1 GROVER algoritmus

A Grover féle algoritmus, arra a problémára ad a klasszikus módszernél hatékonyabb kvantumos eljárást, hogy hogyan kereshető meg egy "tű a szénakazalban", vagy egy a nevek sorrendjébe állított telefonkönyvből hogyan állapítható meg, hogy kinek a telefonszáma egy adott szám.

Az utóbbi problémánál a fordított feladat, azaz egy névhez tartozó telefonszám megtalálása a következő *hatékony* algoritmussal történhet. Megnézzük az N nevet tartalmazó lista közepét és megvizsgáljuk, hogy a keresett név ez előtt van vagy utána. Legyen mondjuk előtte, akkor ennek az előtte levő résznek felénél, vagyis a teljes könyv negyedénél nézzük meg a nevet, majd az itt található név és a kersesett név összehasonlítása alapján ismét felezhetjük az átnézendő listát. Így az l edik lépésben $N/(2^l)$ a hossza annak a listának, amit még át kell nézni. Mivel a nevet akkor találtuk meg, amikor a lista hossza 1, ezért kb. $\log_2 N$ lépés után megtaláljuk a keresett nevet és a hozzá tartozó telefonszámot, azaz az algoritmus $Poly(\log N)$ bonyolultságú, azaz könnyű.

Fordítva azonban a dolog nehéz, mivel a telefonszámok nincsenek sorba rakva. Ahhoz, hogy legalább $1/2$ valószínűséggel megtaláljuk az ismert telefonszámhoz tartozó nevet $N/2$ darab nevet illetve hozzátartozó telefonszámot kell megnézni, azaz $2^{\log_2(N/2)}$ lépést kell tenni, vagyis a feladat exponenciális $\log N$-ben. A Grover féle kvantumos algoritmus segítségével a lépésszám $N/2$ helyett $\sqrt{N}$-nel tehető arányossá, ami nem annyira jelentős mint a Shor féle algoritmus gyorsító hatása a prímfaktorizációra, de azért mégis érdekes eredmény.

A feladat matematikailag a következő. Azonosítsuk a nevek listáját a $\mathbb{Z}_N^0 = \{0, 1, \ldots N-1\}$ halmazzal, és legyen adott ezen egy függvény $x \in \mathbb{Z}_N^0$, $x \to g(x)$, amely megmondja, hogy mennyi a telefonszám: $g(x)$. Tegyük föl most, hogy adott egy telefonszám, $g(\omega)$ és keressük azt az $\omega \in \mathbb{Z}_N^0$-t, amelynek ez a $g(\omega)$ a képe.

Definiáljunk most egy másik függvényt $f(x)$-et, amely a következő tulajdonságú:

$$\begin{aligned} f_\omega(x) &= 1, \quad \text{ha} \;\; x = \omega \\ f_\omega(x) &= 0, \quad \text{ha} \;\; x \neq \omega \end{aligned} \tag{1}$$

Ez egy úgynevezett orákulum, x a bemenet $f(x)$ a kimenet, ez fizikailag lehet maga a telefonkönyv, a lényeges, hogy adott x esetén az f gyorsan (polinomiálisan) kiszámítható legyen. Mint föntebb láttuk ez esetünkben valóban így van, de a fordított feladat, hogy melyik az az $x = \omega$, amelyre $f_\omega(x) = 1$ nehéz.

Az a kérdés igazán, hogy hányszor kell az orákulumhoz fordulni, hogy megtaláljuk ω-t. Definiáljuk a következő kétregiszteres műveletet "kvantumgépet".

$$U_\omega : |x\rangle|y\rangle \to |x\rangle|y \oplus f_\omega(x)\rangle \tag{2}$$

ahol az első regiszteren N különböző számot lehet ábrázolni, vagyis az egy L qubites regiszter, ahol L az a legkisebb szám amelyre $N < 2^L$, és $|x\rangle$ az x szám bináris megfelelőjeként van ábrázolva. A második regiszter legyen egy

qubites. Mint már láttuk a Deutsch féle algoritmusnál, ha a második qubitet az $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ állapotból indítjuk, akkor

$$U_\omega : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}}|x\rangle(|0 \oplus f_\omega(x)\rangle - |1 \oplus f_\omega(x)\rangle) = \tag{3}$$

$$= \begin{cases} \frac{1}{\sqrt{2}}|x\rangle(|0\rangle - |1\rangle) \text{ ha } f_\omega(x) = 0 \\ \frac{1}{\sqrt{2}}|x\rangle(|1\rangle - |0\rangle) \text{ ha } f_\omega(x) = 1 \end{cases} \tag{4}$$

Ez másképpen azt jelenti, hogy

$$U_\omega : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f_\omega(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{5}$$

A továbbiakban el is hagyhatjuk a második regisztert, amelynek az állapota nem változik, és csak az elsőt vizsgáljuk. Mivel a keresett $|\omega\rangle$ is a kitüntetett számítási bázis eleme, az ortogonális az összes többi báziselemre. Emiatt ha a második regisztert fixen tartjuk, az U_ω operátor hatása a következőképpen is írható:

$$U_\omega|x\rangle \rightarrow (-1)^{f_\omega(x)}|x\rangle = (1 - 2|\omega\rangle\langle\omega|)|x\rangle \tag{6}$$

hiszen $\langle\omega\,|x\rangle = 0$, ha $\omega \neq x$. Mivel ez a bázisvektorokra igaz, a linearitás miatt minden vektorra igaznak kell lennie, azaz az U_ω operátor alakja

$$U_\omega = 1 - 2|\omega\rangle\langle\omega|$$

$$U_\omega\,|\psi\rangle = |\psi\rangle - 2|\omega\rangle\langle\omega|\psi\rangle \tag{7}$$

Most megmutatjuk, hogy az U_ω unitér operátor hatása geometriailag úgy képzelhető, hogy az tükröz az $|\omega\rangle$-ra merőleges hipersíkra.

$$\acute{A}BRA \tag{8}$$

Ez azt jelenti, hogy ha egy tetszőleges $|\psi\rangle$ állapotot felbontunk egy $|\omega\rangle$ irányú és egy arra merőleges vektorra, akkor az U_ω hatására az $|\omega\rangle$-val párhuzamos komponens előjelet vált, míg a merőleges komponens nem változik. Egy tetszőleges $|\psi\rangle$ vektorra az említett felbontás a következő:

$$|\psi\rangle = |\omega\rangle\,\langle\omega\,|\psi\rangle + (|\psi\rangle - |\omega\rangle\,\langle\omega\,|\psi\rangle), \tag{9}$$

ahol láthatólag az első tag az $|\omega\rangle$-val párhuzamos, a második, zárójeles tag pedig az $|\omega\rangle$ -ra merőleges komponens. Valóban ha itt az első tag előjelét az ellenkezőjére változtatjuk, azaz tükrözünk az $|\omega\rangle$-ra merőleges síkra, akkor az eredmény

$$|\varphi\rangle = |\psi\rangle - 2\,|\omega\rangle\,\langle\omega\,|\psi\rangle) = U_\omega\,|\psi\rangle \tag{10}$$

azaz éppen $U_\omega\,|\psi\rangle$.

Vezessük be ezután a következő állapotot, amely az összes számítási bázisállapot szimmetrikus lineáris kombinációja:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{11}$$

Tudjuk, hogy $|\omega\rangle$ is a számítási bázis eleme, csak azt nem, hogy melyik. Így, ha a számítási bázisban mérnénk, annak a valószínősége, hogy éppen $|\omega\rangle$-t mérünk $\langle\omega|s\rangle = 1/\sqrt{N}$, azaz $|\langle\omega|s\rangle|^2 = 1/N$, vagyis ugyanaz mintha klasszikusan találomra keresnénk meg $|\omega\rangle$-t.

A Grover eljárás egy iteráció, amely lépésről lépésre növeli az ω megtalálási valószínűségét. Tekintsük ehhez az

$$U_s = 2|s\rangle\langle s| - 1 \tag{12}$$

unitér operátort. Ez utóbbi az összes bázisállapot szimmetrikus átlagának irányába mutató komponenst, azaz az $|s\rangle$ irányú komponenst megőrzi, de tükrözi az $|s\rangle$-re merőleges komponenst.

$$\acute{A}BRA \tag{13}$$

Tekintsük ezután a $G = U_s U_\omega$ Grover operátort. Ezt alkalmazva s-re, majd ismét a kapott eredményre, elegendő sokszor iterálva az s-ből indulva eljutunk a megfelelő ω-hoz. Valóban, legyen

$$\langle\omega|s\rangle = \frac{1}{\sqrt{N}} = \sin\theta \tag{14}$$

ahol ez az egyenlet definiálja θ-t, amely a szimmetrikus vektornak és a keresett $|\omega\rangle$-ra merőleges síknak a szöge. Bontsuk föl most $|s\rangle$-t egy $|\omega\rangle$ irányú és arra merőleges komponensre, ami a következő lesz

$$|s\rangle = |\omega\rangle \sin\theta + |\omega_\perp\rangle \cos\theta \tag{15}$$

ahol $|\omega_\perp\rangle$ az $|s\rangle$-nek az $|\omega\rangle$-ra merőleges altérre való vetülete azaz a $P_\omega^\perp |s\rangle = (1 - |\omega\rangle\langle\omega|)|s\rangle$ irányába mutató egységvektor: $|\omega_\perp\rangle = P_\omega^\perp |s\rangle / |\langle s| P_\omega^\perp |s\rangle| = P_\omega^\perp |s\rangle / \cos\theta$.

Ha alkalmazzuk U_ω-t $|s\rangle$-re akkor az eredmény az $|s'\rangle = -|\omega\rangle \sin\theta + |\omega_\perp\rangle \cos\theta$ Alkalmazzuk ezután erre U_s-et, az eredmény, amint az geometriailag látható, de a fönti formulákból algebrailag is megkapható:

$$G|s\rangle = |s_1\rangle = |\omega\rangle \sin 3\theta + |\omega_\perp\rangle \cos 3\theta \tag{16}$$

aminek következtében az $|s\rangle$ vektor elfordul $\omega_\perp$ -tól és ω felé fordul. Egyszerűen látható, hogy egy újabb G hatására az eredmémy $G^2 s = G s_1 = s_2 = \omega \sin 5\theta + \omega_\perp \cos 5\theta$ lesz, és általában

$$G^n s = s_n = \omega \sin(2n+1)\theta + \omega_\perp \cos(2n+1)\theta \tag{17}$$

Ha a megfelelő pillanatban hagyjuk abba az iterálást, akkor s_n közel lesz ω-hoz azaz $\langle s_n|\omega\rangle \approx 1$ lesz vagyis a számítási bázisban végrehajtott mérésnél nagy valószínőséggel kapjuk meg ω-t. Ez akkor történik meg, amikor az elfordulás szöge közel lesz $\pi/2$-hez.

