KVANTUMINFORMATIKA
Piszkozat

Sailer Kornél

Speciális előadás

Elméleti Fizikai Tanszék
Debreceni Egyetem
Debrecen
2003.

Contents

1 Bevezetés

1.1 A kvantuminformatika célja

A kvantuminformatikán a fizika és az informatika azon határterületét értjük, amelynek célja, hogy informatikai feladatok megoldását megfelelő kvantummechanikai rendszerek fizikai állapotában bekövetkezett változásból olvassa ki.

Az egyszerűbb informatikai feladatok esetén általában egy néhány részecskét tartalmazó rendszert állítanak elő ú.n. *összefonódott állapot*ban és ezt az állapotot használják fel az informatikai feladat megoldására. Ilyen, egyszerűbb feladatok közül az alábbiakat fogom ismertetni:

1. az ismeretlen kvantummechanikai állapot lemásolásának a problémáját, az ún. *kvantumteleportáció*t;
2. az információnak a kvantummechanikai rendszerek segítségével történő *sűrű kódolás*át;
3. a titkosítási kulcs kvantummechanikai eljárással történő kialakításának és továbbításának a titkosításban játszott forradalmi szerepét *kvantumkriptográfia* címen.

A kvantuminformatika igazi nagy reménysége, hogy sikerül bonyolult, a hagyományos számítógépeken gyakorlatilag nem megvalósítható számolásokat végrehajtani. A forradalmi előrelépést az jelentheti, hogy bizonyos típusú számítások elvégzését a kvantumalgoritmusok használata exponenciálisan felgyorsítja a hagyományos számítógépekben elérhető számolási sebességhez képest. A *kvantumszámítógép* egy kvantumfizikai rendszer. A számolás bemenő adatait azáltal adjuk meg, hogy a számítógépet meghatározott kezdőállapotba hozzuk. A számolás elvégzése abból áll, hogy meghatározott algoritmus szerint külső térrel való kölcsönhatásnak vetjük alá a számítógépet. Végül a végállapoton elvégzett mérés segítségével olvassuk ki a számítás eredményét. A számolás exponenciális felgyorsulása annak köszönhetően várható, hogy egy n szabadsági fokú rendszer mikroállapotainak száma $\mathcal{O}(e^n)$ nagyságrendű. Nagy szabadsági fokú rendszer, azaz nagy kvantumszámítógép esetén ez egy nagy szám. A kezdőállapot ennek a sokféle bázisállapotnak valamilyen lineáris szuperpozíciója lehet. Ez a szuperponált kvantummechanikai állapot fejlődik a számítógép működése során. A végállapot elvileg újra felbontható a bázisállapotok szerint és így a végállapotban elvileg egyszerre áll rendelkezésre az összes lehetséges kezdeti adathalmazon, bázisállapoton párhuzamosan, egyidejűleg elvégzett számítás eredménye.

1.2 A hullámfüggvény összeomlása

Zárt rendszer hullámfüggvénye a kvantummechanika szerint unitér időfejlődésnek tesz eleget:

$$\psi(t) = \hat{U}(t, t_0)\psi(t_0) \tag{1.2.1}$$

aminek következtében a hullámfüggvény az időtől függő Schrödinger-egyenlet megoldása:

$$i\hbar\partial_t\psi(t) = \hat{H}\psi(t). \tag{1.2.2}$$

Az időfejlesztő $\hat{U}(t, t_0)$ operátor unitér, ami biztosítja, hogy normált állapot normált állapotba fejlődik. Az időfejlesztő operátor és a Hamilton-operátor az alábbi kapcsolatban állnak egymással: ha a Hamilton-operátor független az időtől, akkor

$$\hat{U}(t, t_0) = e^{-\frac{i}{\hbar}\hat{H}(t-t_0)}, \tag{1.2.3}$$

ha pedig függ tőle, akkor

$$\hat{U}(t,t_0) = P_\tau e^{-\frac{i}{\hbar}\int_{t_0}^{t} d\tau \hat{H}(\tau)}, \tag{1.2.4}$$

ahol P_τ az időrendezés operátora.

Ha a rendszeren mérést végzünk, akkor ez az unitér időfejlődés nyilvánvalóan megszakad, hiszen a rendszer kölcsönhatásba lép a mérőeszközzel. A vizsgált rendszer és a mérőberendezés közötti kölcsönhatás részletes leírása nem tárgya a kvantummechanikának. Helyette a mérés tulajdonságait a következőképpen posztulálja:

1. Legyen a mérés előtti pillanatban az S rendszer a ψ_S állapotban és tegyük fel, hogy az F fizikai mennyiség értékét akarjuk megmérni. Legyen az F mennyiség operátora az $\hat{F}$ önadjungált operátor, amely az S rendszer állapotainak $\mathcal{H}_S$ Hilbert-terén hat.

2. A mérés eredményeként a mérőberendezésen az F mennyiség valamelyik f_n értéke olvasható le. Általában a mérés eredménye többféle lehet, és annak a valószínűsége, hogy az n-edik lehetséges eredményt kapjuk, jól meghatározott, w_n.

3. Az f_n lehetséges értékek az F fizikai mennyiség $\hat{F}$ önadjungált operátorának sajátértékei. Mint ilyenek, mindig valósak és a hozzájuk tartozó ϕ_n sajátállapotok ortonormált teljes rendszert alkotnak. A sajátértékek és sajátfüggvények az

$$\hat{F}\phi_n = f_n\phi_n, \qquad \phi_n \in \mathcal{H}_S \tag{1.2.5}$$

   sajátértékegyenlet megoldásai.

