεικόνιση είναι 1-1: αν $xy_1 \equiv xy_2 \pmod{n}$ τότε $n \mid x(y_1 - y_2)$, και επειδή $\gcd(x, n) = 1$ ο λόγος του Ευκλείδη δίνει $n \mid y_1 - y_2$, δηλαδή $y_1 = y_2$ (εντός του $\{1, \dots, n-1\}$). Σε πεπερασμένο σύνολο, μια 1-1 απεικόνιση είναι και *αντίστοιχη*: τα στοιχεία $xy \bmod n$, καθώς το y διατρέχει το $\mathbb{Z}_n^*$, είναι ακριβώς τα ίδια στοιχεία του $\mathbb{Z}_n^*$, σε άλλη σειρά. Πολλαπλασιάζοντας λοιπόν όλα τα στοιχεία της ομάδας μεταξύ τους, από τη μία πλευρά παίρνουμε $\prod_{y \in \mathbb{Z}_n^*} y$, από την άλλη

$$\prod_{y \in \mathbb{Z}_n^*} (xy \bmod n) \equiv x^{\varphi(n)} \prod_{y \in \mathbb{Z}_n^*} y \pmod{n}.$$

Το γινόμενο $\prod y$ είναι πρώτο προς το n (γινόμενο στοιχείων πρώτων προς το n), οπότε έχει αντίστροφο modulo n και απλοποιείται:

$$x^{\varphi(n)} \equiv 1 \pmod{n}. \quad \blacksquare$$

Πράγματι, για $n = 15$: $2^8 = 256 = 17 \cdot 15 + 1 \equiv 1 \pmod{15}$.

Η τάξη ενός στοιχείου

Ορίζουμε τέλος το βασικό μας αντικείμενο. Για x με $\gcd(x, n) = 1$, η *τάξη* του x modulo n είναι ο μικρότερος θετικός ακέραιος r για τον οποίο

$$x^r \equiv 1 \pmod{n}. \quad (6.7)$$

Η ύπαρξη κάποιου τέτοιου r εγγυάται από το θεώρημα του Euler ($r \leq \varphi(n)$). Η τάξη έχει και μια βαθύτερη ιδιότητα:

Αποτέλεσμα 6.9: Η τάξη διαιρεί τη φ του Euler

Για κάθε x με $\gcd(x, n) = 1$, η τάξη $r = \text{ord}_n(x)$ διαιρεί το $\varphi(n)$.

Απόδειξη. Γράφουμε τη διαίρεση με υπόλοιπο: $\varphi(n) = kr + \beta$ με $0 \leq \beta < r$. Τότε, χρησιμοποιώντας το θεώρημα του Euler και τον ορισμό της τάξης,

$$1 \equiv x^{\varphi(n)} = x^{kr+\beta} = (x^r)^k x^\beta \equiv 1^k \cdot x^\beta = x^\beta \pmod{n}.$$

Αν ήταν $\beta > 0$, θα είχαμε βρει μικρότερο θετικό εκθέτη με $x^\beta \equiv 1$, σε αντίφαση με την ελαχιστότητα του r . Άρα $\beta = 0$, δηλαδή $r \mid \varphi(n)$. ■

Παράδειγμα 6.5: Τάξεις στο $\mathbb{Z}_{15}^*$

Το $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ έχει $\varphi(15) = 8$ στοιχεία. Υπολογίζουμε τις δυνάμεις κάθε στοιχείου μέχρι να φτάσουμε στο 1:

x	δυνάμεις $x, x^2, x^3, \dots$ modulo 15	τάξη r
1	1	1
2	2, 4, 8, <u>1</u>	4
4	4, <u>1</u>	2
7	7, 4, 13, <u>1</u>	4
8	8, 4, 2, <u>1</u>	4
11	11, <u>1</u>	2
13	13, 4, 7, <u>1</u>	4
14	14, <u>1</u>	2

Πράγματι όλες οι τάξεις (1, 2, 4) διαιρούν το $\varphi(15) = 8$. Παρατηρήστε πόσο μικρό ποσοστό των εκθέτων δίνει 1: η «περίοδος» της ακολουθίας $x^k \bmod n$ μπορεί να είναι μεγάλη.

Γιατί είναι δύσκολη η εύρεση της τάξης — κλασικά;

Μοιάζει αθώο: υπολόγισε $x, x^2, x^3, \dots$ modulo n μέχρι το 1. Το πρόβλημα είναι ότι η τάξη μπορεί να είναι *εξαιρετικά μεγάλη*: modulo ένα πρώτο p , υπάρχουν στοιχεία τάξης ακριβώς $p-1$ (οι λεγόμενες πρωταρχικές ρίζες), και σε γενική περίπτωση r μπορεί να φτάσει το $\varphi(n) \approx n$. Η brute-force προσέγγιση χρειάζεται άρα $O(r) = O(n) = O(2^L)$ πολλαπλασιασμούς — εκθετικός χρόνος, ακριβώς όπως η διαίρεση δοκιμής της ενότητας 6.2. Εδώ όμως δεν υπάρχει κανένας γνωστός «Pollard» ή «GNFS»: η εύρεση τάξης είναι κλασικά *ισοδύναμη σε δυσκολία με την ίδια την παραγοντοποίηση* (ένας πολυωνυμικός αλγόριθμος για την τάξη δίνει πολυωνυμικό αλγόριθμο για την παραγοντοποίηση και αντίστροφα — θα δούμε τη μία κατεύθυνση σε λίγο). Η κβαντική λύση που ακολουθεί είναι επομένως μια πραγματικά *νέα* ιδέα, όχι μια βελτίωση κλασικής.

Ο κβαντικός τελεστής $\hat{U}_x$

Ερχόμαστε τώρα στην κβαντική κατασκευή. Δουλεύουμε με ένα *μητρώο εργασίας* L qubit, με $2^L \geq n$, του οποίου τις καταστάσεις βάσης $|y\rangle$, $y = 0, 1, \dots, 2^L - 1$, ερμηνεύουμε ως ακεραίους. Ορίζουμε τον τελεστή

$$\hat{U}_x |y\rangle = \begin{cases} |xy \bmod n\rangle, & y < n, \\ |y\rangle, & y \geq n, \end{cases} \quad (6.8)$$

όπου x ένα στοιχείο του $\mathbb{Z}_n^*$.