Ha N nagy, akkor $\sin\theta = 1/\sqrt{N} \ll 1$ tehát $\theta \approx \sin\theta = 1/\sqrt{N}$. Így a T-edik lépésben a szög $(2T+1)\theta \approx (2T+1)/\sqrt{N}$, és ennek közel kell lennie $\pi/2$-höz, azaz $(2T+1)/\sqrt{N} \approx \pi/2$, amiből a szükséges lépésszám

$$T = \frac{\pi}{4}\sqrt{N} - 1/2 \tag{18}$$

körül lesz azaz arányos $\sqrt{N}$-el. Mivel T-nek egésznek kell lennie, helyesebb $T = \frac{\pi}{4}\sqrt{N}(1 - O(1/\sqrt{N}))$ formula. Ennyi lépés után a találat valószínűsége

$$\mathcal{P}(\omega) = |\langle s_n|\omega\rangle|^2 = \sin^2(2T+1)\theta = 1 - O(1/N) \tag{19}$$

Mivel minden lépésben egyszer kell az U_ω operátort alkalmazni, ami annyit jelent, hogy lépésenként egyszer kell megnézni az f függvényt, a fönti eredmény azt jelenti, hogy a klasszikushoz képest $\sqrt{N}$-szer rövidebb a keresés. Azonban vigyázni kell, ha nem hagyjuk időben abba az iterálást, akkor utána már távolodni fogunk ω-tól.

Tekintsük példaként az egyszerű $N = 4$ esetet, amelynél θ ugyan nem kicsi, de a dolog elvileg mégis igen jól működik, hiszen $\sin\theta = 1/2$, amiből $\theta = \pi/6$, vagyis egyetlen forgatás után a szög $3\theta = \pi/2$, azaz az eredmény pontosan ω. Egy klasszikus keresésnél a próbálkozások számának várható értéke ebben az esetben : $1 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{4} + 4 \cdot \frac{1}{4} = 2,5$ vagy ha figyelembe vesszük, hogy ha háromszor nem sikerült, akkor a negyedikre már nem kell próbálkozni ez a várható érték $2,25$.

A séma kiterjeszthető olyan esetre is, amikor nem egy megjelölt elem van hanem néhány. Ld. Preskill vagy Nielsen Chuang.Kvantum Fourier Transzformáció

A klasszikus (nem kvantumos) Fourier transzformáció rendkívül hatékony eszköz adatsorok, függvények viselkedésének jellemzésére. A transzformáció elsősorban akkkor hasznos, ha a vizsgált függvény néhány különböző frekvenciával, azaz különbözó periódussal változó harmonikus, tehát szinuszos vagy koszinuszos függvény összege, vagy legalábbis közelítőleg ilyen. Ekkor a Fourier tarnszfomáció megadja az egyes különböző periódusú komponensek súlyát, ezt nevezzük a jel (Fourier) spektriumának. Példaként említjük, hogy lényegében egy analóg Fourier transzformációt végez az emberi fül, aminek nyomán pl. meg tudjuk mondani, hogy kinek a hangját halljuk a rádióban. Ugyanakkor minden modern elektronikus kommunikációs eszköz is ezen matematikai módszer segítségével megérthető technikát használ, amikor szétválasztja a rádióállomások különböző periódusú (frekvenciájú) rezgési jeleit, vagy amikor mobiltelefonon csak azt az információt kapom meg, amelyet valóban nekem szántak. A jelfeldolgozás szempontjából nagyon fontos a folytonos függvények Fourier trarszformációja is, a gyakorlatban azonban mindig véges sok adattal dolgozunk, s még ha folytonos is a jel, abból egy mintát veszünk, diszkrét értékeket választunk ki.

A klasszikus diszkrét Fourier transzformációt a.következőképpen definiáljuk. Legyen $c_0, c_1 \dots c_{N-1}$ N db komplex szám. Jelöljük ezek halmazát $\{c_x\}$-el. A Fourier transzformáció ehhez a halmazhoz egy másik, ugyanilyen számosságú $\{\tilde{c}_y\}$ halmazt rendel hozzá, melynek elemei a

$$\tilde{c}_y = \mathcal{F}(\{c_x\}) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \exp(i2\pi xy/N) c_x, \quad y = 0, 1 \dots N-1 \tag{20}$$

számok, ahol tehát y is végigfut a nemnegatív egészeken $N-1$-ig. Megjegyezzük, hogy az összes, azaz N db $\tilde{c}_y$-t N^2 számú szorzással lehet kiszámítni.

Kimutatható, hogy a transzformáció inverze:

$$c_x = \mathcal{F}^{-1}(\tilde{c}_y) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp(-i2\pi xy/N) \tilde{c}_y$$

Ha a $\{c_x\}$ halmazt a komplex számtest fölötti szám N-esek terének egy vektoraként tekintjük a szokásos összeadási és komplex skalárissal történő szorzási szabállyal, akkor a fönti tarnszformáció lineáris. Ha emellett a belső szorzatot a szintén szokásos $(\{c_x\}, \{c'_x\}) = \sum_{x=0}^{N-1} c_x^* c'_x$ összefüggéssel értelmezzük, akkor megmutathatóan az $\mathcal{F}$ transzformáció unitér, tehát speciálisan normatartó is: $\sum_{y=0}^{N-1} |\tilde{c}_y|^2 = \sum_{x=0}^{N-1} |c_x|^2$.

Most bevezetjük a kvantumos transzformációt. Fusson végig az x egész szám a $0, 1, 2 \dots$ $N-1$ számok mindegyikén. Legyen n az a legkisebb egész szám amelyre $N \leq 2^n$. Legyen x bináris alakja $x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \dots + x_0 2^0 = \sum_{l=0}^{n-1} x_l 2^l$, ahol tehát $x_k = 0$ vagy 1, minden k-ra. Ábrázoljuk x-et n qubiten, azaz vezessük be az $|x\rangle = |x_{n-1}\rangle |x_{n-2}\rangle \dots |x_0\rangle$ vektorokat, amelyek egy N dimenziós tenzori szorzattér bázisvektorainak tekinthetünk, ezt számítási bázisnak nevezzük, amely tehát egy n qubites regiszteren ábrázolható. A számítási bázis elemeinek kvantumos Fourier transzformáltja (QFT) a következő:

$$QFT : |x\rangle \to |x\rangle_F = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp(2\pi ixy/N) |y\rangle \tag{21a}$$

ahol $|y\rangle$ is végigfut a számítási bázis elemein. A QFT-ről közvetlenül is belátható, hogy unitér transzformáció, de alább egy szorzatfölbontás révén látni fogjuk, hogy a QFT elemi unitér transzformációk szorzata, tehát maga is unitér. Egy tetszőleges vektor QFT-je ennek alapján a következő:

$$\sum_{x=0}^{N-1} c_x |x\rangle \to \left(\sum_{x=0}^{N-1} c_x |x\rangle \right)_F = \sum_{x=0}^{N-1} c_x |x\rangle_F = \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} c_x \sum_{y=0}^{N-1} \exp(2\pi ixy/N) |y\rangle = \sum_{y=0}^{N-1} \tilde{c}_y |y\rangle \tag{22}$$

hiszen 20 szerint $\tilde{c}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \exp(i2\pi xy/N) c_x$ éppen a c_x együtthatók közönséges Fourier transzformáltja.

Visszatérve a bázisvektorok transzformációjára, megmutatjuk, hogy a transzformáció kvantumos kapukkal $(\log N)^2$ nagyságrendű lépésszámmal megvalósítható.

1. Először bebizonyítjuk, hogy az n qubites bázisvektorok fönti Fourier transzformáltja a következő szorzat alakba írható:

$$|x\rangle \to |x\rangle_F = \frac{1}{\sqrt{N}} \otimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i x 2^{-l}} |1\rangle\right)$$

A bizonyítást teljes indukcióval célszerű elvégezni. Legyen először $|x\rangle = |x_0\rangle$, egy qubites, ahol $|x_0\rangle = |0\rangle$ $|x_0\rangle = |1\rangle$, ekkor $n = 1$ a tér ilyenkor $N = 2$ dimenziós. Ekkor

$$|x_0\rangle_F = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} \exp(2\pi i x_0 y/2) |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i x_0/2} |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot 0, x_0} |1\rangle),$$

mert $|y = 0\rangle$ együtthatója mindenképpen 1, az $|1\rangle$ együtthatója pedig 1, ha $x_0 = 0$ és -1, ha $x_0 = 1$.

Figyeljük meg, hogy egy qubitre a QFT éppen egy Hadamard kapu hatásával egyezik meg, hiszen a fönti képlet szerint

$$|0\rangle_F = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |1\rangle_F = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Az általános eset szempontjából tanulságos, ha megnézzük még az $N = 4$, $n = 2$ esetet is, azaz legyen $|x\rangle = |x_1 x_0\rangle$, x_1 és x_0 bináris számok.

A 21a képlet szerint: $|x\rangle \to |x\rangle_F = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp(2\pi i x y/N) |y\rangle$, ahol, most y 0-tól 3-ig fut:

$$|x_1 x_0\rangle_F = |x\rangle_F = \frac{1}{2}(|00\rangle + e^{2\pi i x/4} |01\rangle + e^{2\pi i x \cdot 2/4} |10\rangle + e^{2\pi i x \cdot 3/4} |11\rangle)$$

Emeljük ki az első két tagból az első $|0\rangle$ qubitet, a harmadik negyedik tagból, pedig $e^{2\pi i x \cdot 2/4} |1\rangle$-et. Egy újabb kiemelés után kapjuk a:

$$\begin{aligned} |x\rangle_F &= \frac{1}{2}\{|0\rangle (|0\rangle + e^{2\pi i x/4} |1\rangle) + e^{2\pi i x \cdot 2/4} |1\rangle (|0\rangle + e^{2\pi i x \cdot 1/4} |1\rangle)\} = \\ &= \frac{1}{2}(|0\rangle + e^{2\pi i x/2} |1\rangle)(|0\rangle + e^{2\pi i x/4} |1\rangle) \end{aligned}$$

a bizonyítandó eredményt $n = 2$-re. Tegyük most föl, hogy igaz a képlet n-re, vizsgáljuk $n + 1$-re.

$$\begin{aligned} |x\rangle_F = \frac{1}{\sqrt{2^{n+1}}}(&\left|\underbrace{0 \ldots 00}_{n+1}\right\rangle + e^{2\pi i x/2^{n+1}} |0 \ldots 01\rangle + e^{2\pi i x \cdot 2/2^{n+1}} |0 \ldots 10\rangle + e^{2\pi i x \cdot 3/2^{n+1}} |0 \ldots 11\rangle + \\ &+ \ldots + e^{2\pi i x (2^{n+1}-2)/2^{n+1}} |1 \ldots 10\rangle + e^{2\pi i x (2^{n+1}-1)/2^{n+1}} |1 \ldots 11\rangle) \end{aligned}$$

Most minden két egymást követő tagból kiemeljük előre a közös faktort, amelyek mind n qubitet tartalmaznak, és kapjuk, hogy

$$\begin{aligned}
|x\rangle_F &= \frac{1}{\sqrt{2^{n+1}}}(\left|\underbrace{0\dots0}_{n}\right\rangle(|0\rangle + e^{2\pi ix/2^{n+1}}|1\rangle) + e^{2\pi ix\cdot 2/2^{n+1}}|0\dots1\rangle(|0\rangle + e^{2\pi ix\cdot/2^{n+1}}|1\rangle) + \\
&+ \dots + e^{2\pi ix(2^{n+1}-2)/2^{n+1}}|1\dots1\rangle(|0\rangle + e^{2\pi ix/2^{n+1}}|1\rangle) = \\
&\frac{1}{\sqrt{2^n}}(\left|\underbrace{0\dots0}_{n}\right\rangle + e^{2\pi ix/2^n}|0\dots01\rangle + e^{2\pi ix\cdot 2/2^n}|0\dots10\rangle + e^{2\pi ix\cdot 3/2^{n+1}}|0\dots11\rangle\dots \\
&+ e^{2\pi ix\cdot 2(2^n-1)/2^{n+1}}|1\dots1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi ix/2^{n+1}}|1\rangle).
\end{aligned}$$

