Kvantumszámítás 2. rész

Vágvölgyi Sándor
SZTE, Számítástudomány Alapjai Tanszék
Szeged, Árpád tér 2
H-6720
E-mail: vagvolgy@inf.u-szeged.hu

Shornak a prímtényezős felbontást kiszámoló algoritmusa

Input: egy N természetes szám.

Output: az N természetes számnak egy valódi osztója.

Műveletek száma: $O((logN)^3)$

Vázlatos áttekintés:

az algoritmus felhasználja a q természetes szám modulo N multiplikatív rendjét kiszámító algoritmust. (Itt q és N relatív prímek.) Ez az algoritmus felhasználja

- azt a hagyományos eljárást amely kiszámítja adott $q \in \{0, 1, \ldots, N-1\}$ és x természetes számra a $q^x \, mod \, N$ értéket $poly(logN)$ időben, és
- a periódus kiszámítására szolgáló algoritmust.

A periódus kiszámítására szolgáló algoritmus felhasználja az Ábel csoport felett vett kvantum Fourier transzformációt.

Definíció 0.1 *Legyenek N és p pozitív egész számok. Azt mondjuk hogy p valódi osztója a N számak ha*

1. $N = pq$,
2. $p \neq 1$, *és*
3. $p \neq N$.

Például a 28 szám valódi osztói a $2, 4, 7, 14$ számok. A 48 szám valódi osztói a $2, 4, 6, 8, 12, 24$ számok.

Definíció 0.2 *Legyenek N és q relatív prím természetes számok. A q szám modulo N multiplikatív rendje az a legkisebb k pozitív egész szám amelyre*

$q^k \equiv 1 \bmod N$.

Azaz q-nak a mod(N) multiplikatív rendje az a k pozitív egész szám, amelyre mint hatványkitevőre q-t emelve a q^k szám 1 maradékot ad N-nel osztva, és ha q^t is 1 maradékot ad valamely $t \geq 1$ számra, akkor $k \leq t$.

Példa. Számítsuk ki a 11 szám modulo 21 multiplikatív rendjét! A $k = 2$ számmal kezdjük és a $k = 3, 4, 5, 6$ számokkal folytatjuk az eljárásunkat.

$k = 2$: $11^2 = 121 = 5 \times 21 + 16$.

Tehát $11^2 \equiv 16$ *mod* 21.

$k = 3$: $11^3 = 11 \times 11^2 = 11 \times 16$ *mod* $21 = 176$ *mod* $21 = 8$ *mod* 21.

Tehát $11^3 \equiv 8$ *mod* 21.

$k = 4$: $11^4 = 11 \times 11^3 = 11 \times 8$ *mod* $21 = 88$ *mod* $21 = 4$ *mod* 21.

Tehát $11^4 \equiv 4 \ mod \ 21$.

$k = 5$: $11^5 = 11 \times 11^4 = 11 \times 4 \ mod \ 21 = 44 \ mod \ 21 = 2 \ mod \ 21$.

Tehát $11^5 \equiv 2 \ mod \ 21$.

$k = 6$: $11^6 = 11 \times 11^5 = 11 \times 2 \ mod \ 21 = 22 \ mod \ 21 = 1 \ mod \ 21$.

Tehát $11^6 \equiv 1 \ mod \ 21$.

Tehát a 11 szám modulo 21 multiplikatív rendje 6.

Sok számolást igényel q^k kiszámítása amikor k sok értéket vesz fel. Vegyük észre hogy k-nal csupán bizonyos értékeire kell kiszámolnunk q^k-t. Valóban írjuk fel k 2-es számrendszerbeli alakját:

$k = k_{m-1}2^{m-1} + k_{m-2}2^{m-2} + \cdots + k_1 2^1 + k_0$

itt $k_i \in \{ 0, 1 \}$, $0 \leq i \leq m-1$. Ekkor

$q^k = q^{k_{m-1}2^{m-1}} \times q^{k_{m-2}2^{m-2}} \times \cdots \times q^{k_1 2^1} \times q^{k_0}$

Ahhoz hogy kiszámítsuk q^k-t szükségünk van a

$q^{2^1}, q^{2^2}, \ldots, q^{2^{m-1}}$

számokra. Példa. Számoljuk ki a 17^{29} számot!

$29 = 16 + 8 + 4 + 1 = 2^4 + 2^3 + 2^2 + 2 + 0$.