4. Az S rendszer kezdeti ψ hullámfüggvénye felírható mint a ϕ_n teljes rendszerben szereplő állapotok lineáris kombinációja:

$$\psi = \sum_n c_n\phi_n. \tag{1.2.6}$$

   Az n-edik mérési eredmény bekövetkezésének valószínűsége:

$$w_n = |\langle\phi_n|\psi\rangle|^2 = |c_n|^2, \tag{1.2.7}$$

   ahol $c_n = \langle\phi_n|\psi\rangle$ annak az amplitudója, hogy a ψ állapotban előfordul a ϕ_n állapot.

5. A mérés következtében az S rendszer hullámfüggvénye ugrásszerűen változik, és felveszi a mért fizikai mennyiség n-edik f_n sajátértékéhez tartozó ϕ_n sajátállapotot. Ez azt jelenti, hogy az eredeti hullámfüggvény, az eredeti lineáris kombináció *összeomlik* annak egyetlen tagjára, mégpedig $w_n = |c_n|^2$ valószínűséggel az n-edik tagra:

$$\psi = \sum_n c_n\phi_n \Longrightarrow \phi_n. \tag{1.2.8}$$

A hullámfüggvény összeomlása matematikai értelemben nem más mint az eredeti hullámfüggvény ortogonális vetítése a $\mathcal{H}_S$ Hilbert-térnek azon alterére, amelyet az $\hat{F}$ mennyiség f_n sajátértékéhez tartozó állapot feszít ki. (Hasonló a helyzet akkor is, ha több állapot, azaz nem egy egy-dimenziós altér tartozik az f_n sajátértékhez.)

Az a tény, hogy a mérés során a hullámfüggvény összeomlik, azt is jelenti, hogy a mérés a kvantummechanikában radikális beavatkozás a vizsgált rendszer állapotába. Elvileg sem képzelhető el olyan mérés, amely infinitezimálisan kicsiny változást okoz, mert a hullámfüggvény összeomlása egy lineáris kombinációból annak egyetlen tagjára nem folytonos változás.

1.3 Az állapotok összefonódása

A többrészecskés állapotot *összefonódottnak* nevezzük, ha a hullámfüggvénye nem áll elő egyrészecskés hullámfüggvények szorzatának alakjában. Erre a kvantummechanikában temérdek példa van. Vegyük pl. a két-részecskés összefonódott állapotokat. Legyen pl. két elektronunk, amelyeknek az eredő spinje $S = 0$ vagy $S = 1$ lehet. Mindkét esetben találunk összefonódott állapotot:

$$\chi_{S=0,S_z=0}(\sigma_1,\sigma_2) = \frac{1}{\sqrt{2}}[\chi_{+\frac{1}{2}}(\sigma_1)\chi_{-\frac{1}{2}}(\sigma_2) - \chi_{-\frac{1}{2}}(\sigma_1)\chi_{+\frac{1}{2}}(\sigma_2)],$$
$$\chi_{S=1,S_z=0}(\sigma_1,\sigma_2) = \frac{1}{\sqrt{2}}[\chi_{+\frac{1}{2}}(\sigma_1)\chi_{-\frac{1}{2}}(\sigma_2) + \chi_{-\frac{1}{2}}(\sigma_1)\chi_{+\frac{1}{2}}(\sigma_2)]. \qquad (1.3.9)$$

Az összefonódott állapotok létezése a kvantummechanikai lineáris szuperpozíció elvének köszönhető. Első ránézésre egy összefonódott állapotban nincsen semmi rendkívüli.

Van azonban az összefonódott állapotoknak egy sajátos vonása, ami – bár szigorúan következik a kvantummechanika elveiből – paradoxnak tűnhet. Ahhoz, hogy ezt megértsük, tegyük fel, hogy pl. vesszük a $\chi_{S=0,S_z=0}(\sigma_1,\sigma_2)$ spin-szinglet állapotot, amelyhez a Pauli-elv szerint két elektron helyvektorainak felcserélésével szemben szimmetrikus térbeli hullámfüggvény tartozik. Tegyük fel, hogy olyan állapotot vizsgálunk, amikor az egyik elektron a vonatkoztatási rendszernek választott A inerciarendszerben nyugalomban van, míg a másik elektron $\approx \vec{p}$ impulzussal mozgó hullámcsomag. A normálási tényezőtől eltekintve, ekkor a teljes hullámfüggvény:

$$\psi(t,\vec{r}_1,\vec{r}_2,\sigma_1,\sigma_2) \propto [\phi(\vec{r}_2 - \frac{\vec{p}}{m}t)\phi(\vec{r}_1) + \phi(\vec{r}_1 - \frac{\vec{p}}{m}t)\phi(\vec{r}_2)]\chi_{S=0,S_z=0}(\sigma_1,\sigma_2). \qquad (1.3.10)$$

Ez a hullámfüggvény olyan két-elektronos állapotot ír le, amikor az egyik elektron impulzusának várható értéke nulla, a másiké pedig $\vec{p}$, miközben spin-állapotuk összefonódott, szinglet-állapot. (A példában a térbeli hullámfüggvény is összefonódott, de ezt nem használjuk ki.) Az állapot időfejlődése tehát olyan, hogy az egyik elektron hullámcsomagja ott marad, ahol előállították, a másiké pedig állandó sebességgel halad.

