30/3/2019

Κβαντική Τεχνολογία

Ο κβαντικός μετασχηματισμός Fourier και ο αλγόριθμος του Shor.

Περιεχόμενα:

1) Εισαγωγή:

Ο αλγόριθμος του Shor, είναι ένας κβαντικός αλγόριθμος, δηλαδή ένας αλγόριθμος, ο οποίος τρέχει σε έναν κβαντικό υπολογιστή, με σκοπό την παραγοντοποίηση ακεραίων αριθμών. Φέρει το όνομα του από τον από τον μαθηματικό Peter Shor, ο οποίος «εμπνεύστηκε» τον αλγόριθμο με σκοπό να λύσει το εξής πρόβλημα:

«Δεδομένου ενός ακέραιου αριθμού N, να βρεθούν οι πρώτοι παράγοντες αυτού του αριθμού».

Σε έναν κλασσικό υπολογιστή, ο αλγόριθμος παραγοντοποίησης τρέχει σε εκθετικό χρόνο(συγκεκριμένα $\boldsymbol{O}(\boldsymbol{e}^{\boldsymbol{1.9}(\boldsymbol{logN})^{\frac{\boldsymbol{1}}{\boldsymbol{3}}}(\boldsymbol{loglogN})^{\frac{\boldsymbol{2}}{\boldsymbol{3}}}})$, σε αντίθεση με τον κβαντικό υπολογιστή, όπου η πολυπλοκότητα είναι $\boldsymbol{O}((\boldsymbol{logN})^{\boldsymbol{2}}(\boldsymbol{loglogN})(\boldsymbol{loglog\ logN}))$**.** Παρατηρείτε λοιπόν, ότι για να τρέξει ο κβαντικός αλγόριθμος, απαιτείται σημαντικά λιγότερος χρόνος.

2) Μαθηματικά εργαλεία:

2.1) *Ευκλείδειος αλγόριθμος για εύρεση μέγιστου κοινού διαιρέτη.*

Έχοντας 2 αριθμούς x,y θέλουμε να βρούμε το Μέγιστο κοινό διαιρέτη αυτών. Ο αλγόριθμος του Ευκλείδη έχει ως εξής:

1. Αν ένα από τα x,y είναι ίσο με μηδέν, τέλος αλγορίθμου.
2. Όσο ο y είναι διάφορος του μηδενός, διαιρούμε τον x με τον y.
3. Παράλληλα σε κάθε βήμα αναθέτουμε το y στο x και το x mod y στο y.
4. Όταν y = 0, τότε επιστρέφουμε τον x σαν ΜΚΔ.

2.2) *Order finding problem.*

Έστω x και N θετικοί αριθμοί χωρίς κάποιο κοινό παράγοντα και τέτοιοι ώστε: x < N. Η τάξη (order) του x είναι ο μικρότερος ακέραιος r τέτοιος ώστε: $x^r = 1 \bmod N$.

Σε αυτό το σημείο, με τη χρήση ενός παραδείγματος θα εξηγηθεί πως γίνεται η modular αριθμητική.

Αρχικά, επιλέγουμε δυο αριθμούς, οι οποίοι δεν έχουν κανέναν κοινό παράγοντα, καθώς ο ΜΚΔ τους είναι το ένα. Έστω επιλέγουμε τους αριθμού x = 5 και N = 44. Για να υπολογιστεί το : $x^r = a \bmod N$, υπολογίζουμε το x^r και αφαιρούμε το N, μέχρι να παρθεί ο τελευταίος ακέραιος μεγαλύτερος του μηδενός. Οι περιπτώσεις όπου $N > x^r$ για κάποιο r, δεν λαμβάνονται υπόψη.

Παράδειγμα:

1**) $5^1 = 5$, $5^2 = 25 < 44$,** (δεν λαμβάνονται υπόψη).

2) **$5^3 = 125 > 44$**, άρα 125 – 44 = 81 > 44 (συνεχίζω)

81 – 44 = 37 < 44. (τέλος)

Τελικά, **$5^3 = 37 \pmod{44}$**.