Az indukciós hipotézis miatt az első 2^n tagból álló tényezőre igaz a tétel, az utolsó tényezővel pedig éppen a kívánt eredményt kapjuk $n+1$-re. ■

2. Megmutatjuk, hogy a fönti képet az alábbi módon is írható

$$|x\rangle = |x_{n-1}, x_{n-2}, \dots x_0\rangle \to |x\rangle_F = \frac{1}{\sqrt{N}}(|0\rangle + e^{2\pi i\cdot 0,x_0}|1\rangle)(|0\rangle + e^{2\pi i\cdot 0,x_1x_0}|1\rangle) \quad (23)$$

$$\dots(|0\rangle + e^{2\pi i\cdot 0,x_{n-1}x_{n-2}\dots x_0}|1\rangle), \quad (24)$$

ahol

$$0, x_k x_{k-1}\dots x_0 = \frac{x_k}{2} + \frac{x_{k-1}}{4} + \dots \frac{x_0}{2^{k+1}},$$

illetve speciálisan

$$0, x_{n-1}x_{n-2}\dots x_0 = \frac{x_{n-1}}{2} + \frac{x_{n-2}}{4} + \dots \frac{x_0}{2^n},$$

bináris törtet jelent. A fönti (23) szorzat formulának megfelelő klasszikus képleten alapszik lényegében az úgynevezett (klasszikus) gyors Fourier transzformáció, az FFT algoritmusa. A megfelelő klasszikus szorzatformulát először Lánczos Kornél javasolta, aki doktori címét a Szegedi Egyetemen szerezte, ezért a 23 kifejezést Lánczos fölbontásnak fogjuk nevezni.

Ehhez az $|x\rangle_F = \frac{1}{\sqrt{N}}\otimes_{l=1}^{n}(|0\rangle + e^{2\pi ix2^{-l}}|1\rangle)$ formulában az $\exp(2\pi ix2^{-l})$ kiszámításánál a kitevőben a $2\pi i$-t szorzó $x2^{-l} = \sum_{s=0}^{n-1} x_s 2^{s-l} = x_0 2^{-l} + x_1 2^{1-l} + x_2 2^{2-l}\dots x_{n-1}2^{n-1-l}$ számoknak csak a tört része az érdekes, mert az egész rész exponenciálisa 1-et ad. Az összegben balról jobbra haladva a 2 kitevője minden tagban eggyel nagyobb. Nyilván addig az s-edik tagig bezárólag kaphatunk egynél kisebb számot, tehát törtet, amelyben szerelő $x_s 2^{s-l}$-ben az $s-l$ kitevő negatív, azaz ha $l > s$, mivel itt minden x_s legföljebb egy lehet. (Ez is csak akkor jelenik meg ténylegesen ha x_s nem 0, hanem 1.) Ezért az $\frac{1}{\sqrt{N}}\otimes_{l=1}^{n}(|0\rangle + e^{2\pi ix2^{-l}}|1\rangle)$ tenzorszorzat $l =$ 1-es indexű első tényezőjében csak az $s = 0$ tag adhat tört részt, és az fönti jelölés szerint $\frac{x_0}{2} = 0.x_0$. Az $l =$ 2-es tényezőben az $s = 0$ és az $s = 1$ tag marad $\frac{x_0}{4} + \frac{x_1}{2} = 0.x_1x_0$ és így

tovább, az $l = n$-re az összeg minden tagja egynél kisebb tört, és így ott éppen $0, x_{n-1}x_{n-2\ldots}x_0$ szerepel, azaz

$$\otimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i x 2^{-l}} |1\rangle\right) =$$
$$= (|0\rangle + e^{2\pi i \cdot 0, x_0} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0, x_1 x_0} |1\rangle) \ldots (|0\rangle + e^{2\pi i \cdot 0, x_{n-1}x_{n-2\ldots}x_0} |1\rangle)$$

és ezzel a kvantum Lánczos formulát bebizonyítottuk. ■

Közbevetőleg megmutatjuk, hogy ez a fölbontás hogyan szolgáltatja a klasszikus gyors Fourier transzformáció algoritmusát. A 22 és 23 szerint

$$\sum_{x=0}^{N-1} c_x |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} c_x \otimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i x 2^{-l}} |1\rangle\right) = \sum_{y=0}^{N-1} \tilde{c}_y |y\rangle . \qquad (25)$$

Szorozzuk a fönti egyenlőség két oldalát $\langle y'|$-vel, akkor a jobboldalon éppen $\tilde{c}_{y'}$-t kapjuk a bázisvektorok ortogonalitása miatt. Így

$$\tilde{c}_{y'} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} c_x \langle y'| \otimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i x 2^{-l}} |1\rangle\right) \qquad (26)$$

Az y' index helyett írjunk ismét y-t, és ennek megfelelően a jobboldalon $\langle y'|$ helyett $\langle y| = \langle y_1 y_{2\ldots} y_n|$-t. A belső szorzatban a megfelelő sorszámú qubiteket összeszorozva és figyelembe véve, hogy y_l maga is vagy 0 vagy 1 lehet továbbá, hogy $\langle 0|1\rangle = \langle 1|0\rangle = 0$, a szorzat minden tényezője egytagúvá redukálódik. $y_l = 0$ esetén az l-edik tényező $1 = 1 - y_l$ viszont $y_l = 1$ esetén $y_l e^{2\pi i x 2^{-l}}$. Így a belső szorzatot az alábbi móon írhatjuk:

$$\langle y_1 y_{2\ldots} y_n| \otimes_{l=1}^{n} (|0\rangle + e^{2\pi i x 2^{-l}} |1\rangle) = \prod_{l=1}^{n} \left(\langle y_l|0\rangle + e^{2\pi i x 2^{-l}} \langle y_l|1\rangle\right) = \prod_{l=1}^{n} \left(1 + (e^{2\pi i x 2^{-l}} - 1) y_l\right) \qquad (27)$$

Eszerint

$$\tilde{c}_y = \sum_{x=0}^{N-1} c_x \prod_{l=1}^{n} \left(1 + (e^{2\pi i x 2^{-l}} - 1) y_l\right) \qquad (28)$$

Most nézzük meg hogyan valósítható meg a QFT kvantumos kapukkal. Alkalmazzuk először az n-edik $|x_{n-1}\rangle$ qubitre a H Hadamard trafót. Az eredmény egyszerűen láthatóan

$$H |x_{n-1}\rangle = (|0\rangle + e^{2\pi i \cdot 0, x_{n-1}} |1\rangle)/\sqrt{2}$$

hiszen $e^{2\pi i \cdot 0, x_{n-1}} = \pm 1$, attól függően, hogy $x_{n-1} = 0$ vagy 1.

A folytatáshoz definiáljuk az R_k-val jelölt kétbites föltételes fázistoló kaput a következőképpen: Ha a kétbites kapu bemenetén $|x\rangle$ és $|y\rangle$ a számítási bázis elemei, akkor a kimeneten $|x\rangle \to e^{2\pi i x y / 2^k} |x\rangle$, $|y\rangle \to |y\rangle$ jelennek meg. A CNOT kapuhoz hasonlóan a bemenet x bitjét az R_k kapu target bitjének, y-t a kontrollbitjének nevezhetjük. Jelöljük most $R_k^{(j)}$-vel azt a kétbites föltételes fázistoló kaput amelynek kontrollbitje a j-edik qubit.

Ekkor $(R_n^{(n)} \dots R_3^{(3)} R_2^{(2)} H)\,|x_1\rangle = (|0\rangle + e^{2\pi i \cdot 0,x_1 x_2 \dots x_n}\,|1\rangle)/\sqrt{2}$, itt tehát minden R_k target bitje az első qubit, kontrollbitje pedig $|x_k\rangle$, vagyis a k-adik bemenő qubit. Alkalmazzuk ezután a második qubitre a következő transzformációsorozatot

$$R_{n-1}^{(n)} \dots R_3^{(4)} R_2^{(3)} H)\,|x_2\rangle = (|0\rangle + e^{2\pi i \cdot 0,x_1 x_2 \dots x_{n-1}}\,|1\rangle\,/\sqrt{2}$$

ahol most R_k kontrollbitje $k+1$-edik bemenő qubit

Ezt sorban folytatva az l edik qubiten $|x_l\rangle$-en is először egy H-t majd R_k-kat alkalmazunk a $k = 2, \dots, n-l+1$ indexekkel egymás után, mindig a megfelelő $k+l-1$-edik bemenetet használva kontrollbitnek. Az utolsó qubiten már csak egy H-t hajtunk végre, s az n db. kimenő biten az eredmény a következő:

$$\frac{1}{\sqrt{N}}((|0\rangle + e^{2\pi i \cdot 0,x_1 x_2 \dots x_n}\,|1\rangle)(|0\rangle + e^{2\pi i \cdot 0,x_{n-1} x_n}\,|1\rangle) \dots (|0\rangle + e^{2\pi i \cdot 0,x_n}\,|1\rangle))$$

ami éppen a keresett (23) állapot qubitjei csak éppen fordított sorrendben. Ezért a végén olyan úgynevezett SWAP (fordító) kapukat kell betenni, amelyek a l-edik és az $n-l$-edik qubit értékét megcseréli. Egy kétbites SWAP kapu hatása $|x\rangle \to |y\rangle$, $|y\rangle \to |x\rangle$ és ez egyszerűen láthatóan három CNOT kapu alkalmazásával egyenértékű, ahol a középső CNOT kontroll bitje azonos a két szélső targetbitjével (mutassuk meg!). A végrehajtott egyedi kapuk transzformációinak mindegyike unitér, ezért a teljes QFT is unitér.

Hány elemi művelet szükséges a tarnszformációhoz? Összesen $1+2+\dots n = n(n+1)/2$ kapu kell a fordításig, utána még $n/2$ db fordító SWAP, azaz $O(n^2) = O(\log N)^2$ a szükséges kapuk száma. Klasszikus FFT esetén $O(n2^n) = O(N \log N)$ db kapu vagy lépés kellene ehhez, tehát a QFT $\sim 2^n$ szer, azaz exponenciálisan gyorsabb mint a klasszikus FFT.