Tegyük fel, hogy Alíz (A) és Béci (B) tanulmányozni akarják az összefonódott állapotokat. Az a tény, hogy létezik olyan állapot, amikor az elektron-pár összefonódott spin-állapotban van, miközben az egyik részecske helyben marad, míg a másik haladó mozgást végez, lehetővé teszi, hogy A és B végrehajtsák a következő kísérletet:

1. Alíz előállítja az elektron-párt az összefonódott spinállapotban, mondjuk spin-szinglett állapotban. Ehhez szüksége van meghatározott bázisválasztásra, pl. választ egy z-tengelyt és a spin z-irányú vetületének sajátállapotait tekinti bázisnak.

2. Ezután Alíz elküldi az összefonódott spinállapotban levő elektronok egyikét Bécinek. Az elektron elküldéséhez természetesen szükséges az a *kvantummechanikai csatorna*, amely biztosítja, hogy amíg az egyik elektron úton van Béci felé, addig nem lépnek az elektron-spinek semmivel sem kölcsönhatásba. Csak így biztosítható, hogy az elektron-pár még akkor is ugyanabban a spin-szinglet állapotban legyen mint kezdetben, amikor az egyik elektron megérkezik Bécihez. Műszóval azt szokás mondani, hogy az elektron továbbítása során meg kell őrizni a spinállapot *koherenciáját*, azaz az egyes spinek hullámfüggvényeinek relatív fázisát.

3. Alíz megméri a nála maradt elektron spinjének z-vetületét a korábban megválasztott bázisban. Tudjuk, 0,5 a valószínűsége, hogy azt $s_A = +\frac{1}{2}$-nek, és ugyennyi, hogy $s_A = -\frac{1}{2}$-nek találja.

4. Alíz valamilyen klasszikus csatornán (pl. fényjel, ill. a gyakorlatban telefon, rádió, fax, stb.) megüzeni saját mérése eredményét Bécinek és egyúttal azt is, hogyan választotta a z-tengelyt, vagyis hogy milyen bázisban mért.

5. Miután Béci az üzenetet vette, alkalmas detektorral meggyőződhet róla, hogy

   - ha Alíz eredménye $s_A = +\frac{1}{2}$ volt, akkor ő bizonyossággal $s_B = -\frac{1}{2}$ eredményt kap;
   - ha Alíz eredménye $s_A = -\frac{1}{2}$ volt, akkor ő bizonyossággal $s_B = +\frac{1}{2}$ eredményt kap.

   Az alkalmas detektor használata azt jelenti, hogy Bécinek ugyanazt a z-tengelyt, ill. ugyanazt a bázist kell használnia mérése során, mint Alíznak.

A kvantummechanika azt mondja, hogy a mérés eredménye az, hogy a *hullámfüggvény összeomlik*. Ez azt jelenti, hogy a két-elektronos rendszer hullámfüggvényének a Hamilton-operátor által meghatározott (és a Schrödinger-egyenlet alapján számolható) időfejlődése megszakad a mérőeszközzel való kölcsönhatás következtében. A mérés eredménye, hogy a hullámfüggvény vetítődik az állapotok azon alterére, amely s_A mért értékéhez tartozik. Arra az altérre, amelyhez tartozó állapotokban s_A sajátértéke pontosan a mért érték. Esetünkben ez az altér egy-dimenziós:

- $s_A = +\frac{1}{2}$ esetén a $\chi_{+\frac{1}{2}}(\sigma_1)\chi_{-\frac{1}{2}}(\sigma_2)$ állapot,
- $s_A = -\frac{1}{2}$ esetén a $\chi_{-\frac{1}{2}}(\sigma_1)\chi_{+\frac{1}{2}}(\sigma_2)$ állapot

feszíti ki, amely alterekben s_B sajátértéke rendre $-\frac{1}{2}$ ill. $+\frac{1}{2}$. A kvantummechanika értelmében a hullámfüggvény összeomlása a pillanatszerűnek feltételezett mérés pillanatában megtörténik, bármilyen messze is legyen a két elektron térben egymástól. A kvantummechanika feltételezi, hogy a mérés következménye időkésés nélkül jelentkezik a hullámfüggvény összeomlásában. Ez ugyanolyan paradox, mint amilyen paradox annak a feltételezése a klasszikus mechanikában, hogy a kölcsönhatás végtelen sebességgel terjed. Mindkettő klasszikus fizikai elmélet, amely nem tesz eleget a speciális relativitáselmélet követelményeinek. Nagy baj még sincsen. Béci ugyanis nem tud addig megbizonyosodni arról, hogy a nála levő elektron milyen állapotba került, amíg meg nem tudja Alíz mérésének eredményét, ez pedig nem juthat el hozzá a vákuumbeli fénysebességnél gyorsabban.

Az összefonódott állapotok létezése tehát a kvantummechanikai lineáris szuperpozíció elvének köszönhető. Informatikai hasznosításukban pedig fontos szerepet fog játszani, hogy mérés következtében a hullámfüggvény összeomlik.

Technikailag az összefonódott állapotú részecskék elküldése nagy távolságra azért ütközik nehézségbe, mert azok bizonyos valószínűséggel (hatáskeresztmetszettel) kölcsönhatásba léphetnek a ,,kvantumcsatornával", amelyben továbbításuk történik. A 2003. évi távolságcsúcs összefonódott állapotú fotonok szabad terjedésére 600 m [4].