3) **$5^4 = 625$.** Επαναλαμβάνοντας την ίδια διαδικασία με προηγουμένως θα πάρουμε ότι

$5^4 = 9 \pmod{44}$.

4) Ίδια διαδικασία επαναλαμβάνεται και για το **$5^5 = 3125$.** Μετά από μια σειρά πράξεων θα καταλήξουμε ότι 71 x 44 =3124. Έτσι έχουμε, $5^5 – 71 \times 44 = 1$, όπου και είναι ο αριθμός στον οποίο τερματίζει ο αλγόριθμος μας.

Τελικά έχουμε, **$5^5 = 1 \pmod{44}$,** δηλαδή r = 5.

2.3) *Κβαντικός μετασχηματισμός Fourier (QFT).*

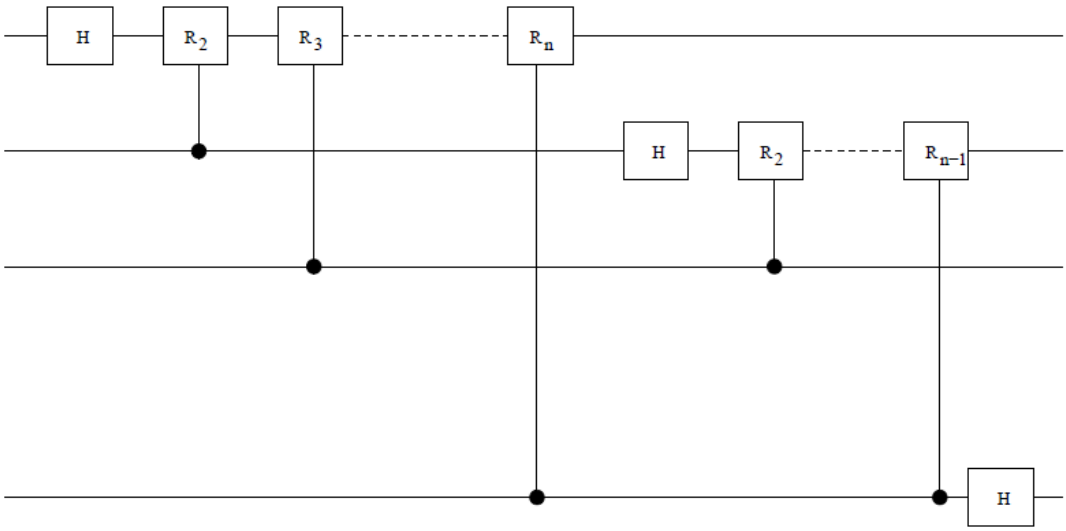
Έχουμε την ακόλουθη βάση: {|x>} = {|0> , …, |q – 1>} .

Ο κβαντικός μετασχηματισμός Fourier μετατρέπει το |x> ως εξής:

$$|x\rangle \xrightarrow{QFT} \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} exp\left\{\frac{2\pi i}{q} xy\right\}|y\rangle$$

Στη γενική του μορφή: $|\Psi\rangle = \sum_x a_x|x\rangle$:

$QFT(|\Psi\rangle) = \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \beta_y|y\rangle$, όπου β_y οι διακριτοί μετασχηματισμοί Fourier του πλάτους α_x .



Κύκλωμα υλοποίησης Κβαντικού μετασχηματισμού Fourier.

Δηλαδή, ο QFT μετασχηματίζει μια βασική κατάσταση ενός κβαντικού καταχωρητή σε υπέρθεση όλων των βασικών καταστάσεων, όπου όλες οι καταστάσεις έχουν το ίδιο πλάτος άλλα διαφορετικές φάσεις.

2.4) Αλγόριθμος εύρεσης περιόδου.

- Δεδομένου μιας περιοδικής συνάρτησης f : {0, … , q-1} -> {0, … , q-1}, όπου q = 2^l.