Eképpen

$17^{29} = 17^{16} \times 17^8 \times 17^4 \times 17^1$.

Megmutatjuk hogy az N szám egy valódi osztójának a keresése visszavezethető valamely q szám modulo N multiplikatív rendjének a kiszámítására. Itt a q számot véletlenszerűen választjuk ki az $\{ 2, \ldots, N-1 \}$ halmazból.

A q szám modulo N multiplikatív rendjének a segítségével keresünk egy r pozitív egész számot úgy hogy

1. N osztója $r^2 - 1$-nek és
2. N nem osztója sem $r - 1$-nek sem $r + 1$-nek.

Így N valamely valódi osztója osztója lesz $r-1$-nek vagy $r + 1$-nek. Így $lnko(r - 1, N)$ vagy $lnko(r + 1, N)$ valódi osztója az N számnak.

Először tekintsük azt az esetet amikor N sem nem páros szám sem valamely prím szám hatványa. Ebben az esetben keresünk egy r pozitív egész számot úgy hogy

1. N osztója $r^2 - 1$-nek és
2. N nem osztója sem $r - 1$-nek sem $r + 1$-nek.

Például amikor $N = 21$, akkor az $r = 8$ értékválasztás megfelelő. 1. és 2. feltételek tejesülnek. $r^2 - 1 = 63 = 3 \times 21$. Figyeljük meg hogy $r - 1 = 7$ valódi osztója $n = 21$-nek.

Valódi osztót kiszámoló algoritmus

1. lépés: Ha N páros akkor visszaadjuk $p = 2$-t.

2. lépés: ha N valamely p prím szám hatványa akkor visszaadjuk p-t.

3. lépés: Egyenletes eloszlással véletlenszerűen válasszunk ki egy q számot, $2 \leq q \leq N-1$. Ha $p = lnko(q, N) > 1$ akkor adjuk vissza a p számot. Különben menjünk a 4. lépésre.

4. lépés: Számoljuk ki a q szám modulo N multiplikatív rendjét. Legyen k a q szám modulo N multiplikatív rendje! Ha k nem páros, akkor menjünk a 3. lépésre.

5. lépés: Legyen $k = 2m$ alakú. Legyen $r = (q^m \ mod \ N)$. Most $1 \leq r < N$. Határozzuk meg az r számot. Ha $1 < p = lnko(r-1, N) < N$, akkor adjuk vissza a p számot. Ha $1 < p = lnko(r+1, N) < N$, akkor adjuk vissza a p számot. Különben (ha nem találtunk N-nek valódi osztóját akkor) menjünk a 3. lépésre.

Tekintsük az 5. lépést! Most $q^{2m} \equiv 1 \ mod \ N$. Tehát N osztója a $(q^m-1)(q^m+1)$ szorzatnak. Az r szám definíciója szerint N osztója az $(r-1)(r+1)$ szorzatnak. Ha $1 < p = lnko(r-1, N) < N$, akkor a p szám valódi osztója N-nek. Ha $1 < p = lnko(r+1, N) < N$, akkor a p szám valódi osztója N-nek.

A q szám modulo N multiplikatív rendjének definíciója és az r szám definíciója alapján N nem osztója az $r-1$

számnak. Viszont N osztója lehet az $r+1$ számnak. Így előfordulhat hogy $1 = lnko(r-1, N)$ és $lnko(r+1, N) = N$. Ha 'szerencsénk van', akkor k páros és N nem osztója az $r+1$ számnak. Ekkor azt kapjuk hogy

$$1 < lnko(r-1, N) < N \text{ és } 1 < lnko(r+1, N) < N.$$

Mennyi annak a valószínűsége hogy 'szerencsénk van'? Legalább $\frac{1}{2}$.

Állítás 0.3 *Legyen N páratlan szám és N ne legyen valamely prímszám hatványa. Egyenletes eloszlással véletlenszerűen válasszunk ki egy q számot, $2 \leq q \leq N-1$. Annak a valószínűsége hogy a fentiekben kiszámolt k szám páros és N nem osztója az $r+1$ számnak legalább $\frac{1}{2}$.*

Legyenek N és q pozitív egész számok! Tekintsük az

$$f_q(x) = q^x \mod N$$

függvényt!