1.4 A kubit

A klasszikus bit fizikai megvalósítása olyan klasszikus fizikai rendszer, amelynek 2 állapota van. Az egyik állapothoz rendeljük az 1, a másikhoz a 0 értéket. Azért mondjuk, hogy az ilyen rendszer 1 bitnyi információ tárolására alkalmas, mert 1 darab igen-nem kérdésre adott válasz kódolható be a rendszer állapotaiba. Pl. az ,,igen" válasznak feleltetjük

meg az 1, a ,,nem" válasznak a 0 értéket. Általában n darab klasszikus bitet tartalmazó rendszer állapotaiba n darab, logikailag független igen-nem kérdésre adott 2^n-féle válasz kódolható be. Azt mondjuk, hogy n darab, logikailag független igen-nem kérdésre adott lehetséges válaszok n bit információt jelentenek. A hagyományos, klasszikus számítógépek az információ tárolására klasszikus biteket használnak.

A *kvantumbit* vagy röviden *kubit* fizikai megvalósítása egy kétállapotú kvantummechanikai rendszer. Pl. egy elektron spinvetületének sajátállapotai, vagy egy foton helicitás-sajátállapotai. A kétállapotú kvantummechanikai rendszernek azonban nem 2 darab lehetséges állapota van, hanem végtelen sok. Azért nevezzük két-állapotúnak, mert állapotainak Hilbert-tere két-dimenziós. Ha $|1\rangle$ és $|0\rangle$ jelöli a kvantumbit két bázisállapotát (példáinkban rendre a spinvetület ill. a helicitás két sajátállapotát), akkor a rendszer Hilbert-tere a lineáris szuperpozíció elvének köszönhetően ezen két állapot bármely komplex együtthatós lineáris kombinációját is tartalmazza, azaz az összes

$$\alpha|1\rangle + \beta|0\rangle \tag{1.4.1}$$

alakú állapotot, ahol α és β tetszőleges komplex számok, amelyek eleget tesznek a normálási feltételből következő

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.4.2}$$

egyenlőségnek. Az általánosság csorbítása nélkül választhatjuk α-t valósnak (az állapotfüggvényt szabad tetszőleges fázisfaktorral szorozni), és írhatjuk, hogy $\alpha = \cos\theta$, $\beta = e^{i\varphi}\sin\theta$, ahol $\theta \in [0,\pi]$, $\varphi \in [0,2\pi]$. A két-állapotú kvantumbit, az ún. kubit állapotainak Hilbert-tere tehát kölcsönösen egyértelműen leképezhető az egységnyi sugarú gömb felületére. A megfelelő képpont helyzetét a (θ,φ) gömbi polárkoordinátákkal adhatjuk meg. A klasszikus bit 2 értékének megfelelő $|1\rangle$ és $|0\rangle$ bázisállapotoknak rendre a gömbfelület északi ($\theta = 0$) ill. déli ($\theta = \pi$) pólusa felel meg.

Sok független kubit állapotainak Hilbert-tere az egyes kubitek Hilbert-tereinek direkt szorzata. Egy *klasszikus bitek értékeivel megadott adatsor*nak ebben a direkt-szorzat térben egy bázisállapot felel meg. A direktszorzattérnek azt a bázisát, amelyet az egyes kubitek $|1\rangle$ és $|0\rangle$ bázisállapotainak direkt szorzataiként kapunk meg, *számolási bázis*nak szokás nevezni. Egy klasszikus bitek értékeivel megadott adatsor tehát a számolási bázis egy meghatározott bázisvektorának megadásával ekvivalens.

1.5 A kvantumlogikai kapuk

Kvantumregiszternek vagy röviden regiszternek szokás nevezni azt a véges sok, n kubitből álló rendszert, amelynek tartalmán műveleteket akarunk végrehajtani. A *művelet* egy egyértelmű leképezés, amely az n darab kubit kezdeti, azaz bemenő állapotához hozzárendeli az n darab kubit valamely kimenő állapotát. Fizikailag a műveleteket a kvantumregiszternek alkalmasan választott külső térrel történő kölcsönhatása révén valósítjuk meg. Ennek a kölcsönhatási folyamatnak a kvantummechanika értelmében unitér időfejlesztő operátor felel meg, amely az n-kubites kvantumregiszter állapotainak Hilbert-terét önmagára képezi le.

A *kvantumlogikai kapuk* az n kubitből álló rendszeren a legegyszerűbb logikai műveleteket végrehajtó fizikai folyamatok, amelyeknek az ezen kubitek Hilbert-terén ható unitér operátorok felelnek meg. Ezek $2^n \times 2^n$-es unitér mátrixokkal ábrázolhatók a számolási bázisban. A művelet, ill. a logikai kapu által befolyásolt kubitek számának megfelelően beszélhetünk 1-, 2-, 3-kubites, stb. kvantumlogikai kapukról. Mielőtt példaként végignézünk néhány fontos kaput, ill. a nekik megfelelő operátorokat és azok hatását a számolási bázis vektoraira, beszéljünk meg egy fontos dolgot a kvantumlogikai kapuk megvalósításáról. Ezeket

fizikailag általában úgy lehet megvalósítani, hogy a szóbanforgó kubitekből álló fizikai rendszert meghatározott ideig meghatározott külső térrel hozzuk kölcsönhatásba. Ez merőben eltér a hagyományos számítógép logikai kapuinak megvalósításától. A hagyományos számítógépekben logikai áramkörök vannak, s azokban a logikai kapuk olyan áramköri elemek, amelyek meghatározott számú bemenő lábán megjelenő, 0-nak és 1-nek megfelelő feszültségszintekhez egy logikai táblázat alapján a kimeneti lábon (lábakon) 0-nak vagy 1-nek megfelelő feszültségi szint jelenik meg.