2 A Shor féle algoritmus számelméleti előzményei

Egy pozitív egész számot prímszámnak nevezünk, ha 1-en és önmagán kívül más egész számmal nem osztható. Az 1-et nem tekintjük prímnek. Már Eukleidész bizonyította hogy végtelen sok prímszám van és lényegében ismerte a számelmélet alaptételét is, amely szerint minden egész szám fölírható prímszámok szorzataként, éspedig a tényezők sorrendjétől eltekintve egyértelműen. Az alaptétel bizonyításra nézve lásd pl.
http://hu.wikipedia.org/wiki/A_számelmélet_alaptétele

Az összetett (nem prím) számok faktorizálására vonatkozó feladat a jelenlegi ismereteink szerint "nehéz", azaz a faktorizáláshoz szükséges lépésszám a szám jegyeinek számával a hatványfüggvénynél gyorsabban nő a leghatékonyabb klasszikus faktorizáló algoritmus esetén is. Meg kell azonban jegyezni, hogy nincs bizonyítva az, hogy nem létezik hatékony klasszikus algoritmus, amely a számjegyek számától polinomiálisan függő lépésszámban oldaná meg a faktorizációt. Ha sikerülne ilyen algoritmust találni, akkor az elektronikus információtovábbítás titkosságának jelenlegi módszere összeomlana, s ez új titkosítási

algoritmusok piacát nyitná meg. Ennek oka, hogy a jelenleg széles körben használatos nyilvános kulcsú un. RSA titkosírás két nagy prímszám szorzatának *gyors* faktorizálásának megoldhatatlanságán alapul. Emiatt igen nagy érdeklődést keltett, amikor 1994-ben Peter Shor közzétett egy olyan *kvantumos* algoritmust, amely polinomiális idő alatt oldja meg a faktorizációt. Az algoritmus egyrészt azon alapul, hogy a faktorizációval szemben a legnagyobb közös osztó megtalálására gyors klasszikus algoritmus ismeretes, másrészt pedig, hogy egy olyan szám megtalálását, amelynek a fölbontandó számmal van közös osztója, át lehet fogalmazni egy számelméleti függvény periódusának meghatározására, amely klasszikusan szintén nehéz feladat, viszont a perióduskeresésre kvantumosan gyors algoritmust lehet találni. Először tehát tételszerűen áttekintjük a szükséges számelméleti előzményeket, majd bemutatajuk a perióduskeresésre vonatkozó kvantumos algoritmust. Eközben röviden érintjük az RSA titkosítást is, mert az ahhoz szükséges előismereteket amúgy is föl kell dolgoznunk a Shor algoritmus megértése céljából.

2.1 Az LKO(a, b) megkeresésére vonatkozó euklideszi algoritmus:

Jelöljük a és b legnagyobb közös osztóját itt LKO(a, b)-vel, ez nyilván az a és b közös prímtényezőinek szorzata, ahol minden prímtényezőt a multiplicitásával együtt tekintünk. A prímtényezők megkeresése azonban nehéz, azonban két szám legnagyobb közös osztójának megkeresésére, amire a későbbiekben szintén szükségünk lesz, létezik egy egyszerű polinomiális algoritmus, amelyet euklideszi algoritmusnak nevezünk, mert ezt már Eukleidész leírta, és valószínűleg már Eudoxosz is ismerte.

Legyen $a > b > 0$ természetes számok, és legyen $a_0 \equiv a$, és $a_1 \equiv b$. Számítsuk az $a/b = a_0/a_1$ osztás maradékát, legyen ez a_2.

$$a_0 = k_1 a_1 + a_2, \qquad a_2 < a_1 \tag{1}$$

ahol k_1 valamilyen egész. Ezután osszuk a_1-t a_2-vel és legyen a maradék a_3, majd folytassuk ezt az eljárást tovább, az alábbiak szerint:

$$a_1 = k_2 a_2 + a_3, \qquad a_3 < a_2 \tag{2a}$$

$$\vdots$$

$$a_{j-1} = k_j a_j + a_{j+1}, \qquad a_j < a_{j-1} \tag{2b}$$

$$\vdots$$

$$a_{n-2} = k_{n-1} a_{n-1} + a_n, \qquad a_n < a_{n-1} \tag{2c}$$

$$a_{n-1} = k_n a_n + 0, \tag{2d}$$

Mivel az $a_0 > a_1 > a_2 > \ldots a_{n-1} > a_n$ sorozat pozitív egész számok szigorúan monoton csökkenő sorozata, az eljárásnak vége kell szakadnia, azaz véges sok lépésben el kell érnünk az $a_{n+1} = 0$- t.

1. Tétel a és b legnagyobb közös osztója éppen a_n.
(i) Ehhez először indukciót alkalmazva megmutatjuk, hogy a és b minden közös osztója osztja a_n-et. Induljunk ki abból, hogy a és b minden közös osztója osztja a_2-t is. Valóban, ha d közös osztó, akkor $a = a_0 = dn_0$ és $b = a_1 = dn_1$, valamilyen egész n_1-el, tehát $a_2 = a_0 - k_1 a_1 = d(n_0 - k_1 n_1)$, vagyis d valóban osztja a_2-t is. Folytatva az eljárást, hasonlóan kapjuk, hogy ha d osztja a_{j-1} et és a_j-t is, akkor osztja a_{j+1}-et is, mert 2b szerint $a_{j+1} = a_{j-1} - k_j a_j = n_{j-1}d - k_j n_j d$ valamilyen egész n_{j-1}, n_j számokkal. Így folytatva az eljárást az indukció a véges $n - edik$ lépésszámnál véget ér, és kapjuk, hogy a és b tetszőleges közös d osztója osztja a_n-et is. Mivel egy szám osztója a pozitív egészek körében mindig kisebb vagy egyenlő mint maga a szám, minden d közös osztóra igaz hogy kisebb mint a_n: $d \leq a_n$. Mivel ez minden közös osztóra igaz, igaznak kell lennie a legnagyobbra is azaz

$$\mathrm{LKO}(a, b) \leq a_n.$$

(ii) Ha viszont a fönti (2) egyenlőségsorozatban az utolsótól kezdve visszafelé indulunk el, akkor indukcióval látható, hogy minden a_j az a_n valamilyen egész számú többszöröse. $j = n$-re ez nyilvánaló, hiszen $a_n = 1a_n$, $j = n-1$ re pedig a fönti utolsó sor, (2d) szerint $a_{n-1} = k_n a_n$. A $j = n - 2-$re, helyettesítsük 2d-et 2c-be:

$$a_{n-2} = k_{n-1}k_n a_n + a_n = (k_{n-1}k_n + 1)a_n$$

Ezután ha tudjuk, hogy a_{j+1}-nek és a_j- nek a_n közös osztója, akkor (2b)-ből következik ez a_{j-1}-re is. Így folytatva az eljárást most a kisebb indexek felé haladva, végül érvényes lesz, hogy az a_n közös osztója az $a_1 = b$-nek és az $a_0 = a$-nak is. Más szóval a_n közös osztó, s így szükségképpen kisebb vagy egyenlő mint a legnagyobb közös osztó:

$$a_n \leq \mathrm{LKO}(a, b).$$

Mivel az (i) pont végén látott eredmény szerint ugyanakkor $LKO(a, b) \leq a_n$, következik, hogy

$$a_n = \mathrm{LKO}(a, b) \qquad \square$$

Fontos tény, hogy az osztás hatékony, azaz polinomiális algoritmus. (Ezt itt nem bizonyítjuk, de gondoljunk arra, ahogyan paíron osztunk: tizes számrendszerben minden lépésben egy nagyságrenddel csökken az osztandó) A fönti sorozatról is látható, hogy polinomiális, mert az a_j-k monoton csökkenő volta miatt

$$a_j = k_{j+1}a_{j+1} + a_{j+2} > k_{j+1}a_{j+2} + a_{j+2} = (k_{j+1} + 1)a_{j+2} \geq 2a_{j+2}$$

azaz

$$a_{j+2} < \frac{a_j}{2}.$$

Vagyis két egymást követő osztás után a jelentkező maradékok legalább megfeleződnek. Így ha n az a legkisebb kitevő, amelyre $a_0 = a \leq 2^n$, akkor a legrosszabb

esetben is, azaz, ha $\mathrm{LKO}(a_0, a_1) = 1$ lenne, a $2n$-edik osztásnál, azaz kevesebb mint $2 \log a_0$ lépésben akkor is célhoz érünk. Másszóval az euklideszi algoritmus *polinomiális*, tehát *hatékony.*

Alkossunk az egymást követő a_j-kból páronként kételemű oszlopvektorokat, melyekkel a fönti (2) rekurziós formuláknak a

$$\begin{pmatrix} a_j \\ a_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_j \end{pmatrix} \begin{pmatrix} a_{j-1} \\ a_j \end{pmatrix} \tag{3}$$

alakú transzformációk felelnek meg: $j = 1, \ldots n$, és $a_{n+1} = 0$. A $Q_j = \begin{pmatrix} 0 & 1 \\ 1 & -k_j \end{pmatrix}$ mátrixokból kiszámított $Q_n Q_{n-1} \ldots Q_1 = Q$ szozatmátrixot (melynek minden eleme egész szám) az $\binom{a_0}{a_1}$ vektorra alkalmazva az $\binom{a_n}{0}$:

$$Q_n Q_{n-1} \ldots Q_1 \binom{a_0}{a_1} = Q \binom{a_0}{a_1} = Q \binom{a}{b} = \binom{a_n}{0} \tag{4}$$

vektort kapjuk. Eszerint

$$a_n = \mathrm{LKO}(a, b) = q_{11} a + q_{12} b, \tag{5}$$

ahol a q_{11} és q_{12} a Q márix megfelelő elemei, s a konstrukcióból következően (lévén a csak egész elemeket tartalmazó Q_j mátrixok szorzatának elemei) maguk is egész számok. Vagyis $\mathrm{LKO}(a, b)$ *mindig fölírható* az a és b *egész együtthatós lineáris kombinációjként.*

Ennél többb is igaz azonban, nevezetesen, hogy a és b pozitív egészek legnagyobb közös osztója az a *legkisebb pozitív* szám, amely az $s = na + mb$ formába írható valamilyen egész n-nel és m-mel, azaz érvényes a

2. Bézout (vagy reprezentációs) tétel

$$\mathrm{LKO}(a, b) = \min_{n,m \in \mathbb{Z}} \{na + mb > 0\} \tag{6}$$

(n és m közül valamelyik szükségképpen nempozitív.) Ezt szokás Bézout féle fölbontásnak nevezni (É. Bézout a 18. sz-ban élt francia matematikus). Ez a tétel az LKO explicit meghatározásásra nem alkalmas, de elvi szempontból érdekes. és röviden a bizonyítást is bemutatjuk, noha nem lesz rá a későbbiekben szükségünk.