Állítás 0.4 *Legyenek N és q relatív prím természetes számok.*

- *A q szám modulo N multiplikatív rendje az $f_q(x) = q^x$ függvény a periódusa.*
- *Minden $x, y \in Z$ esetén, $f(x) = f(y)$ akkor és csak akkor ha $x - y$ többszöröse az a periódusnak.*

A fenti állítás tükrében meghatározzuk az

$$f_q(x) = q^x \ mod \ N$$

függvény a periódusát. Így megkapjuk a q szám modulo N multiplikatív rendjét.

A 5. lépésben tekintettük az $r = (q^m \ mod \ N)$ értékadást. A $f_q(x) = q^x \, mod \, N$ függvény értékének a kiszámítása bonyolult lehet hiszen az x kitevő nagy lehet.

Állítás 0.5 *Létezik hagyományos eljárás amely kiszámítja adott x helyen az*

$f_q(x) = q^x \, mod \, N$

függvény értéket $poly(logN)$ időben.

Bizonyítás. x bináris alakját tekintjük. Kiszámítjuk a

$q^{2^i} \mod N \ i = 1, 2, \ldots$

számokat ismételt négyzetre emeléssel és N-nel való osztás maradékának a kiszámításával.

□

Adott függvény periódusának a kiszámítása felhasználva az Ábel csoport felett vett kvantum Fourier transzformációt

Feladat. Adott egy $f : Z \to Z$ leképezés és egy N egész szám úgy hogy

1. létezik egy $a \leq N$ periódusa f-nek.

2. minden $x, y \in Z$ esetén, $f(x) = f(y)$ akkor és csak akkkor ha $x - y$ többszöröse az a periódusnak.

A fenti feltételek mellett találjuk meg az a természetes számot!

Megjegyezzük hogy a 2. feltétel szerint a Z értelmezési tartomány tetszőleges a periódus hosszú intervallumán (szakaszán) az f függvény injektív.

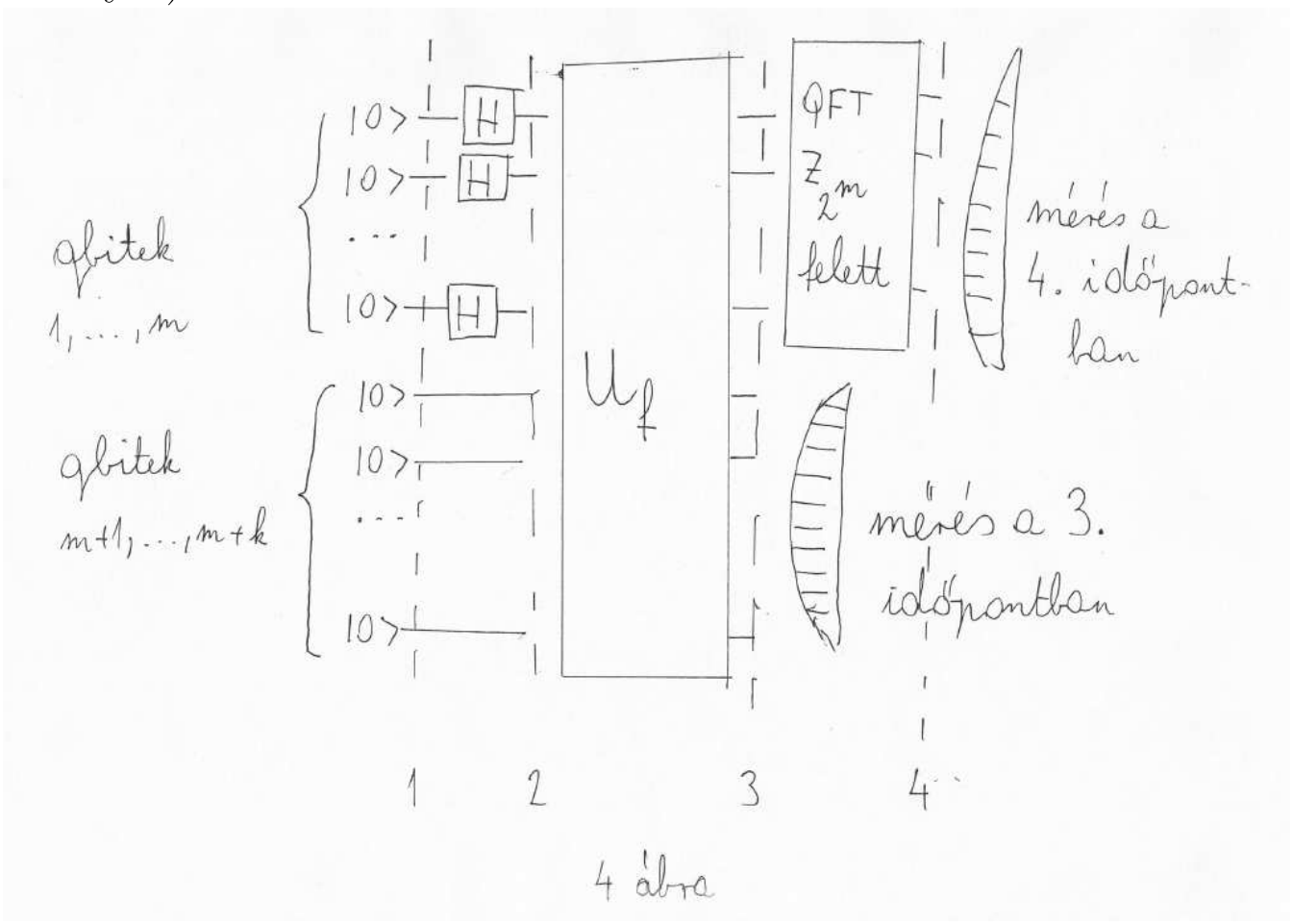
A hagyományos megoldása a fenti problémának tekinti az összes (t, a) párt, ahol $t, a \in \{ 0, 1, \ldots, M \}$, és minden egyes (t, a) párra kiszámítja $f(t)$-t és $f(t + a)$-t és eldönti hogy $f(t) = f(t + a)$ teljesül-e.