Egy n-kubites kvantumlogikai kapu olyan, külső térrel való kölcsönhatást jelent, amelyben n darab kubit vesz részt és az n-kubites részrendszer számolási bázisállapotai a kölcsönhatás eredményeként meghatározott módon transzformálódnak ezen számolási bázisállapotok lineáris kombinációiba.

A példákat akkor tudjuk egyszerű számolással megérteni, ha az 1-kubites állapotokat komplex, 2-dimenziós oszlopvektorokkal, a felettük ható operátorokat 2×2-es, komplex elemű mátrixokkal ábrázoljuk. Az 1-kubites Hilbert-tér bázisvektorai:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.5.1}$$

az 1-kubites operátorok terében a bázis pedig

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.5.2}$$

A legfontosabb kvantumlogikai kapukat alább sorra vesszük és hatásukat a 1. ábrán szemléltetjük.

1. *1-kubites kapuk.*

   (a) *NEM-kapu* megvalósítása a $\hat{U}_{\mathrm{NOT}} = \sigma_1$ operátor, mert

   $$\sigma_1|1\rangle = |0\rangle, \qquad \sigma_1|0\rangle = |1\rangle. \tag{1.5.3}$$

   (b) *Négyzetgyök-NEM-kapu:*

   $$\hat{U}_{\sqrt{\mathrm{NOT}}} = \frac{1}{\sqrt{2}} e^{\frac{i\pi}{4}} (1 - i\sigma_1), \tag{1.5.4}$$

   amelyre egyrészt teljesül, hogy

   $$\hat{U}_{\sqrt{\mathrm{NOT}}} \hat{U}_{\sqrt{\mathrm{NOT}}} = \frac{i}{2}(1 - \sigma_1^2 - 2i\sigma_1) = \sigma_1 = \hat{U}_{\mathrm{NOT}}, \tag{1.5.5}$$

   másrészt pedig

   $$\hat{U}_{\sqrt{\mathrm{NOT}}}|1\rangle = \frac{1}{\sqrt{2}} e^{\frac{i\pi}{4}} (|1\rangle - i|0\rangle), \qquad \hat{U}_{\sqrt{\mathrm{NOT}}}|0\rangle = \frac{1}{\sqrt{2}} e^{\frac{i\pi}{4}} (|0\rangle - i|1\rangle). \tag{1.5.6}$$

   Ez szépen példázza, hogy általában a logikai kapu alkalmazása a számolási bázis állapotainak szuperpozícióját adja eredményül.