(i) Megmutatjuk, hogy $s = \min_{n,m \in \mathbb{Z}} \{na + mb\}$osztója a-nak és b-nek is, azaz közös osztó. Tegyük föl az ellenkezőjét azaz, hogy a legkisebb pozitív $s = na + mb$ alakú szám nem osztja a-t, és ebből ellentmondásra jutunk. Legyen tehát a/s maradéka r:

$$a = ks + r, \quad \text{ahol } \; 1 \leq r \leq s - 1. \tag{7}$$

Ebből következik, hogy $r = a - ks = a - k(na + mb) = (1 - kn)a + (-km)b$ egy olyan pozitív szám, amely a és b egész együtthatós lineáris kombinációja és (7) szerint *kisebb* mint s. De ez ellentmond annak, hogy s a *legkisebb* olyan pozitív szám, amely ilyen lineáris kombináció alakjába írható. Eszerint s -nek osztani

kell a-t, és hasonló eljárással azt kapjuk, hogy b-t is, s tehát közös osztó. Ebből az is következik, hogy kisebb vagy egyenlő a közös osztók legnagyobbikánál:

$$s \leq \mathrm{LKO}(a,b) \tag{8}$$

Másrészt, mivel $LKO(a,b) = l$ osztja a-t és b-t is: $a = q_a l$, $b = q_b l$, ezért osztania kell a pozitív $s = na + mb = (nq_a + mq_b)l$-et is. Mivel egy pozitív szám osztója mindig kisebb vagy egyenlő mint maga a szám, ezért $l \leq s$, azaz

$$\mathrm{LKO}(a,b) \leq s \tag{9}$$

(8) és (9) - ból következik, hogy

$$s = \mathrm{LKO}(a,b)\ \square. \tag{10}$$

Megjegyezzük még, hogy a Bézout fölbontás nem egyértelmű: ha pl. $q_1 a = q_2 b$ az a és b valamelyik közös többszöröse, akkor $s = (n + q_1)a + (m - q_2)b$ egy másik fölbontás. A fönti tétel segítséhével egyszerűen látható az 1. tétel (i) része is, azaz ha c osztja a-t és b-t, akkor c osztja $\mathrm{LKO}(a,b)$-t is. Legyen ugyanis $a = q_a c$ és $b = q_b c$. Mivel a Bézout tétel szerint a legnagyobb közös osztó az $\mathrm{LKO}(a,b) = nq_a c + mq_b c$ alakba írható, ezért nyilván osztható c-vel is.

2.2 A $\mathbb{Z}_N^*$ csoport

Legyen és a és N relatív prím, másképpen *koprím,* azaz $\mathrm{LKO}(a,N) = 1$, továbbá $a < N$. Adott N esetén azon a számok halmazát hozzávéve még az $a = 1$-et is, melyek ilyen tulajdonságúak jelöljük $\mathbb{Z}_N^*$-al.

Belátjuk, hogy a $\mathbb{Z}_N^*$ halmaz két elemének szorzatát N-nel osztva a maradék maga is relatív prím N-nel, azaz $\mathbb{Z}_N^*$ eleme. Ennél pontosabban, érvényes a

3. Tétel: A $\mathbb{Z}_N^*$ halmaz véges abeli csoport a $\bmod N$ szorzásra nézve.

Példa: legyen $N = 10$, a szorzótábla:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Bizonyítás:

(1) Először megmutatjuk, hogy a művelet nem visz ki a halmazból. Legyen a és b két elem $\mathbb{Z}_N^*$-ból, azaz $\mathrm{LKO}(a,N) = 1$ és $\mathrm{LKO}(b,N) = 1$. Kimutatjuk, hogy ebből következik, hogy $\mathrm{LKO}(ab \bmod N, N) = 1$.

a és b egyikének sincs közös osztója N-nel, lévén relatív prímek, emiatt N -nek és a-nak nincs közös prímtényezője, és ugyanez érvényes N és b esetére is. Ezért ab prímtényezős fölbontásában sincs benne N egyetlen prímtényzője sem, s így ab nem osztható N-nel. Így

$$ab = kN + s$$

ahol k és s egész, $1 \leq s \leq N-1$. Itt s-nek sem lehet közös p prímtényezője N-nel, mert ha lenne, akkor ez azt jelentené, hogy $N = pN_1$, $s = ps_1$, s így

$$ab = kp(N_1 + s_1)$$

lenne, tehát ab-nek és N-nek is lenne közös prímtényezője a p. Az ellentmondás miatt tehát $s \in \mathbb{Z}_N^*$.

Ez az (1) pont, a reprezentációs tétel segítségével is belátható, mert aszerint van olyan n_1 és m_1, hogy $n_1 a + m_1 N = 1$, illetve n_2 és m_2, hogy $n_2 b + m_2 N = 1$. Szorozzuk össze ezt a két egyenlőséget, kapjuk, hogy $(n_1 a + m_1 N)(n_2 b + m_2 N) = 1$, azaz $n_1 n_2 ab + m_1 n_2 bN + n_1 m_2 Na + m_1 m_2 N^2 = 1$, és vegyük figyelembe, hogy ab nem lehet osztható N-el, (mert mind a mind b relatív prímek N-el), azaz van olyan k, hogy $ab = kN + s$, ahol s a maradék: $1 \leq s \leq N-1$. A fönti szorzatban ab helyére $kN + c$-t írva azt találjuk, hogy van olyan q_1 és q_2 egész, hogy $q_1 c + q_2 N = 1$. Az 1. tétel szerint a $q_1 c + q_2 N$ alakú pozitív számok közül a legkisebb a c és N legnagyobb közös osztója, és ez itt láthatólag 1. Más szóval c is benne van a Z_N^*-ben.

(2)A közönséges szorzás asszociativitása és kommutativitása miatt a $\bmod N$ szorzás is asszociatív és kommutatív is.

(3) A fönti szorzásra nézve nyilvánvalóan egységelem az 1.

(4) Még azt kell belátnunk, hogy minden elemnek létezik a műveletre nézve inverze, azaz minden $a-$ra van olyan egyértelmű $b = a^{-1}$, hogy $ab = 1 \bmod N$.

Rögzítsünk ehhez egy a elemet és tekintsük az összes ab elemet miközben b végigfut a $\mathbb{Z}_N^*$ elemein. Ekkor a *különböző* b-khez tartozó ab-k *különbözők*. Ugyanis ha $ab \pmod N$ és $ab' \pmod N$ ugyanaz lenne valamilyen $b' < b < N$-re, akkor fönnállna, hogy $ab - ab' = 0 (\bmod N)$, azaz $ab - ab' = a(b - b') = kN$, valamilyen $k > 1$ egésszel. (k nem lehet 0, mert abból $b = b'$ következnék) Az $a(b - b') = kN$ egész szám láthatóan a és N valamilyen közös többszöröse. Ezek közül viszont a legkisebb szükségképpen aN, mivel a-nak és és N-nek nincs közös prímtényezője. Viszont $b - b'$ biztosan kisebb mint N azaz $a(b - b')$ kisebb mint a legkisebb közös többszörös, tehát mégsem lehet közös többszörös. Ellentmondásra jutottunk így valóban a különböző b-k hez tartozó $ab (\bmod N)$ számok melyek melyek az (1) pont szerint szintén a $\mathbb{Z}_N^*$ elemei, mind különbözőek, amíg b végigfut a koprímeken. Emiatt azt az általánosabb és minden csoportra jellemző tételt bizonyítottuk, hogy $ab (\bmod N)$ között $\mathbb{Z}_N^*$ minden eleme pontosan egyszer fordul elő. ebből következik, hogy lesz olyan és pontosan egy olyan $b = a^{-1}$-el jelölt elem amelyree $aa^{-1} = 1 \bmod (\mathrm{N})$. a^{-1} neve a multiplikatív inverze modulo N. □

Be lehet bizonyítani, hogy igaz a fönti tétel megfordítása is, abban az értelemben a csoport tulajdonság fönnállásából következik hogy akkor áll fönn, ha a és N relatív prímek, azaz a $\mathbb{Z}_N^*$ halmaz akkor és csak akkor csoport, ha ha a és N relatív prímek

Az $a \in \mathbb{Z}_N^*$ elem inverze az euklideszi algoritmussal explicite is megkonstruálható. Az előzőek szerint fönn kell ui. állnia az $aa^{-1} = kN + 1$ összfüggésnek valamilyen k-ra, hiszen éppen ez jelenti azt, hogy az aa^{-1} szorzás maradéka,

azaz a mod N szorzás eredménye 1. Ez másképpen azt jelenti, hogy $aa^{-1}-kN = 1$, amely éppen a 6 Bézout féle fölbontásnak megfelelő fölírása az a és N legnagyobb közös osztójának, amelyről tudjuk, hogy 1. Így a 4 szerint most az N és a legnagyobb közös osztójához vezető euklideszi algoritmust alkalmazva

$$Q\begin{pmatrix} N \\ a \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{11}$$

összefüggésnek megfelelően $q_{11}N + q_{12}a = 1$-ből kapjuk, hogy $q_{12} = a^{-1}$ (és $q_{11} = -k$). Azaz itt az euklideszi algoritmust nem az ismert legnagyobb közös osztó, hanem a Q szorzatmátrix q_{12} elemének meghatározására használjuk, mert ez adja a^{-1}-et. Ha itt q_{12} negatívnak adódik, ami előfordulhat, akkor tekintsük azt a legkisebb k_0 pozitív egészt amelyre $q_{12}+k_0N > 0$. k_0Na-t hozzáadva és ki is vonva a fönti Bézout fölbontáshoz kpjuk, hogy $(q_{11}-k_0a)N+(q_{12}+k_0N)a = 1$. s ekkor már egy pozitív $(q_{12} + k_0N) = a^{-1}$ inverzet kapunk.

A csoport tulajdonságból az is következik, hogy minden $a \in \mathbb{Z}_N^*$ -hez van olyan r szám amelyre $a^r = 1$ mod N Ezt a számot az a rendjének nevezzük, amely legföljebb a csoport elemeinek száma lehet.

2.3 Euler tétele és az RSA algoritmus

A $\mathbb{Z}_N^*$ halmaz számosságát a csoport rendjét– azaz az N-nél kisebb, az N-nel relatív prím számok számát – $\varphi(N)$-nel szokás jelölni. a $\varphi(N)$ függvényt Euler vezette be. Ezt az egész számokon értelmezett és egész értékű $\varphi(N)$ függvényt Euler vezette be, $\varphi(N)$-et az angol nyelvű irodalomban *totiens* függvénynek is szokás nevezni. A föntiek szerint a $\varphi(N) = |\mathbb{Z}_N^*|$ a $\mathbb{Z}_N^*$ csoport rendje.

|Euler tétele a következő: Legyen a és N relatív prímek, ekkor $a^{\varphi(N)} \equiv 1$ mod N.

Ekkor a és minden hatványa mod(N) a $\mathbb{Z}_N^*$ csoport eleme. A csoport tulajdonság miatt minden a-hoz létezik olyan r, hogy $a^r \equiv 1$, az $a, a^2, \ldots, a^r = 1$ számok a $\mathbb{Z}_N^*$ egy részcsoportját alkotják. Lagrange tétele szerint a részcsoport rendje osztója a csoport rendjének, ezért $\varphi(N) = kr$ valamilyen k egésszel, így $a^{\varphi(N)} = a^{kr} \equiv (a^r)^k = 1$.

(Lagrange tétele abból következik, hogy ha H egy adott részcsoportja G-nek, akkor az aH baloldali mellékosztályok a csoportelemek egy osztályozását, adják, azaz az a_iH és a_jH halmazok, vagy azonosak, vagy diszjunktak. Tekintsük ezután az összes különböző diszjunkt mellékosztályt, a_1H a_rH ahol minden mellékosztály csak egyszer szerepel. Ezek mindegyike azonos számosságú, éspedig éppen a $H = eH$ számosságával egyezik meg, amelyet , legyen ez n_H Így $rn_H = n_G$)

Euler tételének bizonyos értelemben speciális esete az un. kis Fermat tétel, mely szerint, ha. p prím, és a tetszőleges relatív prím p-vel akkor , akkor $a^p = a$ mod p, ui. $\mathbb{Z}_p^*$ ben az elemek száma $p-1$, tehát ha $a < p$, akkor $a^{p-1} = 1$ mod p, s ez ekvivalens a tétel állításával. A kis Fermat tétel átvihető az $a > p$, LKO$(a, p) = 1$ esetre is.