Választunk egy M természetes számot úgy hogy majd a $\mathbf{Z}_M$ Ábel csoport felett elvégezzük a QFT-t. Tudjuk hogy $a \leq N$. Legyen $M = 2^m$ a legkisebb olyan 2 hatvány hogy $N^2 < M \leq N^4$. $\mathbf{Z}_M = \{ 0, 1, \ldots, M \}$ jelöli az egész számok additív Ábel csoportját modulo M. Legyen k a legkisebb olyan természetes szám amelyre $M \leq 2^k$.

Most kettő esetet különböztetünk meg.

Első eset: az a periódus osztója az M számnak. (Ennek igen kicsi a valószínűsége. Hiszen ekkor a a 2 szám

hatványa.)



4 ábra

Tekintsük a 4. ábrán látható quantum áramkört! Először tekintsük az első m qbitet!

$(H \otimes H \otimes H \otimes \ldots H)(|0\rangle|0\rangle|0\rangle \ldots |0\rangle) =$
$\frac{1}{2^{\frac{m}{2}}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle) =$
$\frac{1}{2^{\frac{m}{2}}}(\Sigma_{x=0}^{2^m-1} |x\rangle$.

Adjunk k qbites regisztert (azaz k qbitet) a kvantum áramkörhöz. Mindegyik hozzáadott qbit a $|0\rangle$ állapotban van. Tegyük fel hogy az U_f áramkör számítja ki az f függvényt, és az eredményt a második regiszterben kapjuk meg. Az első m input qbit értéke közvetlenül az outputra

kerül (azaz az első m output qbitbe).

$$U_f(\frac{1}{2^{\frac{m}{2}}}\sum_{x=0}^{2^m-1}|x\mathbf{0}\rangle) = \frac{1}{2^{\frac{m}{2}}}\sum_{x=0}^{2^m-1}|xf(x)\rangle\ .$$

Tehát az áramkör 2. pontján az első m qbit (az első regiszter) Z_M összes elemének egyenlő együtthatóval vett lineáris kombinációja.

A 3. időpontban megmérjük a második regisztert (azaz az utolsó k darab qbitet)! Az $m+k$ darab qbit állapotvektora:

$$\sqrt{\frac{a}{M}}(|x\rangle + |x+a\rangle + \cdots + |x+(\frac{M}{a}-1)a\rangle)|f(x)\rangle$$

valamely véletlen $x \in Z_M$ esetén. Ugyanis

$f(x) = f(x+a) = \cdots = f(x+(\frac{M}{a}-1)a)$

és ha $y-x$ nem többszöröse a-nak, akkor $f(x) \neq f(y)$. Tehát az f függvény a $0, 1, \ldots M-1$ számok közül pontosan az $x, x+a, \ldots, x+(\frac{M}{a}-1)a$ helyeken veszi fel az $f(x)$ értéket.