Οι περιοδικές συνθήκες είναι:

$$f(a) = f(a + r), r \neq 0$$

$$f(a) \neq f(a + s)\ \forall s < r.$$

- Το κύκλωμα αρχικοποιείται με τη κατάσταση $|\Phi_I\rangle = |0\rangle^{\otimes 2l}$
- Στη συνέχεια εφαρμόζονται πύλες Hadamard στα πρώτα l qubits και ο Identity πίνακας στα υπόλοιπα.

$$|\Phi_0\rangle = H^{\otimes l} \otimes I^{\otimes l} |0\rangle^{\otimes 2l} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes l} \otimes |0\rangle^{\otimes l} = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1} |a\rangle|0\rangle^{\otimes l}$$

- Εφαρμόζεται η συνάρτηση *f*, στη προκειμένη περίπτωση $f = x^a \bmod n$

  $$|\Phi_1\rangle = U_f |\Phi_0\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|f(a)\rangle$$
- Αν γίνει κάποια μέτρηση στο *f*(a), τότε η κατάσταση στην οποία θα βρίσκονται τα πρώτα l qubits θα είναι:

  $$|\Phi_1\rangle_z = \sqrt{\frac{r}{q}}\sum_{a:f(a)=z} |a\rangle.$$
- Επειδή *f* περιοδική συνάρτηση, επιλέγουμε $a_0 = \min\{a | f(a) = z\}$, και ξαναγράφουμε την προηγούμενη εξίσωση.

  $|\Phi_1\rangle_z = \frac{\sqrt{r}}{\sqrt{q}}\sum_{t=0}^{\frac{q}{r}-1} |a_0 + tr\rangle$, θεωρώντας ότι το r διαιρεί το q (δηλ. r|q).
- Στη συνέχεια, εφαρμόζεται QFT.

  $$|\widetilde{\Phi}\rangle_z = \sqrt{\frac{r}{q}}\sum_{t=0}^{\frac{q}{r}-1}\frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} exp\left(\frac{-2\pi i}{q}(a_0 + rt)c\right)|c\rangle = \sqrt{\frac{r}{q^2}}\sum_{c=0}^{q-1} exp\left(\frac{-2\pi i}{q}a_0 c\right)\sum_{t=0}^{\frac{q}{r}-1} exp\left(\frac{-2\pi i}{q1}trc\right)|c\rangle$$
- Η πιθανότητα υπολογισμού ενός c' = kq/r για κάποιο $k \in \mathbb{N}$ είναι:

  $$P[\acute{c}] = \left|\langle c'|\widetilde{\Phi}\rangle\right|^2$$
- Η συνολική πιθανότητα να μετρηθεί ένα c της μορφής kq/r είναι:

  $$\sum_{c=kq/r}\left|\langle c'|\widetilde{\Phi}\rangle\right|^2$$

Το αποτέλεσμα του αλγορίθμου είναι ένας φυσικός αριθμός της μορφής kq/r, με $k \in \mathbb{N}$

2.5) *Συνεχής επέκταση κλασμάτων.*

$$[a_0, a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots}}}$$

Παράδειγμα:

$$\frac{13}{64} = \frac{1}{\frac{64}{13}} = \frac{1}{4+\frac{12}{13}} = \frac{1}{4+\frac{1}{\frac{13}{12}}} = \frac{1}{4+\frac{1}{1+\frac{1}{12}}} \approx \frac{1}{5}$$

($d_0 = a_0$, $d_1 = 1 + a_0a_1$, $d_n = a_nd_{n-1} + d_{n-2}$, $r_0 = 1$, $r_1 = a_1$, $r_n = a_nr_{n-1} + r_{n-2}$).

3) Ανάλυση του αλγορίθμου του Shor:

3.1) Περιγραφή:

Παρακάτω παρουσιάζονται τα βήματα για τον Αλγόριθμο του Shor.

3.1.1) Κλασσικό μέρος

1. Καθορισμός ακεραίου αριθμού n. Αν n άρτιος αριθμός, πρώτος ή πρώτος αριθμός σε δύναμη, τότε ο αλγόριθμος τερματίζεται. Διαφορετικά, συνεχίζουμε στο βήμα 2.
2. Τυχαία επιλογή ενός ακεραίου x < n. Αφού επιλεχτεί ο τυχαίος αριθμός υπολογίζεται με τη βοήθεια του Ευκλείδειου αλγορίθμου ο ΜΚΔ. Αν, ΜΚΔ(x,n) = 1, τότε έχουμε βρει έναν παράγοντα του n.