Ο τελεστής είναι *μοναδιαίος*. Πράγματι, ο πολλαπλασιασμός επί x είναι *μετάθεση* του συνόλου $\{0, 1, \dots, n-1\}$: τον είδαμε ήδη να είναι 1-1 στην απόδειξη του θεωρήματος του Euler (αν $xy_1 \equiv xy_2$ τότε $y_1 = y_2$, με τον λόγο του Ευκλείδη), και μια 1-1 απεικόνιση πεπερασμένου συνόλου στον εαυτό του είναι και αντίστροχη. Το $\hat{U}_x$ λοιπόν απλώς ανακατανέμει τις καταστάσεις βάσης $|y\rangle$ με $y < n$ (και αφήνει ανέπαφες τις υπόλοιπες): είναι *πίνακας μετάθεσης*, και κάθε πίνακας μετάθεσης είναι ορθογώνιος, άρα μοναδιαίος. Οι δυνάμεις του υπολογίζονται επίσης εύκολα, με επαγωγή:

$$\hat{U}_x^a |y\rangle = |x^a y \bmod n\rangle, \quad y < n. \quad (6.9)$$

Οι ιδιοκαταστάσεις $|u_s\rangle$

Το φάσμα του $\hat{U}_x$ προκύπτει από μια όμορφη κατασκευή. Θεωρούμε την «τροχιά» του 1 υπό τον πολλαπλασιασμό επί x :

$$|1\rangle, |x \bmod n\rangle, |x^2 \bmod n\rangle, \dots, |x^{r-1} \bmod n\rangle,$$

και ξανά από την αρχή ($x^r \equiv 1$). Τα r αυτά κράτη είναι διαφορετικά μεταξύ τους: αν $x^k \equiv x^{k'} \pmod{n}$ με $0 \leq k < k' < r$, τότε $x^{k'-k} \equiv 1$ με $0 < k' - k < r$, σε αντίφαση με την ελαχιστότητα της τάξης. Ο τελεστής $\hat{U}_x$ «περπατά» κυκλικά πάνω σε αυτή την τροχιά — και για κυκλικές μετατοπίσεις γνωρίζουμε την αντιμετώπιση: τις διαγωνοποιεί ο μετασχηματισμός Fourier! Ορίζουμε, για κάθε $s = 0, 1, \dots, r-1$,

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-j2\pi sk/r} |x^k \bmod n\rangle. \quad (6.10)$$

Πρόταση. Κάθε $|u_s\rangle$ είναι ιδιοκατάσταση του $\hat{U}_x$ με ιδιοτιμή $e^{j2\pi s/r}$:

$$\hat{U}_x |u_s\rangle = e^{j2\pi s/r} |u_s\rangle. \quad (6.11)$$

Απόδειξη. Εφαρμόζοντας το $\hat{U}_x$ και μετατοπίζοντας τον δείκτη του αθροίσματος ($\mu = k+1$ για $k = r-1$ χρησιμοποιούμε $x^r \equiv 1$, ώστε το $|x^r \bmod n\rangle = |1\rangle$ να «κλείνει τον κύκλο»):

$$\hat{U}_x |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-j2\pi sk/r} |x^{k+1} \bmod n\rangle = \frac{1}{\sqrt{r}} \sum_{\mu=1}^r e^{-j2\pi s(\mu-1)/r} |x^\mu \bmod n\rangle,$$

όπου στην τελευταία σύζευξη το $\mu = r$ ταυτίζεται με το $\mu = 0$. Η φάση αναλύεται ως $e^{-j2\pi s(\mu-1)/r} = e^{j2\pi s/r} e^{-j2\pi s\mu/r}$, οπότε

$$\hat{U}_x |u_s\rangle = e^{j2\pi s/r} \frac{1}{\sqrt{r}} \sum_{\mu=0}^{r-1} e^{-j2\pi s\mu/r} |x^\mu \bmod n\rangle = e^{j2\pi s/r} |u_s\rangle. \quad \blacksquare$$

Οι $|u_s\rangle$ είναι επιπλέον ορθοκανονικές: ο πίνακας μετάβασης από τη βάση $\{|x^k \bmod n\rangle\}_{k=0}^{r-1}$ στα $\{|u_s\rangle\}_{s=0}^{r-1}$ είναι ο $r \times r$ πίνακας του QFT (συζευγμένος), του οποίου τη μοναδιαιότητα αποδείξαμε στο αποτέλεσμα 6.1 — η ίδια γεωμετρική σειρά μηδενίζει όλα τα «εκτός διαγωνίου» εσωτερικά γινόμενα.

Το κόλπο: εκκίνηση από το $|1\rangle$

Μέχρι εδώ όλα φαίνονται απαιτητικά: για να τρέξουμε την εκτίμηση φάσης πρέπει να ετοιμάσουμε μια ιδιοκατάσταση $|u_s\rangle$ — αλλά η κατασκευή (6.10) προϋποθέτει ήδη τη γνώση της τάξης r , που είναι ακριβώς αυτό που ψάχνουμε! Η λύση είναι από τις πιο κομψές στιγμές του αλγορίθμου: δεν χρειάζεται κάποια συγκεκριμένη ιδιοκατάσταση, γιατί η κατάσταση εκκίνησης $|1\rangle$ είναι *ιση επικάλυψη όλων*:

Αποτέλεσμα 6.10: Το $|1\rangle$ ως επικάλυψη ιδιοκαταστάσεων

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle. \quad (6.12)$$

Απόδειξη. Αντικαθιστούμε τον ορισμό (6.10) και αντιμεταθέτουμε τα αθροίσματα:

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

Ο εσωτερικός αθροιστής είναι για άλλη μια φορά γεωμετρική σειρά: για $k = 0$ ισούται με r , ενώ για κάθε $k = 1, \dots, r-1$ μηδενίζεται (η ρίζα $e^{-j2\pi k/r}$ της μονάδας είναι $\neq 1$). Απομένει το $\frac{1}{r} \cdot r |x^0 \bmod n\rangle = |1\rangle$. $\blacksquare$

Εκτίμηση φάσης για την εύρεση τάξης

Όλα είναι πια στη θέση τους. Συνθέτουμε το κύκλωμα της ενότητας 6.4 με $\hat{U} = \hat{U}_x$ και αρχική κατάσταση εργασίας το $|1\rangle$ (που ετοιμάζεται στοιχειωδώς – ενότητα 1.13):

$$|00 \cdots 0\rangle |1\rangle \xrightarrow{\hat{H}^{\otimes t}} \frac{1}{\sqrt{N}} \sum_q |q\rangle |1\rangle \xrightarrow{\text{ελεγχ. } \hat{U}_x^{2^k}} \frac{1}{\sqrt{N}} \sum_q |q\rangle \hat{U}_x^q |1\rangle.$$

Χάρη στη σχέση (6.12), η τελευταία κατάσταση αναλύεται ως άθροισμα t -qubit «κυμάτων», ένα για κάθε $|u_s\rangle$: κάθε συνιστώσα $\frac{1}{\sqrt{r}} |u_s\rangle$ εξελίσσεται αυτόνομα και δίνει στο μητρώο μέτρησης την κατάσταση (6.5) με φάση $\varphi = s/r$. Μετά τον αντίστροφο QFT και τη μέτρηση παίρνουμε λοιπόν έναν ακέραιο b με

$$\frac{b}{N} \approx \frac{s}{r}, \quad s \text{ ομοιόμορφα τυχαίο στο } \{0, 1, \dots, r-1\},$$

με την προσέγγιση να είναι καλή (σφάλμα $\leq 1/(2N) < 1/(2r^2)$) με πιθανότητα τουλάχιστον $4/\pi^2$, όπως στο αποτέλεσμα 6.6 – θυμόμαστε επίσης ότι το $s = 0$ (πιθανότητα $1/r$) δίνει πάντα $b = 0$ και δεν μεταφέρει καμία πληροφορία.