Állítás 0.6 *Legyen $M = 2^m$! A Z_M monoid feletti kvantum Fourier transzformáció az alábbi unitér operátort valósítja meg:*

$QFT : H_M \to H_M$

$$|x\rangle \mapsto \frac{1}{\sqrt{M}}\sum_{y\in Z_M}\omega^{xy}|y\rangle$$

ahol $\omega = exp(\frac{2\pi i}{M})$ az 1 szám M-edik gyöke.

A harmadik szakaszban elvégezzük a $\mathbf{Z}_M = \mathbf{Z}_{2^m}$ Ábel csoport feletti QFT-t az első m darab biten. Legyen

$$\omega = exp(\frac{2\pi i}{2^m}) = exp(\frac{2\pi i}{M}) \ .$$

A QFT áttranszformálja az első m qbitet a

$$\frac{\sqrt{a}}{M} \sum_{y \in Z_M} (\sum_{j=0}^{\frac{M}{a}-1} \omega^{(x+ja)y}) |y\rangle = \frac{\sqrt{a}}{M} \sum_{y \in Z_M} \omega^{xy} (\sum_{j=0}^{\frac{M}{a}-1} \omega^{jay}) |y\rangle \tag{1}$$

állapotba valamely $x \in Z_M$ véletlen számra.

Mivel M többszöröse a-nek, azt kapjuk hogy ha $\omega^{ay} \neq 1$ azaz ha
$y \notin \{ 0, \frac{M}{a}, \frac{2M}{a}, \ldots, \frac{(a-1)M}{a} \}$, akkor

$$\sum_{j=0}^{\frac{M}{a}-1} (\omega^{ay})^j = \frac{1 - \omega^{My}}{1 - \omega^{ay}} = 0.$$

Ebből azt kapjuk hogy a (1) egyenlőségben azon $|y\rangle$ bázis állapotok együtthatói (valószínűségi amplitúdói) ahol y nem többszöröse $\frac{M}{a}$-nek egyenlőek 0-val.

Mivel M többszöröse a-nek, azt kapjuk hogy ha $\omega^{ay} = 1$ azaz ha $y \in \{ 0, \frac{M}{a}, \frac{2M}{a}, \ldots, \frac{(a-1)M}{a} \}$, akkor

$$\sum_{j=0}^{\frac{M}{a}-1} (\omega^{ay})^j = \sum_{j=0}^{\frac{M}{a}-1} 1 = \frac{M}{a}.$$

Ezért a (1) egyenlőségben szereplő állapot az

$$\{ |0\rangle, |\frac{M}{a}\rangle, \cdots, |(a-1)\frac{M}{a}\rangle \}$$

bázis állapotok lineáris kombinációja. Továbbá ezeknek a bázis állapotoknak az együtthatóinak (valószínűségi amplitúdóinak) abszolút értéke egyenlőek egymással.

Az így kapott állapotot megmérjük. Eképpen a mérés véletlenszerűen egyenletes eloszlással adja az $|y\rangle = |c\frac{M}{a}\rangle$ állapotot. A kapott $|y\rangle = |c\frac{M}{a}\rangle$ állapot címkéje $y = c\frac{M}{a}$, továbbá $0 \leq c \leq (a-1)$ véletlenszerűen egyenletes eloszlással. Tehát

$$\frac{y}{M} = \frac{c}{a}\,.$$

Egyszerűsítsűk le a bal oldalt $lnko(y, M)$-nel! Kapjuk:

$\frac{y'}{M'} = \frac{c}{a}$.

Tegyük fel hogy $lnko(c, a) = 1$! Most $y'a = cM'$. Mivel $lnko(y', M') = 1$ és $lnko(a, c) = 1$ kapjuk hogy $y' = c$ és $a = M'$. Tehát a az $\frac{y'}{M'}$ tört nevezője. A fentiek alapján a következő módon járunk el. Képezünk egy törtet aminek a számlálója a mért állapot y címkéje és aminek a nevezője M. Majd egyszerűsítjük a törtet: az $lnko(y, M)$ legnagyobb közös osztóval osztjuk a számlálót is és a nevezőt is. Az így kapott tört nevezője az a értéke.