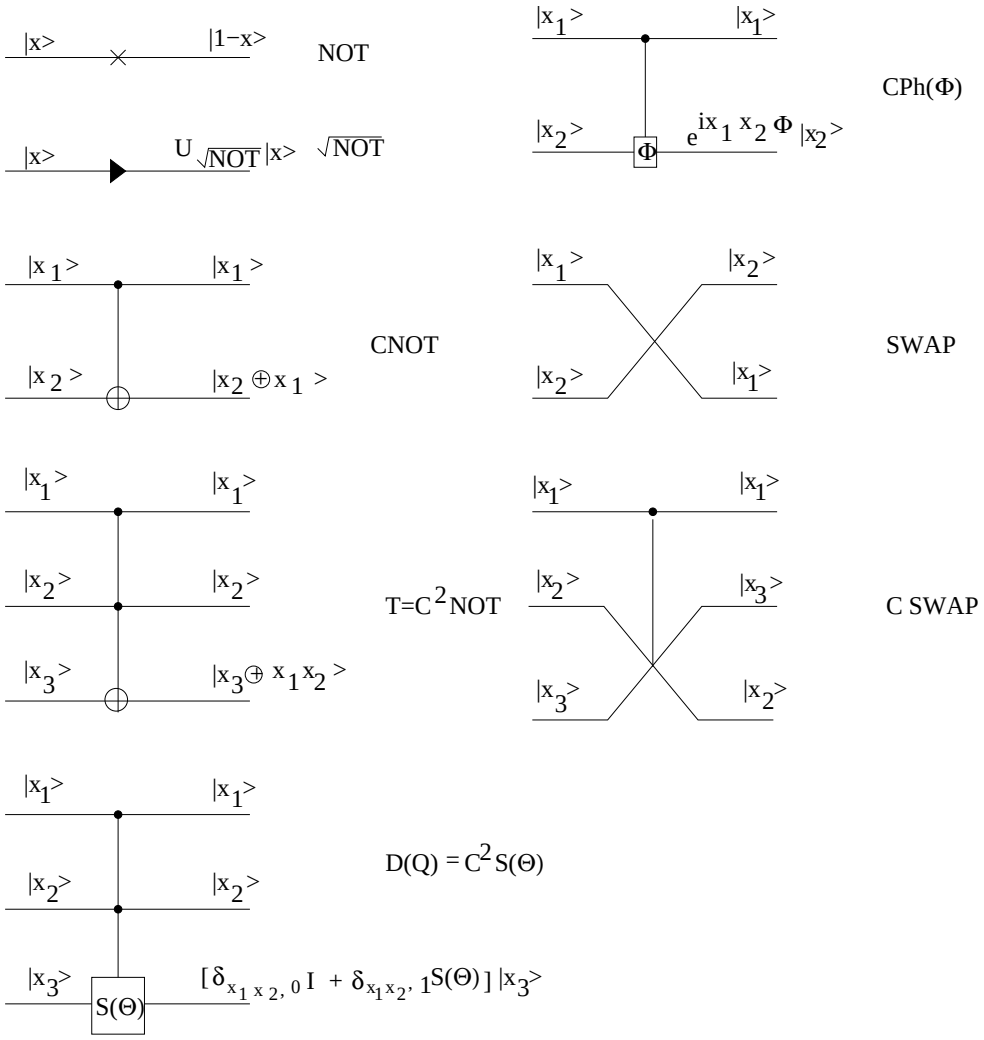

Figure 1: A legegyszerűbb kvantumlogikai kapuk.

(c) *Hadamard-kapu:*

$$\hat{U}_{\mathrm{H}} = \frac{1}{\sqrt{2}}(\sigma_3 + \sigma_1) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.5.7}$$

Ennek hatása a számolási bázis vektoraira:

$$\hat{U}_{\mathrm{H}}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad \hat{U}_{\mathrm{H}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.5.8}$$

2. *2-kubites kapuk.* Jelöljük a 2-kubites Hilbert-térben a számolási bázis vektorait rendre az alábbiak szerint:

$$|00\rangle = |0\rangle \otimes |0\rangle, \qquad |01\rangle = |0\rangle \otimes |1\rangle, \qquad |10\rangle = |1\rangle \otimes |0\rangle, \qquad |11\rangle = |1\rangle \otimes |1\rangle. \tag{1.5.9}$$

Itt a bázisvektorok sorszámát kapjuk, ha az egyenlőségek bal oldalán használt jelölést bináris számként értelmezzük. Ebben a bázisban, a bázisvektorok fenti sorrendjéhez ragaszkodva a 2-kubites kapuk 4×4-es mátrixok.

(a) *Feltételes nem-kapu:*

$$\hat{U}_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{1.5.10}$$

ami az alábbi hatást jelenti:

$$\begin{aligned} \hat{U}_{\mathrm{CNOT}}|00\rangle &= |00\rangle, \qquad \hat{U}_{\mathrm{CNOT}}|01\rangle = |01\rangle, \\ \hat{U}_{\mathrm{CNOT}}|10\rangle &= |11\rangle, \qquad \hat{U}_{\mathrm{CNOT}}|11\rangle = |10\rangle. \end{aligned} \tag{1.5.11}$$

Ezek szerint a 2. kubit állapotát aszerint hagyja változatlanul, vagy változtatja tagadásába ez a kapu, hogy az első kubit állapota rendre $|0\rangle$ vagy $|1\rangle$. Ezért nevezzük ezt a kaput feltételes nem-kapunak.

(b) *Feltételes fázis-kapu:* hatására a második kubit $e^{i\phi}$ fázist kap, ha az első kubit az $|1\rangle$ számolási bázisállapotban van:

$$\hat{U}_{\mathrm{CPh}(\phi)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}. \tag{1.5.12}$$

Egy hasznos azonosság kapcsolatot teremt a feltételes nem-kapu és a feltételes fázis-kapu között:

$$(1 \otimes \hat{U}_H)\hat{U}_{\mathrm{CPh}(\phi)}(1 \otimes \hat{U}_H) = \hat{U}_{\mathrm{CNOT}}. \tag{1.5.13}$$

(c) *Billentő kapu:* felcseréli a két kubit állpotát:

$$\hat{U}_{\mathrm{SWAP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.5.14}$$

Értelmezni lehet a $\sqrt{\mathrm{SWAP}}$-kaput azzal a tulajdonsággal, hogy a négyzete a billentő kapu:

$$\hat{U}_{\sqrt{\mathrm{SWAP}}}\hat{U}_{\sqrt{\mathrm{SWAP}}} = \hat{U}_{\mathrm{SWAP}}. \tag{1.5.15}$$

3. *3-kubites kapuk.*

   (a) *T(offoli)-kapu, azaz C^2NOT-kapu:* a kapu hatására az első két kubit állapota változatlan marad, a harmadik kubit állapota pedig ellentétesre változik akkor és csak akkor, ha az első két kubit az $|1\rangle$ állapotban van.

   (b) *Deutsch-kapu, azaz $C^2S(\theta)$-kapu:* a kapu hatására az első két kubit állapota változatlan marad, a harmadik kubit állapota pedig az x-tengely körül Θ szöggel fordul el pozitív irányban, majd az állapot i-vel szorzódik, ahol $\Theta \neq n\pi$ (n tetszőleges egész szám).

   A Deutsch-kapu jelentősége abban áll, hogy Deutsch-kapuk ismételt egymás utáni alkalmazásával (a) a T-kapu tetszőleges pontossággal megközelíthető, és (b) egy tetszőleges α szögű, x-tengely körüli elforgatás is tetszőlegesen megközelíthető. Ennek a fizikai megvalósítások során van jelentősége.

   (c) *Fredkin-kapu, azaz feltételes billentő kapu:* az első kubit állapota változatlan marad, a második és harmadik kapu állapota pedig akkor és csak akkor cserélődik fel, ha az első kubit állapota $|1\rangle$, egyébként ezek is változatlanok maradnak.