Αξίζει μια μικρή παρατήρηση: μετά τη μέτρηση, το μητρώο εργασίας καταρρέει σε κάποια ιδιοκατάσταση $|u_s\rangle$ – όχι στο $|1\rangle$ από το οποίο ξεκινήσαμε. Δεν έχει καμία συνέπεια για τον αλγόριθμο: το μητρώο εργασίας απλώς επανεκκινείται στο $|1\rangle$ σε κάθε νέα προσπάθεια.

Συνεχή κλάσματα: από το b/N στο s/r

Μένει το κλασικό βήμα επεξεργασίας: δοθέντος του μετρημένου b (και του γνωστού $N = 2^t$), πώς ανακτάμε το κλάσμα s/r ; Η απάντηση δίνεται από ένα εργαλείο με ιστορία άνω των δύο χιλιετιών: τα *συνεχή κλάσματα*.

Κάθε πραγματικός αριθμός z αναπτύσσεται σε *συνεχές κλάσμα*

$$z = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}} =: [a_0; a_1, a_2, a_3, \dots],$$

με a_0 ακέραιο και $a_1, a_2, \dots$ θετικούς ακέραιους. Οι συντελεστές προκύπτουν επαναλαμβανόμενα: $a_0 = \lfloor z \rfloor$, μετά $z = a_0 + 1/z_1$ με $z_1 > 1$, πάλι $a_1 = \lfloor z_1 \rfloor$ κ.ο.κ. Για ρητούς αριθμούς η διαδικασία τερματίζει (το υπόλοιπο μηδενίζεται μετά από πεπερασμένα βήματα) και δίνει ένα πεπερασμένο ανάπτυγμα $[a_0; a_1, \dots, a_m]$. Περικόπτοντας το ανάπτυγμα μετά τον όρο a_i παίρνουμε τις συγκλίνουσες $p_i/q_i = [a_0; \dots, a_i]$, που προσεγγίζουν το z όλο και καλύτερα. Υπολογίζονται αναδρομικά,

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

με αρχικές τιμές $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$. Οι παρονομαστές q_i αυξάνονται αυστηρά, οπότε ένα ρητό με t δυαδικά ψηφία έχει το πολύ t συγκλίνουσες – η όλη επεξεργασία είναι γρήγορη, $O(L)$ ακεραίες πράξεις.

Το θεώρημα που κάνει τα συνεχή κλάσματα το σωστό εργαλείο για εμάς:

Αποτέλεσμα 6.11: Θεώρημα του Legendre

Αν το κλάσμα p/q (σε απλοποιημένη μορφή, $\gcd(p, q) = 1$) ικανοποιεί

$$\left| z - \frac{p}{q} \right| < \frac{1}{2q^2},$$

τότε το p/q είναι μία από τις συγκλίνουσες του z .

Η σημασία είναι προφανής στην περίπτωση μας: το αποτέλεσμα 6.6 μας εγγυάται $|b/N - s/r| < 1/(2r^2)$ — άρα, όταν η εκτίμηση φάσης πετύχει, το κλάσμα s/r (σε απλοποιημένη μορφή) είναι κατ' ανάγκη συγκλίνουσα του b/N , και επομένως ανακτήσιμο από τον κατάλογο των συγκλινουσών, που υπολογίζεται εύκολα!

Παράδειγμα 6.6: Συνεχές κλάσμα του 167/256

Ας πάρουμε $t = 8$, οπότε $N = 256$, και υποθέσουμε ότι η μέτρηση έδωσε $b = 167$. Το ανάπτυγμα υπολογίζεται με διαδοχικές διαιρέσεις:

$$\frac{167}{256} = [0; 1, 1, 1, 7, 11],$$

αφού $256 = 1 \cdot 167 + 89$, $167 = 1 \cdot 89 + 78$, $89 = 1 \cdot 78 + 11$, $78 = 7 \cdot 11 + 1$, $11 = 11 \cdot 1 + 0$. Οι συγκλίνουσες είναι

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

Αν π.χ. η πραγματική φάση ήταν $\varphi = s/r = 2/3$ (κάποια τάξη $r = 3$), παρατηρούμε ότι πράγματι $|167/256 - 2/3| = 11/768 \approx 0,014 < 1/18 = 1/(2 \cdot 3^2)$: το $2/3$ είναι η τρίτη συγκλίνουσα. Πώς θα ξέραμε ότι είναι η σωστή και όχι π.χ. το $1/2$; Δοκιμάζοντας: με $\hat{U} = \hat{U}_x$, ελέγχουμε κλασικά αν $x^3 \equiv 1 \pmod{n}$. Αυτός ο έλεγχος είναι το κλειστό του αλγορίθμου.

Αποτέλεσμα 6.12: Κβαντικός αλγόριθμος εύρεσης τάξης

Είσοδος: σύνθετο περιττό n , $x \in \mathbb{Z}_n^*$. Έξοδος: η τάξη $r = \text{ord}_n(x)$.

1. Θέσε $L = \lceil \log_2 n \rceil$, $t = 2L + 1$, $N = 2^t$. Ετοίμασε το μητρώο μέτρησης στο $|00 \dots 0\rangle$ (t qubit) και το μητρώο εργασίας στο $|1\rangle$ (L qubit).
2. Τρέξε το κύκλωμα εκτίμησης φάσης της ενότητας 6.4 με $\hat{U} = \hat{U}_x$ και μέτρησε τον ακέραιο b .
3. Υπολόγισε τις συγκλίνουσες p_i/q_i του b/N .
4. Για κάθε παρονομαστή $q_i \leq n$, με αύξουσα σειρά, έλεγξε αν $x^{q_i} \equiv 1 \pmod{n}$ (με γρήγορο υπολογισμό δυνάμεων modulo — βλ. εμβάθυνση 6.4).
5. Αν κάποια q_i περάσει τον έλεγχο, είναι η τάξη: *τέλος*. Διαφορετικά, γύρνα στο βήμα 1.

Γιατί είναι ορθός ο έλεγχος του βήματος 4; Επειδή $x^q \equiv 1 \pmod{n}$ ισχύει αν και μόνο αν $r \mid q$: κάθε αποδεκτή τιμή είναι πολλαπλάσιο του r , και το μικρότερο θετικό πολλαπλάσιο του r που μπορεί να εμφανιστεί ως παρονομαστής συγκλίνουσας είναι το ίδιο το r (οι παρονομαστές των συγκλινουσών αυξάνουν, οπότε το πρώτο αποδεκτό q_i που συναντάμε είναι και το μικρότερο). Αντίστροφα, όταν η εκτίμηση φάσης πέτυχε και το s είναι πρώτο προς το r , το κλάσμα s/r εμφανίζεται αυτούσιο στις συγκλίνουσες και ο αλγόριθμος το εντοπίζει.