Tegyük fel hogy $lnko(c, a) \neq 1$! Most is a mért állapot y címkéjének és M-nek az $lnko(y, M)$ legnagyobb közös osztójával osztjuk M-et; de az így kapott hányados nem lesz az a értéke.

Mennyi a valószínűsége annak hogy $lnko(c, a) = 1$? A

számelmélet szerint nagy a számra az a-nél kisebb egyenlő, a-hez relatív prím számok száma megközelítőleg:

$e^{-\gamma}\frac{a}{log\,log\,a}$.

Itt $\gamma = 0.5772156...$ Euler konstansa. Ennek megfelelően annak a valószínűsége hogy egy véletlenül választott c relatív prím a-vel megközelítőleg

$e^{-\gamma}\frac{1}{log\,log\,a}$.

Emlékezzünk hogy $a < N$! Tekintsünk tetszőleges 1-hez közeli p valószínűséget. A fenti eljárást $O(log\,log\,N)$-szer elvégezve, p-nél nagyobb a
valószínűsége annak hogy hogy sikerül meghatározni az a számot.

Második eset. a nem osztója M-nek. Végezzük el újra a fenti eljárást. Ha $N \geq 100$, akkor legalább $\frac{2}{5}$ a valószínűsége annak hogy a kapott y címkére teljesül hogy

$|\frac{y}{M} - \frac{c}{a}| < \frac{1}{2M}$ valamely $0 \leq c < a$ esetén.

Tekintsünk két egymástól különböző törtet amelyek nevezője legfeljebb N. A különbség kiszámításához kiszámolt közös nevező legfeljebb N^2. Ezért a két tört különbsége legalább $\frac{1}{N^2} > \frac{1}{M}$. Így $\frac{c}{a}$ az az egyértelműen meghatározott tört amelynek a nevezője legfeljebb N és $\frac{y}{M}$-től vett távolsága (a különbség abszolútértéke) kisebb mint $\frac{1}{2M}$. A $\frac{c}{a}$ szám értékét meg tudjuk határozni. Ismét tegyük fel hogy $lnko(c, a) = 1$! Most ki tudjuk számolni a értékét.

Az első esethez hasonlóan kapjuk az alábbiakat. Tek-

intsünk tetszőleges 1-hez közeli p valószínűséget. A fenti eljárást $O(log\, log\, N)$-szer elvégezve, p-nél nagyobb a valószínűsége annak hogy sikerül meghatározni az a számot.

A kvantum Turing gép A kvantum Turing gép egy rendezett ötös (Q, A, δ, q_0, q_f), ahol

- Q a véges állapot halmaz,
- A az ábécé,
- δ a Turing gép átmenet amplitúdó függvénye.

$\delta : Q \times A \times Q \times A \times \{-1, 0, 1\} \to \mathbf{C}_{[0,1]}$
egy leképezés. $\delta(q_1, a_1, q_2, a_2, d)$ az amplitúdója annak hogy ha a Turing gép q_1 állapotban van és az a_1 szimbólumot olvassa akkor a_1 helyébe a_2 szimbólumot ír és a q_2 állapotba lép és az író-olvasó fejet a $d \in \{-1, 0, 1\}$ irányban elmozdítja.

- $q_0, q_f \in Q$ rendre a kezdő állapot, és a végállapot. Az átmenet amplitúdó függvény kielégíti az alábbi feltételt.

$$\text{minden } (q_1, a_1) \in Q \times A \text{ esetén}$$

$$\sum_{(q_2,a_2,d)\in Q\times A\times\{-1,0,1\}} |\delta(q_1, a_1, q_2, a_2, d)|^2 = 1$$

A bázis konfiguráció megfelel a hagyományos Turing gép konfigurációjának.

A kvantum Turing gép általános konfigurációja

$$\alpha_1|c_1\rangle + \cdots + \alpha_m|c_m\rangle$$

alakú ahol c_i bázis konfiguráció és $\alpha_i \in \mathbf{C}$ és
$|\alpha_1|^2 + \cdots + |\alpha_m|^2 = 1$

A bázis konfigurációk egy ortonormális bázist alkotnak egy végtelen dimenziós vektortér felett.