Most röviden tárgyaljuk az RSA algoritmust. Legyen

$N = pq$, ahol p és q prímek. Az N-nél kisebb, vele *nem* relatív prímek nyilván p és q többszörösei, $q, 2q, \ldots$ $(p-1)q$ illetve $p, 2p, \ldots (q-1)p$, s ezek

száma $p-1+q-1$. Emiatt a relatív prímek száma $N-1-(p-1+q-1) = N-p-q+1 = (p-1)(q-1)$. Ha ismerjük p-t és q-t akkor $\varphi(N) = (p-1)(q-1)$ könnyen meghatározható, egyébként azonban a feladat nehéz. Ezen alapszik az RSA algoritmus.

Az algoritmust, melyet 1980-ban közölt R. Rivest, Shamir és Adleman arra használjuk, hogy A titkos üzenetet küldjön B-nek. B választ egy nagy összetett N számot, amely két prím szorzata $N = pq$, továbbá egy $k < N$ számot, amely relatív prím N -nel és amely relatív prím $\varphi(N) = (p-1)(q-1)$-el is. B a p-t és q-t illetve $\varphi(N)$-et gondosan titokban tartja, viszont nyilvánosan elküldi k-t (a használandó **kódot**) és N-et A-nak. Ez a $P = (N, k)$ a nyilvános kulcs. A az üzenetét számsorozattá alakítja, legyen ez $a < N$, és előállítja a

$$b = f(a) = a^k (\mathrm{mod}\, N)$$

számot, amelyet gyorsan ki tud számolni, és elküldi Bobnak. Tegyük föl, hogy a koprím N-nel, ami rendkívül valószínű, ha N nagy, de ez ellenőrizhető is. Ezután Bob gyorsan vissza tudja fejteni az üzenetet, ha kiszámítja k multiplikatív inverzét a $\mathbb{Z}_N^*$ csoportban, azaz megkeresi azt a d számot amelyre $kd = 1 \mod \varphi(N)$. Ez a d a **dekódoláshoz** használt szám. A d explicit megkeresésére, a 11 szerint az $\mathrm{LKO}(\varphi(N), k)$ euklideszi algoritmushoz tartozó Q mátrix megfelelő elemét.kell kiszámtani, s ez a föntiek szerint gyorsan megtalálható, ha tudjuk k-t és $\varphi(N)$-et. B, akinél megvan d, akkor

$$f^{-1}(b) = b^d (\mathrm{mod}\, N) = a^{kd} (\mathrm{mod}\, N) = a^{m\varphi(n)+1} (\mathrm{mod}\, N) = a (\mathrm{mod}\, N)$$

Aki csak N-et és a-t ismeri nem tudja meghatározni d-t, mert ahhoz ismernie kellene $\varphi(N)$-et, amihez faktorizálnia kellene N-et, mint tudjuk nehéz feladat. az RSA keretében arra is mód van, hogy B hitelesítse aláírással az üznetét. Ehhez elküldi az s aláíráshoz tartozó a titkos d kóddal előállított $s_1 = s^d \mod N$ kódolt üzenetet. Az előzőek szerint most $s_1^k = s \mod(N)$, amelyet A a k nyilvános kulccsal visszakódol és meggyőződik róla, hogy ez B megbeszélt aláírása. Ugyanis csak a B által használt titkos d esetén kapjuk vissza így s-et. Ha tehát $s_1^k = s \mod(\mathrm{N})$, ahol s a megbeszélt aláírás, akkor A biztos lehet benne, hogy az üzenet attól érkezett, aki azt d-vel kódolta, azaz B-től, aki egyedül ismeri d-t .

2.4 Periódus keresés és faktorizáció

Most megmutatjuk, hogy az N szám prímtényezőkre bontása, visszavezethető egy egész számokon értelmezett függvény periódusának megkeresésére, úgy hogya függvény periódusának ismeretében a faktorizáció már hatékonyan elvégezhető. (Ebből már gondolható, hogy a periódus keresésre sem ismert hatékony klasszikus algoritmus). Tekintsük az N számhoz tartozó $\mathbb{Z}_N^*$ csoportot. Mint föntebb Euler tétele kapcsán láttuk, a csoporttulajdonságból következik, hogy tetszőleges $a \in \mathbb{Z}_N^*$-hoz létezik egy olyan r szám, amelyre $a^r = 1 \mod N$, a legkisebb ilyen

szám az a elem rendje a csoportban. Ebből következik hogy ha N és $a < N$ relatív prím, azaz $\mathrm{LKO}(a, N) = 1$, azaz $a \in \mathbb{Z}_N^*$, akkor az

$$f_{N,a}(x) = a^x (\mathrm{mod}\, N)$$

egész x-eken értelmezett függvény ($x \in \mathbb{N}$) periodikus. Más szóval létezik olyan pozitív egész $r > 0$, hogy $f_{N,a}(x+r) = f_{N,a}(x)\ \forall x$ re. Valóban, a föntiek szerint ez az r éppen az a elem rendje a $\mathbb{Z}_N^*$ csoportban.

6. **Tétel** Legyen r az $f_{N,a}(x) = a^x (\mathrm{mod}\, N)$ függvény periódusa, és legyen
(i) r páros,
(ii) $a^{r/2} \neq -1 (\mathrm{mod}\, N)$.

Ekkor létezik a nemtriviális $\mathrm{LKO}(N, a^{r/2} \pm 1)$, (azaz nem N és nem 1), tehát ennek megkeresésével N egy osztóját hatékonyan meg lehet találni.

Bizonyítás. Legyen $a^r = 1\ (\mathrm{mod}\, N)$, és r páros akkor $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$-nek nemtriviális osztója N. Valóban $(a^{r/2} - 1)$ nek nem lehet osztója, mert akkor már $r/2$ is periódusa lenne a fönti függvénynek. Ha $(a^{r/2} + 1)$-nek osztója lenne, az azt jelentené, hogy $a^{r/2} = -1 (\mathrm{mod}\, N)$, de ezt kizártuk. Így van egy nemtriviális közös osztójuk, amelyet r ismeretében az euklideszi algoritmussal hatékonyan meg lehet keresni.□

Tekintsük példaként azt legkisebb nemtriviális esetet, ahol N két páratlan prím szorzata, ez $N = 15$. A $\mathbb{Z}_{15}^*$ elemei ekkor a következők: 1,2,4,7,8, 11,13, 14. Legyen $a = 11$, akkor $a^2 = 121 = 1 (\mathrm{mod}\ 15)$. azaz a periódus $r = 2$, $a^{r/2} - 1 = 10$, $a^{r/2} + 1 = 12$, ezeknek valóban nem osztója 15, de a legnagyobb közös osztók $\mathrm{LKO}(10, 15) = 5$, illetve $\mathrm{LKO}(12, 15) = 3$, éppen a kívánt faktorokat adják. Egyszerűen látható ebben a példában, hogy ha $a = 2, 4, 7, 8, 11, 13, 14$.akkor a megfelelő r-ek rendre a 4,2,4,4,2,4,2 számok, azaz mind páros, és az $a = 14$ esetet kivéve ($14^{2/2} = -1 \mathrm{mod}(15)$) mindegyik teljesíti az $a^{r/2} \neq -1 (\mathrm{mod}\, N)$ (ii) föltételt is.

Meg lehet mutatni, hogy ha adott N esetén egy vele koprím a-t véletlenszerűen választunk, akkor annak valószínűsége, hogy a rendje vagyis r páros és $a^{r/2} \neq -1 (\mathrm{mod}\, N)$, mindig nagyobb mint 1/2. illetve, ha N különböző prímfaktorainak száma m, akkor ez a valószínűség nagyobb mint $1 - 1/2^m$.

Az is egyszerűen belátható, hogy az $f_{Na}(x)$ függvény kiszámítása legföljebb $O(logN)^3$ lépésben klasszikusan is végrehajtható.

3 A kvantumos perióduskeresési algoritmus

Egy $f(x)$ függvény periódusának megtalálása klasszikusan nem hatékony algoritmus, de a QFT segítségével azzá tehető. Más feladatoknál is érdekes lehet egy függvény periódusának meghatározása, de szempontunkból, a faktorizációs probléma megoldása szempontjából az $f(x) := f_{N,a}(x) = a^x \bmod N$ periódusának megtalálása az érdekes, mert mint az előbbi szakaszban láttuk, az $f_{N,a}(x)$ periódusának, r-nek ismeretében, az $\mathrm{LKO}(N, a^{r/2} \pm 1)$, gyorsan meghatározható, tehát N gyorsan faktorizálható.

Legyen tehát egy akár klasszikus komputerünk, amely kiszámítja a periodikus $f(x)$ értékét, ahol x célszerűen 0–tól $M \simeq N^2$ ig fut. A függvény

kiszámítása gyors, polinomiális algoritmus. Ennek a függvénynek a periódusát fogjuk majd megkeresni egy QFT segítségével.

Tekintsünk egy kvantumos eszközt, amelynek két db. egyenként n bites regisztere van, ahol $n \geq \log M = 2\log N$. Ha most kezdetben az első regiszter minden qubitjébe $|0\rangle$ kerül és ezek *mindegyikén* végrehajtunk egy Hadamard transzformációt, akkor mint egyszerűen látható, eredményül a

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \tag{12}$$

állapotot kapjuk, azaz a számítási bázis elemeinek egyenlő súlyú (és azonos fázisú) úgynevezett szimmetrikus szuperpozícióját.

Tekinsük most a két regiszter olyan együttes transzformációját, amely a számítási bázison

$$U_f : \quad |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle \tag{13}$$

alakú unitér transzformáció, tehát elvileg kvantumosan realizálható. Itt $f(x)$ a gyorsan kiszámítható függvény. Ha ezt a transzformációt úgy hajtjuk végre, hogy az első regiszterbe a fönti szimmetrikus szuperpozíciót tesszük, akkor az eredmény

$$U_f : \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|f(x)\rangle \tag{14}$$

ahol az utóbbi $f(x)$ periodikus volta $f(x+r) = f(x)$ miatt az

$$\begin{aligned} \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{K-1} \sum_{x=0}^{r-1} |x+jr\rangle|f(x)\rangle = \\ = \tfrac{1}{\sqrt{M}} \left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \ldots + |r-1\rangle|f(r-1)\rangle + \right. \\ \left. (|r\rangle|f(0)\rangle + |r+1\rangle|f(1)\rangle + \ldots + |2r-1\rangle|f(r-1)\rangle) + \right. \\ \vdots \\ \left. |(K-1)r\rangle|f(0)\rangle + |(K-1)r+2\rangle|f(1)\rangle + |(K-1)r+x_1\rangle|f(x_1)\rangle\right) = \end{aligned} \tag{15}$$

$$= \frac{1}{\sqrt{M}} \sum_{x=0}^{r-1} \Big(\sum_{j=0}^{K-1} |x+jr\rangle\Big)|f(x)\rangle \tag{16}$$

alakba is írható, ahol $(K-1)r + x_1 = M-1$, valamilyen x_1-el, amelyre $0 \leq x_1 \leq r-1$, .ugyanakkor $Kr > M-1$, azaz $Kr \geq M$. (Speciális az az eset, ha $Kr = M$). Ugyanakkor $Kr + 1 > M$, amiből $M/r < K + 1/r < K + 1$) tehát K az a legkisebb egész szám, amely nagyobb vagy egyenlő mint M/r azaz $M/r \leq K < M/r + 1$ egész szám, amelyre persze most még r-et nem ismerjük.).