Πότε αποτυγχάνει μια προσπάθεια; Σε τρεις περιπτώσεις: (α) η εκτίμηση φάσης έδωσε «κακό» b (πιθανότητα το πολύ $1 - 4/\pi^2 \approx 0,6$: οι περισσότεροι κακοί b απλώς δεν οδηγούν σε καμία αποδεκτή συγκλίνουσα). (β) $s = 0$, που δίνει $b = 0$ (πιθανότητα $1/r$). (γ) το s έχει κοινό διαιρέτη $d > 1$ με το r — τότε οι συγκλίνουσες περιέχουν το απλοποιημένο κλάσμα $\frac{s/d}{r/d}$, του οποίου ο παρονομαστής αποτυγχάνει στον έλεγχο (η πιθανότητα αυτής της περίπτωσης είναι $1 - \varphi(r)/r$: για παράδειγμα, με r πρώτο είναι μόλις $1/r$). Σε κάθε περίπτωση η αποτυχία είναι *αθόρυβη*: απλώς δεν βρίσκουμε αποδεκτή συγκλίνουσα και επαναλαμβάνουμε. Ο συνολικός αριθμός επαναλήψεων είναι της τάξης των λίγων — ουδέποτε εκθετικός.

Εμβάθυνση 6.4: Η υλοποίηση των ελεγχόμενων $U_x^{2^k}$

Τοποθετούμε επιτέλους το τελευταίο τεχνικό διακύβευμα: το κύκλωμα εκτίμησης φάσης απαιτεί τις ελεγχόμενες πύλες $U_x^{2^k}$ — και μοιάζει σαν η $U_x^{2^k}$ να χρειάζεται 2^k εφαρμογές του U_x , που θα ήταν καταστροφή (k φτάνει το $t - 1 \approx 2L$). Η λύση εκμεταλλεύεται τη δομή του τελεστή:

1. Κλασικός υπολογισμός. Ο αριθμός $c_k = x^{2^k} \pmod{n}$ υπολογίζεται κλασικά με επαναλαμβανόμενη

τετράγωνιση: $x^{2^k} = (x^{2^{k-1}})^2$, μόλις k πολλαπλασιασμοί modulo n , δηλαδή $O(L^2)$ στοιχειώδεις πράξεις ανά k και $O(L^3)$ συνολικά.

2. *Αντίστροφος πολλαπλασιασμός.* Η πύλη $U_x^{2^k} = U_{c_k}$ είναι ο πολλαπλασιασμός επί τη σταθερά c_k modulo n , και υλοποιείται *απευθείας*: σε ένα επιπλέον βοηθητικό μητρώο που ξεκινά από το $|0\rangle$, υπολογίζουμε αντιστρέψιμα το γινόμενο $c_k \cdot y \bmod n$ με κυκλώματα σχολικής αριθμητικής κόστους $O(L^2)$, σε πλήρη αναλογία με τα αντίστροφα κυκλώματα του λογικού ΚΑΙ που κατασκευάσαμε στο παράδειγμα 4.8 (ενότητα 4.4): το κύκλωμα γράφει τα «σκουπίδια» του υπολογισμού σε βοηθητικά qubit, και τα ξεγράφει στο τέλος (uncomputation), ώστε να μη μείνει καμία επαφή με το περιβάλλον.
3. Η ελεγχόμενη έκδοση προκύπτει εύκολα: όλα τα βήματα του υπολογισμού ελέγχονται από το qubit-έλεγχο.

Συνολικά: $t = O(L)$ ελεγχόμενοι πολλαπλασιασμοί των $O(L^2)$ πυλών – $O(L^3)$ πύλες για όλη την οικογένεια. Αυτή είναι η πηγή του κυβικού κόστους στον πίνακα της ενότητας 6.2.

Παράδειγμα 6.7: Εύρεση τάξης σε δράση: $n = 21, x = 2$

Παραγοντοποιούμε το $n = 21$ με την υπορουτίνα εύρεσης τάξης, για $x = 2$ (η τάξη, για έλεγχο, είναι $r = 6: 2, 4, 8, 16, 11, 1$). Το πρόγραμμα προσομοιώνει ολόκληρο το κύκλωμα εκτίμησης φάσης – $t = 2L + 1 = 11$ qubit μέτρησης και $L = 5$ qubit εργασίας, 2^{16} πλάτη συνολικά – και κατόπιν εκτελεί το κλασικό βήμα των συνεχών κλασμάτων με τον έλεγχο:

```
import functools
import math

import numpy as np

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

# Παραγοντοποίηση του n = 21 με εκτίμηση τάξης του x = 2.
n = 21
x = 2

L = math.ceil(math.log2(n)) # qubit εργασίας: 2^L = 32 >= 21
t = 2 * L + 1               # qubit μέτρησης εκτίμησης (φάσης)
N = 2 ** t                  # διάσταση μητρώου μέτρησης : 2^11 = 2048
M = 2 ** L                  # διάσταση μητρώου εργασίας : 32

# --- Οτελεστής U_x στο μητρώο εργασίας : |y> -> |x y mod n> ---
Ux = np.zeros((M, M))
for y in range(M):
    z = (x * y) % n if y < n else y
    Ux[z, y] = 1.0

# --- Προσομοίωση της εκτίμησης φάσης ---
# Κατάσταση ψ [c, w]: μητρώο μέτρησης c (t qubit) ⊗ μητρώο εργασίας w (L qubit).
psi = np.zeros((N, M), dtype=complex)
psi[0, 1] = 1.0 # |0...0> ⊗ |1>

# Hadamard σε όλα τα qubit μέτρησης (–WalshHadamard μετασχηματισμός)
H1 = np.array([[1, 1], [1, -1]]) / np.sqrt(2)
Ht = functools.reduce(np.kron, [H1] * t)
psi = Ht @ psi

# Ελεγχόμενες δυνάμεις U^{2^k}: το qubit μέτρησης βάρους 2^k ελέγχεται την U^{2^k}
for k in range(t):
    mask = (np.arange(N) >> k) & 1 == 1
```

```

U_pow = np.linalg.matrix_power(Ux, 2 ** k)
psi[mask] = psi[mask] @ U_pow.T

# Αντίστροφος QFT στομητρώομέτρησης
k_idx, p_idx = np.meshgrid(np.arange(N), np.arange(N), indexing="ij")
F = np.exp(2j * np.pi * k_idx * p_idx / N) / np.sqrt(N)
psi = F.conj().T @ psi

# Τομητρώοεργασίαςκαταρρέεισειδιοκατάσταση |u_s> καιόχι στο |1>:
# ηπιθανότητανατομετρήσουμε στο |1> είναι 1/r εδώ( 1/6).
print("Μητρώο( εργασίαςστο |1> μετάτημέτρηση ) =", np.sum(np.abs(psi[:, 1]) ** 2))

# Κατανομήτωναποτελεσμάτωνμέτρησης b
p = np.sum(np.abs(psi) ** 2, axis=1)
print("αποτελέσματα b με P > 0.5%:")
for b in np.nonzero(p > 0.005)[0]:
    print(f" b = {b:4d} P = {p[b]:.4f}")

# --- Συνεχήκλάσματα : απότο b/2^t στο s/r ---
def continued_fraction(num, den):
    a = []
    while den:
        a.append(num // den)
        num, den = den, num % den
    return a

def convergents(a):
    p_prev, p_cur = 1, a[0]
    q_prev, q_cur = 0, 1
    out = [(p_cur, q_cur)]
    for a_i in a[1:]:
        p_cur, p_prev = a_i * p_cur + p_prev, p_cur
        q_cur, q_prev = a_i * q_cur + q_prev, q_cur
        out.append((p_cur, q_cur))
    return out

def try_recover_order(b):
    # Ελέγχουμετιςπαρονομαστέςτωνσυγκλινουσώντων b/2^t ωςυποψήφιεστάξεις
    for _, q in convergents(continued_fraction(b, N)):
        if 1 <= q <= n and pow(x, q, n) == 1:
            return q
    return None

# --- Προσπάθειεςμέχριναβρεθείητάξη ---
rng = np.random.default_rng(5)
r = None
for shot in range(1, 13):
    b = int(rng.choice(N, p=p))
    q = try_recover_order(b)
    if q is not None:
        r = q
        print(f"προσπάθεια {shot:2d}: b = {b:4d} -> r = {r} επιτυχία ()")
        break
    print(f"προσπάθεια {shot:2d}: b = {b:4d} -> καμίαέγκυρητάξηνηά ( προσπάθεια)")

print("βρέθηκε ητάξη r =", r, "· επαλήθευση: 2^6 mod 21 =", pow(2, r, 21))

# --- Τελικόβήμα : απότηντάξηστουςπαράγοντεςεπόμενη ( ενότητα) ---
w = pow(x, r // 2, n)