Σε αυτό το σημείο, το κλασσικό κομμάτι του αλγορίθμου ολοκληρώθηκε και «αναλαμβάνει» η κβαντική φύση του αλγορίθμου.

3.1.2) Κβαντικό μέρος

1. Επιλέγεται q, το οποίο είναι η μικρότερη δύναμη του 2, με $n^2 \leq q \leq 2n^2$.
2. Χρησιμοποιείται κβαντικός παραλληλισμός για να υπολογιστεί το x^a για όλα τα a ταυτόχρονα.
3. Βρίσκεται η περίοδος r, του x^a (mod n).
4. Κάνοντας μέτρηση βρίσκεται μια μεταβλητή c, η οποία έχει την ιδιότητα: $\frac{c}{q} \approx \frac{d}{r}$, όπου d ανήκει στο σύνολο των φυσικών αριθμών.
5. Καθορισμός των d, r μέσω της συνεχής επέκτασης κλασμάτων. Τα d, r καθορίζονται εφόσον ΜΚΔ(d,r) = 1.
6. Σε περίπτωση που η περίοδος r είναι περιττός αριθμός, τότε επιστρέφουμε πίσω στο βήμα 2. Εάν πάλι $x^{r/2} = -1 \bmod n$, επιστρέφουμε στο βήμα 2. Διαφορετικά οι παράγοντες είναι οι p,q = ΜΚΔ($x^{r/2} \pm 1$,n).

3.2) Παράδειγμα - Εφαρμογή:

Θα δοκιμάσουμε να εφαρμόσουμε τον αλγόριθμο του Shor κάνοντας παραγοντοποίηση τον αριθμό 21. Συνολικά, όπως αναφέρθηκε, πρέπει να πραγματοποιηθούν 8 βήματα.

1. Επιλογή του x.
2. Καθορισμός του q.
3. Αρχικοποίηση του 1ου «καταχωρητή» (r_1).

4. Αρχικοποίηση του 1ου «καταχωρητή» (r_2).
5. Εφαρμογή του Κβαντικού μετασχηματισμού Fourier στο 1ο καταχωρητή.
6. Μέτρηση.
7. Εφαρμογή της μεθόδου συνεχής επέκτασης κλασμάτων για καθορισμό της περιόδου r.
8. Έλεγχος του r και καθορισμός των παραγόντων.

1)Τυχαία επιλογή ακεραίου x, 1 < x < n.

Αν ο αριθμός δεν είναι πρώτος με το 21, όπως για παράδειγμα το 6, τότε:

gcd(x, n) = gcd(6, 21) = 3 -> 21/3 = 7.

Και αυτό είναι και το τέλος του αλγορίθμου.

Αν όμως, x, n δεν είναι πρώτοι μεταξύ τους, πχ x = 11, τότε συνεχίζουμε στο επόμενο βήμα:

gcd(11, 21) = 1.

2)Καθορισμός του q.

$n^2 = 441 \leq q = 2^l < 2\ n^2 = 882$.

Άρα, $q = 512 = 2^9$.

Επιπλέον, βρέθηκε ότι η αρχική κατάσταση αποτελείται από δυο καταχωρητές μήκους l: $|\Phi_i\rangle = |0\rangle_{r_1}|0\rangle_{r_2} = |0\rangle^{\otimes 2^l}$

3)Αρχικοποίηση του r_1.

Αρχικοποίηση του 1ου καταχωρητή με την υπέρθεση όλων των καταστάσεων a(mod q):

$$|\Phi_0\rangle = \frac{1}{\sqrt{512}}\sum_{a=0}^{511}|a\rangle|0\rangle$$

Η οποία είναι Hadamard gate επί όλων των bit.

4)Αρχικοποίηση του r_2.