Most ebben az állapotban végrehajtunk egy mérést a második regiszteren. Ennek nyomán az valamelyik $|f(x_0)\rangle$ állapotba kerül, ahol x_0 a $0, 1 \ldots r-1$

számok valamelyike, a teljes állapot pedig a

$$\frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |x_0 + jr\rangle) \, |f(x_0)\rangle \tag{17}$$

Az első regiszter ezután tehát

$$|\Phi_{x_0}\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |x_0 + jr\rangle = \sum_{j=0}^{K-1} c_x \, |x\rangle \tag{18}$$

állapotú, ahol

$$c_x = \frac{1}{\sqrt{K}} \delta_{x,x_0+jr} \tag{19}$$

Ebből most egy QFT-vel fogjuk megállapítani r-et. A QFT hatása

$$\sum_{x=0}^{M-1} c_x \, |x\rangle \rightarrow \sum_{y=0}^{M-1} \tilde{c}_y \, |y\rangle$$

ahol

$$\tilde{c}_y = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} c_x e^{2\pi i x y/M} \tag{20}$$

Írjuk be ide a fönt fönt kapott $c_x = \frac{1}{\sqrt{K}} \delta_{x,x_0+jr}$ -t:

$$\tilde{c}_y = \frac{1}{\sqrt{MK}} \sum_{j=0}^{K-1} e^{2\pi i (x_0+jr) y/M} = \frac{1}{\sqrt{MK}} e^{2\pi i x_0 y/M} \sum_{j=0}^{K-1} e^{2\pi i j r y/M}, \tag{21}$$

ahol összegezni most csak arra K db tagra kell, amelyek esetén a $c_x = \frac{1}{\sqrt{K}} \delta_{x,x_0+jr}$-k nem tűnnek el. Mérjünk ezután az első regiszteren a számítási bázisban.. A mérés után az állapot a $\sum_{j=0}^{M-1} \tilde{c}_y \, |y\rangle$ lineárkombináció valamelyik összetevője: $|y_0\rangle$ lesz, és annak a valószínűsége, $|y_0\rangle$-t mérek:

$$|\tilde{c}_{y_0}|^2 = \frac{1}{MK} \left| \sum_{j=0}^{K-1} e^{2\pi i (j r y_0/M)} \right|^2 \tag{22}$$

A módszer ezután azon alapul, hogy meg lehet mutatni, hogy ez az összeg akkor nagy, ha ry_0/M közel van egy egész számhoz.

Az általános eset vizsgálata helyett tegyük most föl, bár ez nem szükségszerű, hogy M/r egész, ez annak felel meg, hogy a 15 kiefjtésben x_1 éppen a legnagyobb érték: $r-1$, ekkor mint látható $M = Kr$ azaz $K = M/r$. Ebben az esetben az összeg csak akkor nem tűnik el, ha

$$y_0/(M/r) = y_0/K =: s$$

egész szám. Az összeg ugyanis ekkkor

$$\sum_{j=0}^{K-1} e^{2\pi i(jry_0/M)} = \sum_{j=0}^{K-1} e^{2\pi i(jy_0/K)}$$

a K-adik komplex egységgyökök összege. Ez eltűnik, kivéve ha $y_0 = Ks$, amikor is minden tag 1, és a tagok összege K. Képletben: $\sum_{j=0}^{K-1} e^{2\pi ijy_0/K} = K\delta_{y_0,Ks}$. Eszerint $|\tilde{c}_{y_0}|^2 = \frac{K}{M}\delta_{y_0,Ks} = \frac{1}{r}\delta_{y_0,Ks}$. A mérés eredménye ekkor tehát csak olyan lehet, hogy

$$y_0 = Ks = \frac{M}{r}s,$$

ahol most M/r és lévén az s egész. Megjegyezzük, hogy s szükségképpen kisebb mint r, mert $y_0 < M$. Az

$$\frac{y_0}{M} = \frac{s}{r}$$

összefüggés alapján a mérésből megkapott y_0-ból és az eleve ismert M-ből az y_0/M-et addig egyszerűsítjük, amíg a számláló és a nevező relatív prímek lesznek. Ekkor a nevező nagy valószínűséggel éppen r,.ami akkor következik be, ha s és r relatív prímek.

Előfordulhat azonban, hogy s-nek és a keresett r- nek van közös faktora. Ez azonban kevéssé valószínű, mert a nevezetes prímszámtétel szerint az r-nél kisebb prímek száma legalább $r/(2\log r)$, tehát annak a valószínűsége, hogy s prím, s emiatt relatív prím r-rel legalább $1/(2\log r) > 1/2\log N$ Ha tehát az algoritmust $2\log N$-szer ismételjük, akkor nagy valószínűséggel olyan törtet kapunk, amelynek nevezője r. Az, hogy a kapott eredmény eredényünk jó-e gyorsan ellenőrizhető, hiszen a fordított kérdés, hogy egy adott r tényleg periódusa e a függvénynek – azaz igaz-e, hogy a választott a rendje éppen r – hatékonyan megválaszolható. Vannnak más, gyorsabb módszerek is ennek megoldására, ezzel itt nem foglalkozunk.

Kérdés mi a helyzet ha M/r nem egész. Az előbb mondottak szerint a 22 összeg akkor nagy, ha ry_0/M közel van egy egészhez, ebből a megfelelő r-et az ry_0/M lánctört alakba fejtésével lehet megkeresni, lsd Preskill, ill Nielsen Chuang.

Mint láttuk a QFT-hez szükséges műveletek száma $O(logN)^2$, és mint említettük az $f_{Na}(x)$ függvény kiszámítása $O(logN)^3$ számú lépést igényel. Így egy QFT-t végrehajtó géppel a faktorizáció $O(logN)^3$ számú lépésben azaz hatékonyan megoldható lenne.

4 Kvantumos titkosítás kétállapotú kvantumrendszerrel Kriptográfia

4.1 Klasszikus kriptográfia

Egy szöveg rejtjelezése a titkosírás vagy idegen szóval kriptográfia régóta használatos üzenetek küldésésre, kommunikációra. A kvantummechanika kétállapotú rend-

szerei pl. fotonok polarizációja erre egy érdekes lehetőséget nyújt. Mielőtt ezt tárgyalnánk röviden ismertetjük az úgynevezett klasszikus titkos kulcsú titkosírás módszerét. A szöveg titkosítást egy kulcs segítségével végezzük, amely az egyes betűket számokkal helyettesíti. Pl::

A	*Á*	*B*	*C*	*D*	*E*	*É*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
N	*O*	*Ö*	*P*	*Q*	*R*	*S*	*T*	*U*	*Ü*	*V*	*W*	*X*	*Y*	*Z*
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Helyettesítsünk minden betűt 5-tel nagyobb számmal Mod 30. Ekkor A KOCKA EL VAN VETVE szöveg így néz ki: E ÖSGÖE IP AER AIXAI. Az üzenet olvasásához kulcsot ismernie kell küldőnek és a fogadónak is, de másoknak nem. Egy ilyen egyszerű módon kódolt szöveg azonban gyorsan feltörhető és vagyis a kulcs megfejthető.

Azonban ha a betűt kódoló számhoz más és más véletlenszerűen generált számot adunk, majd az így kapott szöveget írjuk le, az már nem lesz megfejthető, csak annak számára aki a kulcsot is ismeri. Ez utóbbi a Vernam kód, Gilbert Vernam amerikai kutató nevéről, aki ezt a módszert 1918-ban javasolta. A kulcsot azonban időről időre változtatni kell, mert egyébként az is megfejthető. Be lehet ugyanis bizonyítani, ez 1925 körül történt, hogy a biztonságos továbbításhoz, vagyis a megfejthetetlenséghez az kell, hogy a kulcs és a kódolandó szöveg hossza azonos legyen. Ezt a kulcsot egyszeri blokknak (one time pad) szokás nevezni. Ilyen titkosírással üzent Che Guevara a boliviai őserdőkből Fidel Castronak, illetve Dr. Sorge a szovjet elhárítás Japánban kémkedő tisztje a II. világháborúban. Ő pl. Németország statisztikai évkönyvének előre megbeszélt számtáblázatait használta a kódolásra. Általában a kulcs azonosságának a biztosítása a kritikus pont a küldő és a fogadó részéről. Megjegyezzük, hogy manapság pl. banki adatok továbbítására más módszert használnak, egy úgynevezett nyilvános kulcsú titkosírást, amely azonban valójában szintén alkalmaz egy gyakorlatilag megfejthetetlen, titkos kulcsot is. Ezt az un. RSA algoritmuson alapuló módszert itt nem ismertetjük.

Erre lehet találni olyan kvantumos módszert, amelyet elvileg is titkosan lehet elküldeni két fél Aliz és Bob között. Ezt kvantumos kulcstovábbításnak, vagy újabbaan kvantumos kulcsgenerálásnak szokás nevezni, ez az alapja a kvantumos titkosírásnak a kvantumkriptográfiának.

4.2 Kvantumkriptográfia

A kvantumkriptográfia visszatérés a titkos kulcsú titkosíráshoz. A két fél: Aliz (A) és Bob (B) üzenetei nyilvánosak lehetnek, de a kódoláshoz és a visszafejtéshez titkos kulcsot használnak, amelyet csak ők ismernek. A kvantumos módszer valójában a titkos kulcs átviteléhez szükséges A és B között, ezért a módszert kvantumos kulcstovábbításnak (vagy kulcs-szétosztásnak) szokás nevezni. Az angol quantum key distribution szavak rövidítéseként QKD módszerről illetve protokollról is szoktak beszélni. A kulcsot mint megfelelő qubitek sorozatát juttatják el egymáshoz, így ha azokon egy harmadik, illetéktelen személy, mérést

hajtana végre, akkor elrontja az eredeti állapotot, amit a két fél statisztikai módszerek alapján észre tud venni. Ugyanez a helyzet, ha a kvantumos csatornát figyelve csak másolni szeretné a kulcs qubitjeit, mert az alább ismertetendő nemklónozhatósági tétel miatt ezt nem tudja megtenni, csak ha ortogonálisok a qubitek. Ez egyúttal mutatja is hogy a kódolást nemortogonális módon kell végrehajtani.