```

```
print(f"x^(r/2) mod n = 2^{r // 2} mod 21 = {w}")
print("gcd(w - 1, n) =", math.gcd(w - 1, n), ", gcd(w + 1, n) =", math.gcd(w + 1, n))
```

Η κατανομή του αποτελέσματος μέτρησης συγκεντρώνεται σε έξι «κορυφές», στα $b \approx N \cdot s/6$ για $s = 0, 1, \dots, 5$ — ακριβώς όπως προβλέπει η θεωρία. Η τυχαία προσπάθεια μπορεί να αποτύχει (π.χ. κακό b , ή s με κοινό διαιρέτη με το 6), οπότε το πρόγραμμα επαναλαμβάνει· στο τέλος ανακτά το $r = 6$, το επαληθεύει ($2^6 \bmod 21 = 1$) και, ως προοικονομία της επόμενης ενότητας, υπολογίζει ήδη $\gcd(2^3 - 1, 21) = 7$ και $\gcd(2^3 + 1, 21) = 3$.

6.6 Παραγοντοποίηση με την τάξη ως μαύρο κουτί

Σ' αυτή την ενότητα κλείνουμε τον κύκλο: θα δείξουμε ότι, αν έχουμε στη διάθεσή μας μια αποδοτική (κλασική ή κβαντική) διαδικασία εύρεσης τάξης, τότε μπορούμε να παραγοντοποιήσουμε το n με καθαρά κλασικά βήματα πάνω σε αυτήν. Η κβαντική συμβολή του Shor είναι ακριβώς η υπορουτίνα της προηγούμενης ενότητας: όλα τα υπόλοιπα είναι στοιχειώδης —αν και εξαιρετικά έξυπνη— θεωρία αριθμών.

Μη τετριμμένες τετραγωνικές ρίζες της μονάδας

Η γέφυρα μεταξύ τάξης και παραγόντων είναι η εξής παρατήρηση. Έστω ότι βρήκαμε έναν αριθμό w με

$$w^2 \equiv 1 \pmod{n},$$

δηλαδή μια *τετραγωνική ρίζα της μονάδας modulo n* . Οι ρίζες $w = \pm 1$ υπάρχουν πάντα και δεν μας λένε τίποτα. Για σύνθετο n , όμως, μπορεί να υπάρχουν και άλλες — και τότε το n «μας δίνει» τους παράγοντές του:

Αποτέλεσμα 6.13: Μη τετριμμένες ρίζες της μονάδας αποκαλύπτουν παράγοντες

Έστω n σύνθετο περιττός και w με $w^2 \equiv 1 \pmod{n}$ αλλά $w \not\equiv \pm 1 \pmod{n}$. Τότε και τα δύο

$$\gcd(w - 1, n) \quad \text{και} \quad \gcd(w + 1, n)$$

είναι *μη τετριμμένοι* παράγοντες του n : αυστηρά μεταξύ 1 και n .

Απόδειξη. Έχουμε $n \mid w^2 - 1 = (w - 1)(w + 1)$. Θέλουμε να δείξουμε ότι ο $d = \gcd(w - 1, n)$ δεν είναι ούτε 1 ούτε n : το ίδιο επιχείρημα ισχύει για το $\gcd(w + 1, n)$.

- Αν $d = n$, τότε $n \mid w - 1$, δηλαδή $w \equiv 1 \pmod{n}$ — το αποκλείουμε εξ ορισμού.
- Αν $d = 1$, τότε τα $w - 1$ και n είναι σύντητα, και επειδή $n \mid (w - 1)(w + 1)$, ο λόγος του Ευκλείδη (εμβάθυνση 6.3) δίνει $n \mid w + 1$, δηλαδή $w \equiv -1 \pmod{n}$ — πάλι το αποκλείουμε.

Άρα $1 < d < n$, και το d διαιρεί το n — είναι γνήσιος παράγοντας. Το κομμάτι $n / \gcd(w - 1, n)$ (ή ο ανάλογος λόγος για το $w + 1$) συμπληρώνει την παραγοντοποίηση. ■

Παράδειγμα 6.8: Μια μη τετριμμένη ρίζα της μονάδας modulo 15

Ο αριθμός $w = 4$ ικανοποιεί $4^2 = 16 \equiv 1 \pmod{15}$, αλλά $4 \not\equiv \pm 1 \pmod{15}$. Πράγματι:

$$\gcd(w - 1, 15) = \gcd(3, 15) = 3, \quad \gcd(w + 1, 15) = \gcd(5, 15) = 5,$$

και $15 = 3 \cdot 5$. Μια και μόνο «καλή» τετραγωνική ρίζα της μονάδας οδηγεί σε πλήρη παραγοντοποίηση.

Από την τάξη στη ρίζα

Πώς βρίσκουμε μη τετριμμένη τετραγωνική ρίζα της μονάδας με τη βοήθεια της τάξης; Επιλέγουμε τυχαίο $x \in \mathbb{Z}_n^*$ και υπολογίζουμε τη τάξη $r = \text{ord}_n(x)$. Αν το r είναι *άρτιο*, θεωρούμε

$$w = x^{r/2} \bmod n.$$

Τότε πράγματι $w^2 = x^r \equiv 1 \pmod{n}$: το w είναι τετραγωνική ρίζα της μονάδας. Δύο είναι οι τρόποι να αποτύχουμε:

- r περιττό: δεν υπάρχει καν « $x^{r/2}$ » με αυτόν τον τρόπο — πρέπει να ξαναδιαλέξουμε x .
- $w \equiv -1 \pmod{n}$: η ρίζα που βρήκαμε είναι η τετριμμένη -1 — πάλι νέα επιλογή x .