2 Speciális informatikai feladatok megoldása

2.1 Ismeretlen állapot lemásolása: kvantumteleportáció

A *kvantumteleportáció* azt jelenti, hogy a valahol rendelkezésre álló i kubit ismeretlen $|\Psi\rangle$ állapotát lemásoljuk, azaz egy másik helyen található, az i-vel fizikailag azonos f kubitet a (változatlanul ismeretlen) $|\Psi\rangle$ állapotba hozzuk. Mivel a kvantummechanikai állapot azonnal megváltozik, ha mérést végzünk rajta, ezért az eredeti állapotot anélkül kell lemásolnunk, hogy közben megtudnánk, miféle állapotot másolunk le. A kvantumteleportáció további jellegzetessége, hogy a másoláshoz az eredeti kubitet kölcsönhatásba kell hozni egy másik kvantummechanikai rendszerrel, pl. egy összefonódott állapotban levő részecskepárral, s ennek következtében a másolás mindig maga után vonja az eredeti kubit állapotának megváltozását. Ugyanakkor egy klasszikus bit értékének (állapotának) kiolvasása mindig elvégezhető volt anélkül, hogy ezáltal megváltozott volna az eredeti bit állapota, s így az állapot lemásolása is úgy történt, hogy tudtuk, milyen állapotot másolunk le.

Tegyük fel, hogy A(líz) rendelkezik az ismeretlen,

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1.1}$$

állapotú i kubittel, amelynek állapotát B(éci) le akarja másolni. A kvantumteleportációt megvalósíthatjuk egy összefonódott, 2-kubites állapot segítségével. Legyen ez pl.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{2.1.2}$$

és tegyük fel, hogy az első, a kubit A-nál, a második, b kubit pedig B-nél van. A 3 darab kubitből álló (iab)-rendszer tehát kezdetben a $|\Psi\rangle|\Phi\rangle$ állapotban található. Az ismeretlen $|\Psi\rangle$ állapot lemásolása az alábbi lépésekben történhet:

1. *lépés:* A a nála levő ia kubitekre a feltételes nem-kapuval hat, aminek következtében az (iab)-rendszer az alábbi állapotba kerül:

$$\begin{aligned}|\Psi\rangle|\Phi\rangle \Longrightarrow \frac{1}{\sqrt{2}}\Big[&(\hat{U}_{\mathrm{CNOT}}\alpha|0\rangle|0\rangle)|0\rangle + (\hat{U}_{\mathrm{CNOT}}\beta|1\rangle|0\rangle)|0\rangle \\ &+ (\hat{U}_{\mathrm{CNOT}}\alpha|0\rangle|1\rangle)|1\rangle + (\hat{U}_{\mathrm{CNOT}}\beta|1\rangle|1\rangle)|1\rangle\Big] \\ = \frac{1}{\sqrt{2}}\Big[&\alpha|0\rangle|0\rangle|0\rangle + \beta|1\rangle|1\rangle|0\rangle + \alpha|0\rangle|1\rangle|1\rangle + \beta|1\rangle|0\rangle)|1\rangle\Big]\end{aligned} \tag{2.1.3}$$

2. *lépés:* A az ismeretlen állapotú i kubitre a Hadamard-kapuval hat, s ekkor az (iab)-rendszer állapota az alábbi lesz:

$$\begin{aligned}\Longrightarrow \frac{1}{\sqrt{2}}\Big[&\alpha(\hat{U}_{\mathrm{H}}|0\rangle)|0\rangle|0\rangle + \beta(\hat{U}_{\mathrm{H}}|1\rangle)|1\rangle|0\rangle + \alpha(\hat{U}_{\mathrm{H}}|0\rangle)|1\rangle|1\rangle + \beta(\hat{U}_{\mathrm{H}}|1\rangle)|0\rangle|1\rangle\Big] \\ = \frac{1}{2}\Big[&(|0\rangle + |1\rangle)|0\rangle\alpha|0\rangle + (|0\rangle - |1\rangle)|1\rangle\beta|0\rangle + (|0\rangle + |1\rangle)|1\rangle\alpha|1\rangle \\ &+ (|0\rangle - |1\rangle)|0\rangle\beta|1\rangle\Big]\end{aligned}$$

$$= \frac{1}{\sqrt{2}}|0\rangle|0\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{\sqrt{2}}|0\rangle|1\rangle\frac{1}{\sqrt{2}}(\alpha|1\rangle + \beta|0\rangle)$$
$$+ \frac{1}{\sqrt{2}}|1\rangle|0\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{\sqrt{2}}|1\rangle|1\rangle\frac{1}{\sqrt{2}}(\alpha|1\rangle - \beta|0\rangle)$$
$$= \frac{1}{\sqrt{2}}|0\rangle|0\rangle|\Psi\rangle + \frac{1}{\sqrt{2}}|0\rangle|1\rangle(\hat{\sigma}_1|\Psi\rangle) + \frac{1}{\sqrt{2}}|1\rangle|0\rangle(\hat{\sigma}_3|\Psi\rangle) + \frac{1}{\sqrt{2}}|1\rangle|1\rangle(i\hat{\sigma}_2|\Psi\rangle). \tag{2.1.4}$$

3. *lépés:* A megméri a nála levő (ia) kubitek spinjét. A lehetséges eredmények és a hozzájuk tartozó valószínűségek:

$$|0\rangle|0\rangle: \quad 0,25; \qquad |0\rangle|1\rangle: \quad 0,25; \qquad |1\rangle|0\rangle: \quad 0,25; \qquad |1\rangle|1\rangle: \quad 0,25. \tag{2.1.5}$$