Αρχικοποίηση του 2ου καταχωρητή με την υπέρθεση όλων των καταστάσεων x^a(mod n):

$$|\Phi_1\rangle = \frac{1}{\sqrt{512}}\sum_{a=0}^{511}|a\rangle|11^a(\ mod 21)\rangle = \frac{1}{\sqrt{512}}(|0\rangle|1\rangle + |1\rangle|11\rangle + |2\rangle|16\rangle + \cdots)\ .$$

r	0	1	2	3	4	5	6	7	8	9	…
11^r(mod21)	d	d	16	8	4	2	1	11	16	8	…

Με αυτό τον τρόπο βρήκαμε την περίοδο r = 6, ωστόσο επειδή δεν έχει γίνει ακόμα μέτρηση δεν είναι παρατηρίσιμη.

5)QFT στον 1ο καταχωρητή.

$$|\widetilde{\Phi}\rangle = \frac{1}{512}\sum_{r=0}^{511}\sum_{c=0}^{511} e^{\frac{2\pi i r c}{512}} \quad |c\rangle|11^r (mod 21)\rangle$$

6) Μέτρηση.

Για να υπολογιστεί η πιθανότητα για την κατάσταση $|c, x^r (mod 21)\rangle$ δίνω τυχαία r = 2 και προκύπτει:

$$p(c) = \left|\left\langle c' \middle| \widetilde{\Phi}\right\rangle\right|^2 = \left|\frac{1}{512}\sum_{r:11^r mod 21=16} e^{2\pi i r c/512}\right|^2 = \left|\frac{1}{512}\sum_t e^{2\pi i(6t+2)c/512}\right|^2,$$

a_0 = 2, r = 6, q = 512 και

$$\langle c|c\rangle = \langle 11^6 mod 21|11^6 mod 21\rangle = 1$$

Η εύρεση των κορυφών, που προκύπτουν από τον μετασχηματισμό, γίνεται μέσω της εξίσωσης cr = dq, όπου r η περίοδος, c τα peaks, και $d \in \mathbb{N}$.

Λύνοντας ως προς c θα έχουμε: $c = \frac{q}{r}d = \frac{512}{6}d, d \in \mathbb{N}$

7) Καθορισμός της περιόδου r.

Ας υποθέσουμε ότι d = 2 . Τότε c / q = 171 / 512 και σε αυτό το σημείο θα χρησιμοποιήσουμε την συνεχή επέκταση κλασμάτων για να υπολογίσουμε το κλάσμα d/r.

$$\frac{171}{512} = 0 + \frac{1}{\frac{512}{171}} = 0 + \frac{1}{2+\frac{170}{171}} = 0 + \frac{1}{2+\frac{1}{\frac{171}{170}}} = 0 + \frac{1}{2+\frac{1}{1+\frac{1}{170}}},$$

d_0 = 0 , d_1 = 2 , d_2 = 1 και r_0 = 1, r_1 = 2 , r_2 = 3.

Έτσι προκύπτουν τα ακόλουθα κλάσματα:

$d_0 / r_0 = 0/1 = 0$, $d_1 / r_1 = 2/2 = 1$, $d_2 / r_2 = 1/3$.

Άρα, το r = 3 δεν μας καλύπτει καθώς δεν καλύπτει την προϋπόθεση, r άρτιος.

Αν τώρα d = 6, τότε c = 427 και c/q = 427/512. Χρησιμοποιούμε πάλι την ίδια μέθοδο για να υπολογίσουμε το d/r.

$$\frac{427}{512} = 0 + \frac{1}{\frac{512}{427}} = 0 + \frac{1}{1+\frac{1}{5+\frac{1}{42+\frac{1}{2}}}},$$

Ακολουθώντας την ίδια διαδικασία με προηγουμένως, θα έχουμε $d_2/r_2 = 5/6$.

Άρα, υπολογίσαμε την περίοδο r = 6, και καλύπτει όλες τις προϋποθέσεις.

r = 6 άρτιος, 11^3 = 1331, 1331 – (63)21 = 8 ≠ -1 , άρα 11^3 = 8 mod21.