Αξίζει να σημειωθεί ότι η περίπτωση $w \equiv +1$ δεν μπορεί να συμβεί: θα σημαίνει $x^{r/2} \equiv 1$ με $r/2 < r$, σε αντίφαση με την ελαχιστότητα της τάξης.

Ο αλγόριθμος μείωσης

Συνθέτουμε τα παραπάνω στον αλγόριθμο που ανάγει την παραγοντοποίηση στην εύρεση τάξης. Προϋποθέτουμε ότι το n είναι σύνθετο, περιττό και δεν είναι δύναμη πρώτου (και οι τρεις έλεγχοι γίνονται κλασικά σε πολυωνυμικό χρόνο: την πρωτογένεια την ξέρουμε ήδη από την ενότητα 6.2· για τις δυνάμεις πρώτων, αρκεί να ελέγξουμε αν $n = m^a$ για κάποιον ακέραιο $a \geq 2$, με δυαδική αναζήτηση στη ρίζα — το αναλυτικό επιχείρημα βρίσκεται στα πρόσθετα κείμενα του μαθήματος).

Αποτέλεσμα 6.14: Παραγοντοποίηση μέσω εύρεσης τάξης

Είσοδος: σύνθετο περιττό n που δεν είναι δύναμη πρώτου. *Υπορουτίνα:* εύρεση τάξης (π.χ. ο κβαντικός αλγόριθμος 6.12).

1. Επιλέξε τυχαίο $x \in \{2, 3, \dots, n-2\}$ και υπολογίστε $d = \gcd(x, n)$.
2. Αν $1 < d < n$: τελος — βρέθηκε παράγοντας (και τα δύο d και n/d είναι γνήσιοι). (Το $d = n$ συμβαίνει μόνο αν το x μοιράζεται όλους τους πρώτους του n — σπάνιο· απλώς επιλέξτε ξανά.)
3. Υπολογίστε τη τάξη $r = \text{ord}_n(x)$ με την υπορουτίνα.
4. Αν το r είναι περιττό, πηγαίνετε στο βήμα 1.
5. Θέστε $w = x^{r/2} \bmod n$. Αν $w \equiv n-1 \pmod{n}$, πηγαίνετε στο βήμα 1.
6. Επιστρέψτε τους παράγοντες $\gcd(w-1, n)$ και $\gcd(w+1, n)$.

Η ευτυχής συγκυρία του βήματος 2 αξίζει σχόλιο: ένα «τυχαίο» x που δεν είναι σύνθετο με το n δεν μας βοηθάει καθόλου — αλλά ένα x που είναι, μας δίνει παράγοντα δωρεάν. Στην πράξη το βήμα αυτό σπάνια πετυχαίνει (τα περισσότερα τυχαία x είναι πρώτα προς το n), αλλά δεν κόστιζει τίποτα να το ελέγξουμε.

Παράδειγμα 6.9: Παραγοντοποίηση του 15 με το χέρι

Παίρνουμε $n = 15$ και, ας πούμε, $x = 7$ (που είναι σύνθετο με το 15, οπότε το βήμα 2 αποτυγχάνει). Από τον πίνακα του παραδείγματος 6.5, η τάξη είναι $r = 4$ — άρτια. Υπολογίζουμε

$$w = 7^{4/2} \bmod 15 = 7^2 \bmod 15 = 49 \bmod 15 = 4,$$

και ελέγχουμε: $4 \not\equiv \pm 1 \pmod{15}$, οπότε δεν είμαστε σε αποτυχία. Κατά συνέπεια

$$\gcd(4-1, 15) = 3, \quad \gcd(4+1, 15) = 5,$$

και η παραγοντοποίηση $15 = 3 \cdot 5$ ολοκληρώθηκε — έχοντας καλέσει την υπορουτίνα εύρεσης τάξης μία φορά. (Για εξάσκηση: δοκιμάστε και άλλα x από τον πίνακα του παραδείγματος 6.5. Θα διαπιστώσετε ότι μόνο το $x = 1$, που έχει περιττή τάξη, και το $x = 14$, για το οποίο $w = 14 \equiv -1$, οδηγούν σε αποτυχία· τα υπόλοιπα έξι στοιχεία του $\mathbb{Z}_{15}^*$ παραγοντοποιούν αμέσως το 15.)

Πόσο συχνά πετυχαίνει ο αλγόριθμος;

Το κρίσιμο ερώτημα: αν διαλέξουμε τυχαίο x , με ποια πιθανότητα η διαδρομή «άρτια τάξη και $w \not\equiv -1$ » οδηγεί σε επιτυχία; Η απάντηση εξαρτάται από τον αριθμό των διαφορετικών πρώτων παραγόντων του n · γράφουμε $n = p_1^{a_1} \cdots p_m^{a_m}$.

Αποτέλεσμα 6.15: Πιθανότητα επιτυχίας της μείωσης

Για τυχαίο ομοιόμορφο $x \in \mathbb{Z}_n^*$, η πιθανότητα να ισχύει ταυτόχρονα «το $r = \text{ord}_n(x)$ άρτιο» και « $x^{r/2} \not\equiv -1 \pmod{n}$ » ικανοποιεί

$$P \geq 1 - \frac{1}{2^{m-1}} \geq \frac{1}{2}, \quad m = \text{πλήθος διαφορετικών πρώτων του } n.$$

Στην κρυπτογραφικά ενδιαφέρουσα περίπτωση $n = pq$ (δύο πρώτοι): $P \geq 1/2$.

Οπότε ο αλγόριθμος 6.14, σε κάθε γύρο, πετυχαίνει με πιθανότητα τουλάχιστον $1/2$ (πολλαπλασιασμένη με τη σταθερή πιθανότητα επιτυχίας της ίδιας της εύρεσης τάξης): ο αναμενόμενος αριθμός επαναλήψεων είναι σταθερός — λίγες προσπάθειες αρκούν, και το κόστος κάθε γύρου είναι το κόστος μιας κλήσης της υπορουτίνας εύρεσης τάξης επί μια σταθερά.

Εμβάθυνση 6.5: Γιατί $P \geq 1/2$ όταν $n = pq$: η απόδειξη

Αποδεικνύουμε το φράγμα για $n = pq$ (η γενική περίπτωση $m > 2$ προκύπτει με τον ίδιο τρόπο, και το φράγμα $1 - 1/2^{m-1}$ σφίγγει). Η σκέψη έχει τρία βήματα.

Βήμα 1: ανεξάρτητες συνιστώσες. Η συμπεριφορά του x modulo το p και modulo το q είναι ανεξάρτητη: καθώς το x διατρέχει ομοιόμορφα το $\mathbb{Z}_n^*$, το ζεύγος $(x \bmod p, x \bmod q)$ διατρέχει ομοιόμορφα όλα τα ζεύγη του $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ (αυτό είναι ουσία του κινεζικού θεωρήματος υπολοίπων· το παραθέτουμε χωρίς απόδειξη). Συνεπώς μπορούμε να αναλύσουμε ξεχωριστά το x ως στοιχείο του $\mathbb{Z}_p^*$ και του $\mathbb{Z}_q^*$.