A kvantum Turing gép számolása egy irányított, körmentes gráffal írható le. A gráfnak van gyökere, a gyökérből minden szögpontba vezet út. A gráf szögpontjai bázis konfigurációk. A gyökér a kezdő konfiguráció. Minden egyes c csúcsnak a gyermekei azok a bázis konfigurációk amikbe van átmenet a c csúcsból. Minden élhez hozzárendelünk egy valószínűségi amplitúdót: annak a valószínűségi amplitúdóját hogy a számolás azt az élet követi. A valószínűségi amplitúdó egy olyan komplex szám amelynek az abszolút értéke kisebb egyenlő 1-nél. Tekintsünk egy tetszőleges, gyökérből kiinduló utat a fában! Az út valószínűségi amplitúdója az út éleinek valószínűségi amplitúdóinak a szorzata. Az irányított gráf valamely szögpontjában lévő tetszőleges bázis konfiguráció valószínűségi amplitúdója a győkérből a konfigurációba vezető utak valószínűségi amplitúdóinak az összege.

Az M kvantum Turing gép az összes gyökérből kiinduló utat egyszerre lépésről lépésre követi. A gráf n-edik szintje adja meg M n-edik általános konfigurációját, $n = 0, 1, \ldots$. Legyen $n \geq 0$ tetszőleges. Tekintsük azokat a bázis konfigurációkat amelyekbe a gyökérből kiinduló n hosszú utak vezetnek. Ezeket megszorozzuk a valószínűségi amplitúdójukkal és összeadjuk őket. Az így kapott általános konfiguráció M állapota n lépés után.

A δ átmenet amplitúdó függvény meghatároz meghatároz egy M_δ lineáris leképezést a vektor térben. Ezt átmeneti

relációnak (időbeni fejlődés leképezésnek) nevezzük. Ezt az átmeneti relációt követjük amikor a gyökérből az 1. mélységű szintre lépünk, amikor az 1. mélységű szintről a 2. mélységű szintre lépünk. Általában amikor az i-edik szintről az $i+1$-edik szintre lépünk.

M_δ mátrixa egy végtelen mátrix. M_δ-nak unitérnek kell lennie. Ezért az M_δ mátrixának az adjungáltja (transzponálás majd elemenként konjugált képzés) az M_δ^{-1} operátor mátrixa.

Mivel M_δ unitér, létezik az M_δ^{-1} lineáris leképezés a vektor térben. M_δ^{-1} relációt követjük amikor a gyökérre lépünk az 1. mélységű szintről, majd amikor az 1. mélységű szintre épünk a 2. mélységű szintről. Általában amikor az i-edik szintre lépünk az $i+1$-edik szintről.

Azt mondjuk hogy M megáll egy K általános konfiguráción ha K valamely bázis végkonfigurációk lineáris kombinációja. (Azaz K csak bázis végkonfigurációkat tartalmaz.) Ekkor minden bázis végkonfiguráció szalagtartalmához hozzárendeljük a végkonfiguráció valószínűségét. (Ha több bázis végkonfiguráció szalagtartalma megegyezik akkor a valószínűségek összeadódnak.) Íly módon minden inputra egy output valószínűségi eloszlást kapunk.

Amit Turing géppel ki lehet számolni azt ki lehet számolni kvantum Turing géppel is. Fordítva amit kvantum Turing géppel ki lehet számolni azt ki lehet számolni Turing géppel is.

Azt mondjuk hogy T kvantum Turing gép az M kvantum Turing gépet $f : N \to N$ számolási lépésben ϵ pontossággal utánozza ha a következő teljesül. Tetszőleges x inputon M k lépéses számolása során kapott általános konfiguráció és T $f(k)$ lépéses számolása során kapott általános konfiguráció különbségének a normája kisebb mint ϵ.

Az univerzális kvantum Turing gép tetszőleges M kvantum Turing gép számolását tetszőleges pontossággal tudja utánozni. Létezik olyan T kvantum Turing gép hogy ha bemenetként megkapja

tetszőleges M kvantum Turing gép leírását (kódját),

M-nek tetszőleges x inputját.

tetszőleges k természetes számot,

és tetszőleges $\epsilon > 0$, számot,

akkor M k darab számítási lépését T ϵ pontossággal utánozza $p(k, \frac{1}{\epsilon})$ lépés alatt, valamely p polinomra.

Irodalom

A Ekert and R Jozsa. Quantum Algorithms: Entanglement Enhanced Information Processing. Phil. Trans. Roy. Soc. Lond. A **356**: 1779-1782 (1998).

Peter W. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. **26**(5): 1484-1509 (1997).