4.3 Nemklónozhatósági tétel.

4.3.1 Első változat

Az eredeti nemklónozhatósági tétel arra az esetre vonatkozik, hogy ha a H Hilbert térből (regiszterből) a H_E-ben lévő regiszterbe óhajtunk másolni állapotokat. Tegyük föl, hogy ψ és φ nemortogonális állapotok H-ban: $\langle\varphi|\psi\rangle \neq 0$ és azt kívánjuk, hogy egy alkalmas unitér transzformáció segítségével bármelyiket át tudjuk másolni H_E-be, anélkül, hogy az eredeti állapotok megváltoznának. Azaz foltesszük, hogy létezik olyan unitér transzformáció, amellyel

$$U : |\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$$
$$U : |\varphi\rangle \otimes |0\rangle \rightarrow |\varphi\rangle \otimes |\varphi\rangle .$$

Ha most összeszorozzuk skalárisan a kiinduló és a transzformált állapotokat, abból vagy $\langle\varphi|\psi\rangle = 0$ következik, amit kizártunk, vagy $\langle\varphi|\psi\rangle = 1$,amiből viszont $\varphi = \psi$ következik.Tehát csak egy állapotot lehet klónozni, vagy csak ortogonális állapotokat, legalábbis ha kikötjük, hogy a transzformáció unitér legyen.

4.3.2 Második változat

Nem lehet különbséget tenni két nem ortogonális állapot között anélkül, hogy megzavarnánk az állapotokat. Legyen ψ és φ két nem ortogonális állapot, $\langle\varphi|\psi\rangle \neq 0$ és tegyük föl, hogy van egy unitér trafó a $H \times H_E$-ban = úgy hogy az mind ψ és φ is változatlanul hagyja. H_E Eve Hilbert tere.

$$U : |\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |u\rangle \tag{23}$$
$$U : |\varphi\rangle \otimes |0\rangle \rightarrow |\varphi\rangle \otimes |v\rangle \tag{24}$$

Mivel a trafó unitér

$$\langle\varphi|\psi\rangle = (\langle 0| \otimes \langle\varphi|)(|\psi\rangle \otimes |0\rangle) \tag{25}$$
$$= \langle u| \otimes \langle\varphi|)(|\psi\rangle \otimes |v\rangle) \tag{26}$$
$$= \langle\varphi|\psi\rangle \langle u|v\rangle \tag{27}$$

Így mivel $\langle\varphi|\psi\rangle \neq 0$, $\langle u|v\rangle = 1$, azaz mivel a vektorok normáltak, $u = v$ azaz a végeredményben nincs különbség akár ψ akár φ az induló állapot.

4.4 A BB84-es protokoll

Az első QKD protokoll, a BB84-nek nevezett módszer, amelyet C. Bennett és Brassard javasolt 1984-ben. Ez két nem ortogonális állapotot használ a kód előállítására. A BB84 a következőképpen működik. A előállít egy *klasszikus* véletlen bitsorozatot, melynek k-adik tagja legyen a_k. Ezen bitsorozat egy alkalmas részsorozata lesz majd a titkos kulcs. Ezt fogja kódolni egy $|\varphi_k\rangle$ qubit sorozattal, de a kódolás módjának meghatározásához egy *másik* véletlen *klasszikus* bitsorozatot a'_k-t használ a következőképpen: a_k-t attól függően kódolja két különböző bázisban, hogy mi az a'_k értéke. Azért, hogy fizikailag is el tudjuk képzelni a dolgot, a qubitekről konkrétan mint fotonok polarizációs állapotairól fogunk beszélni, a jelenleg már előrehaladott stádiumban lévő kísérleteknél valóban ezeket is használják.

A két bázist a következőképpen választjuk. Az egyiket Z bázisnak nevezzük, amelynek bázisvektorai $|H\rangle$ és $|V\rangle$ a horizontálisan, (azaz vízszintesen) illetve vertikálisan (azaz függőlegesen) polarizált fotonállapotot jelentik. Ezeket ortonormáltnak tekinthetjük, mivel $\langle H|V\rangle = 0$, $\langle H|H\rangle = 1$, $\langle V|V\rangle = 1$. A Z bázis elemei legyenek $|H\rangle$ vagy $|V\rangle$ Eszerint, ha $a'_k = 0$, akkor a Z bázist használja, amelynek elemei $|H\rangle$ vagy $|V\rangle$ vagyis ha ha $a_k = 0$ akkor $|\varphi_k\rangle = |H\rangle = \longleftrightarrow$ illetve, ha $a_k = 1$, akkor $|\varphi_k\rangle = |V\rangle = \updownarrow$. Viszont, ha $a'_k = 1$, akkor az X bázist használja, és ekkor, ha $a_k = 0$ akkor, $|\varphi_k\rangle = |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = |\nearrow\rangle$ illetve ha $a_k = 1$, akkor $|\varphi_k\rangle = |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = |\nwarrow\rangle$. Ezután A átküldi a $|\varphi_k\rangle$ kvantumos véletlen kódsorozatot B-nek, aki mérést hajt végre a $|\varphi_k\rangle$ állapotokon. Mérőberendezését ő is véletlenszerűen állítja be Z vagy X irányba egy általa választott b'_k klasszikus bitsorozat segítségével, ugyanazon előírás szerint mint A. Vagyis, ha $b'_k = 0$ akkor B is Z irányban mér, míg ha $b'_k = 1$, akkor X irányban. A mérés eredményétől függően ő is létrehozza saját *klasszikus* b_k bitsorozatát ugyanazon előírás szerint ahogyan A, azaz ha a mérési eredmény a Z beállítás során H, akkor $b_k = 0$, ha V akkor $b_k = 1$, illetve ha a z Világos, hogy ha B éppen véletlenül azonos bázisban mért mint amelyben A kódolt, akkor az eredmény elvileg egységnyi valószínűséggel ugyanaz mint amit A kódolt. Ha viszont B nem azonos bázisban mért mint amelyben A kódolt, akkor az eredménye csak $1/2$ valósznűséggel esik egybe a_k-val. Az alább látható táblázatban összefoglalva láthatók a lehetséges kimenetelek, a táblázat 3-6 sorában a 4–7 oszlopokban a megfelelő mérési valószínűségeket adtuk meg:

		$\|\varphi_k\rangle$	$b'_k = 0$		$b'_k = 1$	
			$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|A\rangle$
$a'_k = 0$	$a_k = 0$	$\|H\rangle$	1	0	1/2	1/2
$a'_k = 0$	$a_k = 1$	$\|V\rangle$	0	1	1/2	1/2
$a'_k = 1$	$a_k = 0$	$\|D\rangle$	1/2	1/2	1	0
$a'_k = 1$	$a_k = 1$	$\|A\rangle$	1/2	1/2	0	1
			$b_k = 0$	$b_k = 1$	$b_k = 0$	$b_k = 1$

Ezek után B egy nyilvános csatornán közli A-val az ő b'_k sorozatát, de titokban tartja b_k-kat. A most már meg tudja mondani B-nek, hogy melyek voltak ezek

közül olyanok, amelyekkel az ő kódolási módja megegyezett, azaz kiválasztják azokat a vesszőtlen elemeket, amelyekre a vesszősek megegyeztek. Látható, hogy ha $b'_k = a'_k$ akkor $b_k = a_k$ egységnyi valószínűséggel. Az ezeknek a k-nak megfelelő biteket megtarthatják mint titkos kulcsot ekkor ugyanis a kiválasztott a_k-k részhalmaza megegyezik a megfelelő b_k halmazával a másik oldalon. Ha valaki viszont csak a vesszős bitsorozatról szerez tudomást, számára az a_k (és b_k-k is) egyforma, azaz 1/2 valószínűséggel lehetnek 0-k vagy 1-ek . Hiába tudja meg valaki a nyilvános csatorna lehallgatásával a b'_k-k értékét, annak alapján pontosan 1/2 annak a valószínűsége, hogy a_k értéke 0 volt vagy 1, azaz nem jut információhoz.

Valójában azonban A és B nem lehetnek biztosak abban, hogy a két megtartott bitsorozat pontosan azonos, aminek két fő oka lehet. Egyrészt lehetséges, hogy maga a qubiteket átvivő csatorna nem tökéletes, azaz zajos, másrészt előfordulhat, hogy van egy harmadik személy, aki lehallgatja az átvitt információt. Ezt a személyt E-nek szokás nevezni az angol "eavesdropper" (hallgatózó) szó miatt. Természetesen E-nek az az érdeke hogy A és B ne vegyék észre, hogy ő lehallgatta az üzenetet. A kvantumos csatorna használata miatt azonban A tudomást szerezhet arról, hogy a csatornát lehallgatják. Hogy ezt hogyan tehetik meg, az alábbiakban tárgyaljuk.

E két módon próbálhat tudomást szerezni arról, hogy milyen $|\varphi_k\rangle$ qubit állapot ment át A és B között. Egy primitív módszer lehet ha E mérést hajt végre a qubiteken. Tudjuk azonban, hogy a kvantummechanikában egy mérés általában befolyásolja az állapotot kivéve, ha E abban a bázisban mér, amelyben A kódolt. Noha E esetleg tudja azt, hogy A melyik két bázisban (az X vagy a Z bázisban) kódolt, mivel ez véletlenszerűen történik, E még e tudás birtokában is átlagosan csak méréseinek felében nem fogja megváltoztatni az eredményt. Maguknak a választott bázisoknak a száma is lehet több stb. Egyébként, ha a kvantumos információátvitel egyes fotonokkal történik a közbeavatkozás nyomán a foton elnyelődik és meg sem érkezik B-hez.

Egy ravaszabb módszer lehet emiatt, ha E megpróbálja lemásolni az átvitt qubit értékét egy általa külön erre a célra használt kvantumregiszterbe. Ezt azonban szintén nem tudja megtenni a nemklónozhatósági tétel második változata miatt:

Tehát látjuk, hogy vagy a csatorna zajossága miatt vagy E közbevatkozása miatt az átvitt qubitrendszer megváltozik. Erről A és B olymódon vesz tudomást, hogy föláldozza a megtartott és a közbeavatkozás nélkül biztosan megegyezőnek gondolt bitjeinek egy részét. A gyakorlati esetben erre a

4.5 A B92-es protokoll

Még a fentinél is egyszerűbb QKD protokoll az úgynevezett B92-es, amelyet C. Benett javasolt 1992-ben.

Aliz generál egy *klasszikus* véletlen bitsorozatot, legyen ez a_k ahol $a_k = 0$ vagy 1. Ezen bitsorozat egy alkalmas részsorozata lesz majd a titkos kulcs. Ezek után A átküld B-nek egy $|\varphi_k\rangle$ qubit sorozatot, úgy hogy a $\varphi_k = |H\rangle = |\longleftrightarrow\rangle$ ha $a_k = 0$ és $|\varphi_k\rangle = |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = |\nearrow\rangle$, ha $a_k = 1$. B mérést

végez a megérkező kvantumbiten Mérőberendezését ő véletlenszerűen állítja be Z vagy X irányba egy általa választott b'_k klasszikus bitsorozat segítségével. Ha $b'_k = 0$ akkor Z irányban, ha $b'_k = 1$ akkor X irányban mér: az eredmény 0 vagy 1. Most viszont a k-adik eredményt mondja meg $b_k = 0$ vagy 1 és a választott bázist tartja titokban. Azokat a b'_k-ket megtartva amelyre $b_k = 1$, $a_k = 1 + b'_k \mod 2$.