Βήμα 2: κριτήριο αποτυχίας. Έστω $r_p = \text{ord}_p(x)$, $r_q = \text{ord}_q(x)$ οι «τοπικές» τάξεις. Επειδή $x^k \equiv 1 \pmod{n}$ ισχύει αν και μόνο αν ισχύει και modulo p και modulo q , η συνολική τάξη είναι

$$r = \text{lcm}(r_p, r_q).$$

Η αποτυχία σημαίνει: ή r περιττό, ή $x^{r/2} \equiv -1$. Γράφουμε $v_2(m)$ για τη μέγιστη δύναμη του 2 που διαιρεί έναν ακέραιο m (π.χ. $v_2(12) = 2$, αφού $4 \mid 12$ αλλά $8 \nmid 12$). Τότε:

- r περιττό $\iff v_2(r_p) = v_2(r_q) = 0$.
- $x^{r/2} \equiv -1 \pmod{n} \iff x^{r/2} \equiv -1$ και modulo p και modulo $q \iff$ ούτε η τάξη r_p ούτε η r_q διαιρεί το $r/2 \iff v_2(r_p) = v_2(r) = v_2(r_q) - \text{με άλλα λόγια, οι δυνάμεις του 2 στις δύο τοπικές τάξεις είναι ίσες (και ίσες με τη μέγιστη τους, που είναι του } r).$

Συνοψίζοντας: αποτυχία $\iff v_2(r_p) = v_2(r_q)$.

Βήμα 3: πιθανότητα ισότητας. Η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική τάξης $p-1$ (την απόδειξη θα βρείτε στα πρόσθετα κείμενα): υπάρχει «γεννήτορας» g τέτοιος ώστε κάθε στοιχείο γράφεται $x = g^k$ με μοναδικό k modulo $p-1$. Για τυχαίο x , ο εκθέτης k είναι ομοιόμορφος. Αν $p-1 = 2^d \cdot$ (περιττό), τότε η τοπική τάξη του $x = g^k$ έχει $v_2(r_p) = d - v_2(k)$ (με την κατανόηση ότι εκθέτες k με $v_2(k) \geq d$ δίνουν $v_2(r_p) = 0$). Ακριβώς οι μισοί εκθέτες είναι περιττοί (k περιττό), οπότε

$$\Pr[v_2(r_p) = v_2(p-1)] = \frac{1}{2}, \quad \Pr[v_2(r_p) < v_2(p-1)] = \frac{1}{2}.$$

Έστω τώρα $P_p(j) = \Pr[v_2(r_p) = j]$ η κατανομή για το p και $P_q(j)$ για το q . Η πιθανότητα αποτυχίας είναι $\sum_j P_p(j)P_q(j)$. Το κόλπο: η κατανομή P_p έχει μέγιστη τιμή $1/2$ (στο $j = v_2(p-1)$), και το υπόλοιπο μισό της μάζας είναι απλωμένο σε μικρότερα j : για οποιαδήποτε τέτοια κατανομή ισχύει $\sum_j P_p(j)^2 \leq \frac{1}{4} + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$ (η τετραγωνική μάζα των «άλλων» τιμών είναι το πολύ το τετράγωνο του αθροίσματός τους). Με την ανισότητα Cauchy–Schwarz:

$$\Pr[\text{αποτυχία}] = \sum_j P_p(j)P_q(j) \leq \sqrt{\sum_j P_p(j)^2} \sqrt{\sum_j P_q(j)^2} \leq \frac{1}{2}.$$

Άρα $P \geq 1/2$. Το φράγμα είναι σφιχτό: για $n = 21 = 3 \cdot 7$, όπου $v_2(2) = v_2(6) = 1$, η ακριβής πιθανότητα επιτυχίας είναι $6/12 = 1/2$ (ο αναγνώστης μπορεί να το επαληθεύσει αριθμητικά από τον

πίνακα των τάξεων του $\mathbb{Z}_{21}^*$). Για $n = 15 = 3 \cdot 5$, όπου $v_2(2) = 1$ αλλά $v_2(4) = 2$, η πιθανότητα ανεβαίνει στο $6/8 = 3/4$, όπως είδαμε στο παράδειγμα 6.9.

6.7 Σύνοψη: ο πλήρης αλγόριθμος του Shor

Όλα τα κομμάτια είναι έτοιμα — ας τα βάλουμε στη σειρά.

Αποτέλεσμα 6.16: Ο αλγόριθμος του Shor

Είσοδος: σύνθετος ακέραιος n (L δυαδικά ψηφία). *Έξοδος:* ένας μη τετριμμένος παράγοντας του n .

1. *Κλασικοί έλεγχοι.* Αν το n είναι άρτιο, επιστρέψε τον παράγοντα 2. Αν το n είναι πρώτος ή δύναμη πρώτου, χειρίσου κλασικά (πρώτος: δεν υπάρχει παράγοντας· δύναμη πρώτου: δυαδική αναζήτηση στη ρίζα). Επιλέξε τυχαίο $x \in \{2, \dots, n-2\}$ και υπολόγισε $d = \gcd(x, n)$. αν $1 < d < n$, επιστρέψε το d .
2. *Κβαντικό βήμα (εύρεση τάξης).* Ετοίμασε $t = 2L + 1$ qubit μέτρησης στο $|00 \dots 0\rangle$ και L qubit εργασίας στο $|1\rangle$. Εφάρμοσε Hadamard σε όλα τα qubit μέτρησης, κατόπιν τις ελεγχόμενες πύλες $U_x^{2^k}$ (υλοποιημένες ως πολλαπλασιασμοί επί των κλασικά υπολογισμένων $x^{2^k} \bmod n$ — εμβάθυνση 6.4), κατόπιν τον αντίστροφο QFT $F_N^\dagger$ στο μητρώο μέτρησης. Μέτρησε τον ακέραιο b .
3. *Κλασική επεξεργασία.* Υπολόγισε τις συγκλίνουσες του b/N · για τις παρονομαστές $q \leq n$ έλεγξε αν $x^q \equiv 1 \pmod{n}$. Βρήκες τάξη r ; Συνέχισε· διαφορετικά γύρνα στο βήμα 2.
4. *Από την τάξη στους παράγοντες.* Αν το r είναι περιττό ή $x^{r/2} \equiv -1 \pmod{n}$, γύρνα στο βήμα 1. Διαφορετικά, υπολόγισε $w = x^{r/2} \bmod n$ και επιστρέψε τους παράγοντες $\gcd(w-1, n)$ και $\gcd(w+1, n)$.