Τελικά, μπορούμε να καθορίσουμε τους παράγοντες:

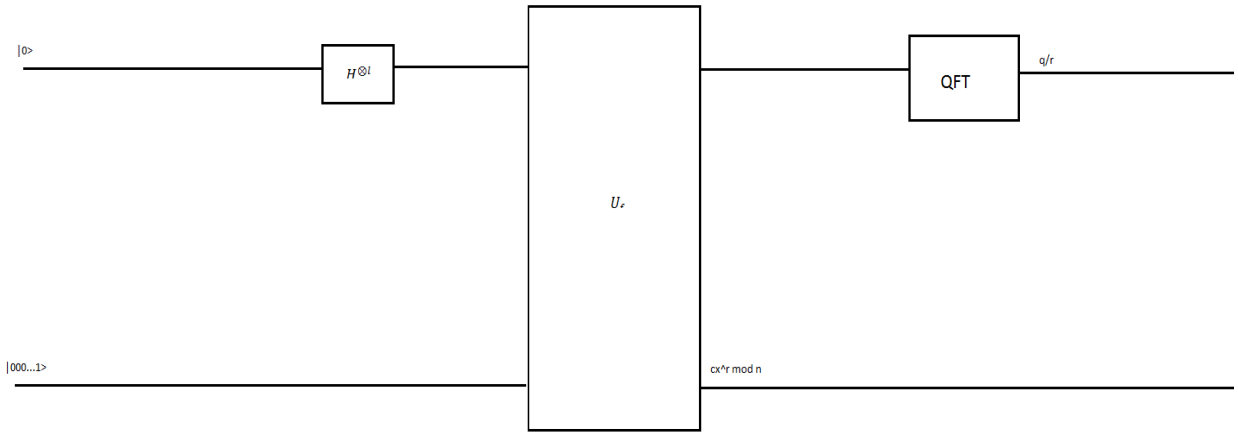
$$x^{r/2}\ mod\ n - 1 = 11^3\ mod\ 21 - 1 = 7$$

$$x^{r/2}\ mod\ n + 1 = 11^3\ mod\ 21 + 1 = 9$$

Εφαρμόζοντας, άλλη μια φορά τον αλγόριθμο του Ευκλείδη βρίσκουμε τους ΜΚΔ.

gcd(7,21) = 7 και gcd(9,21) = 3.

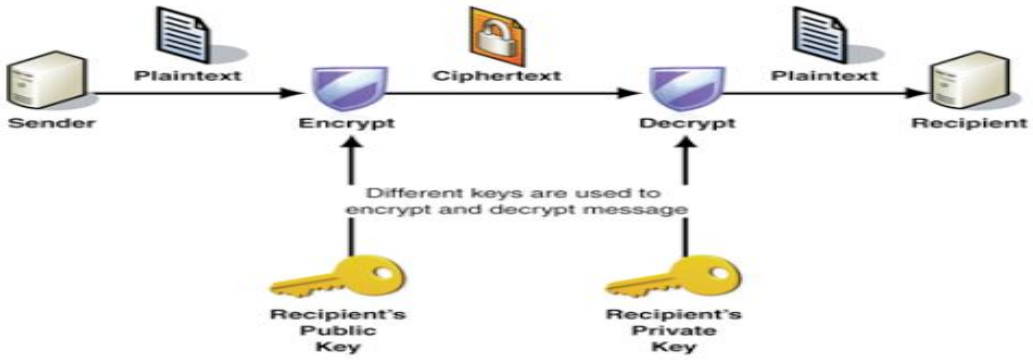
Ο αλγόριθμος λοιπόν του Shor παραγοντοποίησε το 21 = 3 x 7.



Κύκλωμα υλοποίησης του αλγορίθμου του Shor.

4) Συμπέρασμα:

Ο αλγόριθμος του Shor είναι αρκετά χρήσιμος για την ασφάλεια συστημάτων. Η παραγοντοποίηση μεγάλων αριθμών σε γινόμενο πρώτων παραγόντων, με μεγάλη ταχύτητα, θα ανοίξει νέους ορίζοντες για την κρυπτογραφία, καθώς πολλά από τα σημαντικότερα συστήματα κρυπτογράφησης βασίζεται πάνω στη δυσκολία αυτή.



Τρίμας Χρήστος