Πολυπλοκότητα

Μετράμε τις πύλες του κβαντικού βήματος ως συνάρτηση του L . Το πιο ακριβό μέρος είναι οι ελεγχόμενοι πολλαπλασιασμοί modulo n : $t = 2L+1$ από αυτούς, ο καθένας κόστους $O(L^2)$ πυλών, άρα $O(L^3)$ συνολικά. Ο αντίστροφος QFT σε $t = O(L)$ qubit κοστίζει $O(L^2)$ πύλες — αμελητέο μπροστά στο προηγούμενο. Τα κλασικά βήματα (Ευκλείδης, συνεχή κλάσματα, δυνάμεις modulo) είναι όλα πολυωνμικά, με το βήμα των συνεχών κλασμάτων να κυριαρχεί σε $O(L^3)$ στοιχειώδεις πράξεις, και επαναλαμβάνονται κατά προσέγγιση σταθερό πλήθος φορές (τυχαιότητα των βημάτων 1–4). Συνολικά:

Συστατικό	Κόστος
Ελεγχόμενοι πολλαπλασιασμοί modulo n	$O(L^3)$ πύλες
Αντίστροφος QFT ($t = 2L + 1$ qubit)	$O(L^2)$ πύλες
Συνεχή κλάσματα + έλεγχοι	$O(L^3)$ κλασικές πράξεις
Επαναλήψεις (αναμενόμενες)	$O(1)$

Το συνολικό κόστος είναι άρα πολυωνμικό, της τάξης των $O(L^3)$. Για σύγκριση, ο καλύτερος κλασικός αλγόριθμος έχει υποεκθετικό κόστος $\exp(O(L^{1/3}(\log L)^{2/3}))$: για το RSA-2048 ($L = 2048$), ο Shor απαιτεί της τάξης 10^{10} πύλες — τεράστιο αλλά *μη* εκθετικό νούμερο — ενώ ο GNFS απαιτεί της τάξης 10^{20} πράξεις. Η διαφορά μεγαλώνει δραματικά με το L , όπως είδαμε στην εμβάθυνση 6.1.

Το ηθικό της ιστορίας

Ας αποτιμήσουμε τι μάθαμε, γιατί το μάθημα ξεπερνά το συγκεκριμένο πρόβλημα:

- Η δύναμη βρίσκεται στη δομή, όχι στην ταχύτητα. Ο QFT δεν είναι «γρήγορο DFT»· είναι ένα εργαλείο που αναγνωρίζει περιοδικότητες κωδικοποιημένες σε φάσεις. Η περιοδικότητα της ακολουθίας $x^k \bmod n$ είναι το «κρυφό μοτίβο» που κρύβει τους παράγοντες του n — και το κβαντικό κύκλωμα το ανιχνεύει σε έναν υπολογισμό.

- Η κβαντική συνεισφορά είναι ένα ακριβώς βήμα. Όλος ο υπολογισμός —έλεγχοι, τυχαίες επιλογές, Ευκλείδης, συνεχή κλάσματα— είναι κλασικός· το κβαντικό βήμα είναι μία μόνο, εύστοχα σχεδιασμένη επέμβαση: η εκτίμηση φάσης. Αυτό είναι το γενικό σχήμα των περισσότερων γνωστών κβαντικών αλγορίθμων με εκθετική επιτάχυνση.
- Οι αποτυχίες είναι φιλικές. Ό,τι δεν πετυχαίνει (κακό b , περιττό r , $w \equiv -1$) απλώς ανιχνεύεται και επαναλαμβάνεται — τυχαία επιλογή x με σταθερή πιθανότητα επιτυχίας ανά γύρο.

Ο αλγόριθμος του Shor παραμένει η σημαντικότερη θεωρητική απόδειξη ότι η κβαντική υπολογιστική δεν είναι απλώς μια εναλλακτική τεχνολογία, αλλά μια διαφορετική μαθηματική πραγματικότητα για ορισμένα προβλήματα. Η πρακτική του αξιοποίηση απαιτεί κβαντικούς υπολογιστές με εκατομμύρια φυσικά qubit (λόγω των σημερινών ποσοστών σφάλματος, κάθε λογικό qubit χρειάζεται κώδικα διόρθωσης λαθών με πολλαπλάσια αντίγραφα) — μια πρόκληση μηχανικής που παραμένει ανοιχτή, αλλά στην οποία έχει σημειωθεί συνεχής πρόοδος από τα πρώτα πειράματα two-qubit της δεκαετίας του 1990 μέχρι τους σημερινούς επεξεργαστές εκατοντάδων qubit.

Σύνοψη Ενότητας

Το πρόβλημα. Παραγοντοποίηση μεγάλων σύνθετων n : κλασικά καλύτερο γνωστό κόστος υποεκθετικό $\exp(O(L^{1/3}(\log L)^{2/3}))$ · κβαντικά $O(L^3)$ (Shor, 1994).

Ο QFT (ενότητα 6.3): πύλη $\hat{F}_N |p\rangle = \frac{1}{\sqrt{N}} \sum_k e^{j2\pi kp/N} |k\rangle$, μοναδιαία (γεωμετρικές σειρές). Ο τύπος γινομένου (6.3) δίνει κύκλωμα n Hadamard + $\binom{n}{2}$ ελεγχόμενες φάσεις $R_\nu + \lfloor n/2 \rfloor$ SWAP: $O(n^2)$ πύλες, εκθετικά λιγότερες από τον κλασικό FFT ($O(2^n n)$).

Εκτίμηση φάσης (ενότητα 6.4): για $\hat{U} |u\rangle = e^{j2\pi\varphi} |u\rangle$, το κύκλωμα «Hadamard $\rightarrow$ ελεγχόμενες $U^{2^k} \rightarrow$ αντίστροφος QFT $\rightarrow$ μέτρηση» δίνει b με $b/N \approx \varphi$ · με $t = 2L + 1$ qubit και $\varphi = s/r$, $r \leq 2^L$: σφάλμα $< 1/(2r^2)$ με πιθανότητα $\geq 4/\pi^2$.

Τάξη (ενότητα 6.5): $r = \text{ord}_n(x)$, ο μικρότερος θετικός με $x^r \equiv 1 \pmod{n}$ · διαιρεί το $\varphi(n)$. Ο τελεστής $\hat{U}_x |y\rangle = |xy \bmod n\rangle$ (μετάθεση, άρα μοναδιαίος) έχει ιδιοκαταστάσεις $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_k e^{-j2\pi sk/r} |x^k \bmod n\rangle$ με ιδιοτιμές $e^{j2\pi s/r}$, και το $|1\rangle = \frac{1}{\sqrt{r}} \sum_s |u_s\rangle$: εκτίμηση φάσης στο $|1\rangle$ δίνει $b \approx N \cdot s/r$. Συνεχή κλάσματα + έλεγχος $x^q \equiv 1$ ανακτούν το r .

Από την τάξη στους παράγοντες (ενότητα 6.6): αν r άρτια και $w = x^{r/2} \not\equiv -1$, τότε $w^2 \equiv 1$ μη τετριμμένα και $\gcd(w \mp 1, n)$ είναι παράγοντες. Επιτυχία τυχαίου x με πιθανότητα $\geq 1 - 1/2^{m-1} \geq 1/2$.

Συνολικά (ενότητα 6.7): κλασικοί έλεγχοι $\rightarrow$ κβαντική εύρεση τάξης $\rightarrow$ κλασική ανακάλυψη παραγόντων· κόστος $O(L^3)$.