   Ezen mérés lehetséges eredményeinek megfelelően a B-nél levő b kubit rendre az alábbi állapotokba kerül:

$$|\Psi\rangle; \qquad \hat{\sigma}_1|\Psi\rangle; \qquad \hat{\sigma}_3|\Psi\rangle; \qquad i\hat{\sigma}_2|\Psi\rangle. \tag{2.1.6}$$

4. *lépés:* A megüzeni B-nek hagyományos módon (klasszikus fizikai csatornán) a saját mérési eredményét. Ez az üzenet 2 klasszikus bit-nyi információt, azaz 2 cbit információt tartalmaz, amely rendre

$$00; \qquad 01; \qquad 10; \qquad 11. \tag{2.1.7}$$

5. *lépés:* A üzenetének ismeretében B rendre vagy az $\hat{1}$, vagy a $\hat{\sigma}_1$, vagy a $\hat{\sigma}_3$, vagy az $i\hat{\sigma}_2$ kapuval hat a nála levő b kubitre, aminek eredményeként az a lemásolandó, de még mindig ismeretlennek megmaradt $|\Psi\rangle$ állapotba kerül.

A fenti eljárással tehát le lehet másolni egy tetszőleges kubit állapotát. Ehhez egy összefonódott állapotban lévő részecske-párra szükséges, amelyek egyikét a lemásolandó állapotú kubitet birtokló A(líz)hoz, másikát a másolatot elkészíteni kívánó B(éci)hez kell eljuttatni. Szükséges még ezen kívül egy klasszikus fizikai kommunikációs csatorna, amelyen 2 (klasszikus) bit információt kell A-nak eljuttatnia B-hez. **Félreértések elkerülése végett, nem az i kubitet juttattuk el valamilyen „misztikus" úton A-tól B-hez, hanem csak az állapota lett lemásolva.** Ráadásul a másolat megtörténtére vonatkozó ismeret nem állhat elő hamarabb, mint ahogy az A mérésének eredményére vonatkozó üzenet klasszikus fizikai úton (a vákuumbeli fénysebességet meg nem haladó sebességgel) eljut B-hez.

2.2 Sűrű kódolás

A *sűrű kódolás* bizonyos értelemben annak a megfordítottja, amit a kvantumteleportáció, azaz a kvantummechanikai állapot lemásolása jelent. A kvantumteleportáció során egy kubitnyi információt (egy kubit állapotát) másoltuk le az eredetitől adott távolságra 2 klasszikus bitnyi információ ismeretében, amelyet klasszikus fizikai úton, azaz *klasszikus csatornán* juttattunk el erre a távolságra. A sűrű kódolásnál egy kubitet, az azt megvalósító fizikai rendszert juttatjuk el kvantummechanikai úton, azaz *kvantumcsatornán* adott távolságra abból a célból, hogy ezáltal 2 klasszikus bitnyi információt továbbítsunk. Mindkét esetben összefonódott állapotot használunk fel az eljáráshoz.

Tegyük fel, hogy van egy ,,forrás", amely létrehozza a

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{2.2.1}$$

összefonódott, 2-kubites állapotot és megküldi az egyik, mondjuk az első kubitet (a) A(líz)nak, a másodikat (b) pedig B(éci)nek. Ezután az eljárás lépései a következők:

1. *lépés:* A(líz) az (ab) kubitek összefonódott állapotába 2 klasszikus bitnyi információt *kódol* úgy, hogy a nála lévő a kubitre a megfelelő kvantumlogikai kapuval hat. A különböző lehetséges információk és a bekódolásukhoz szükséges kvantumlogikai kapuk, ill. az ennek hatására előálló $|\Phi_{\mathrm{K}}\rangle$ állapotok rendre:

Kód	Kapu	$\lvert\Phi_{\mathrm{K}}\rangle$
00	$\hat{1}\otimes\hat{1}$	$\lvert\Phi\rangle$
01	$\hat{\sigma}_3\otimes\hat{1}$	$\frac{1}{\sqrt{2}}(\lvert0\rangle\lvert0\rangle - \lvert1\rangle\lvert1\rangle)$
10	$\hat{\sigma}_1\otimes\hat{1}$	$\frac{1}{\sqrt{2}}(\lvert1\rangle\lvert0\rangle + \lvert0\rangle\lvert1\rangle)$
11	$i\hat{\sigma}_2\otimes\hat{1}$	$\frac{1}{\sqrt{2}}(\lvert1\rangle\lvert0\rangle - \lvert0\rangle\lvert1\rangle)$

(2.2.2)

2. *lépés:* Ezután A elküldi Bécinek kvantummechanikai úton a nála levő a kubitet (pl. fotont optikai szálon). **Fontos** követelmény, hogy a kvantumcsatorna ne hasson kölcsön a rajta továbbított részecske spinjével.

3. *lépés:* Miután B megkapja az a kubitet is, elkezdi a *dekódolást.* Először a feltételes nem-kapuval hat a $|\Phi_{\mathrm{K}}\rangle$ állapotra:

$$|\Phi_{\mathrm{K}}\rangle \Longrightarrow \hat{U}_{\mathrm{CNOT}}|\Phi_{\mathrm{K}}\rangle = \frac{1}{\sqrt{2}}\begin{cases}(|0\rangle + |1\rangle)|0\rangle\\(|0\rangle - |1\rangle)|0\rangle\\(|1\rangle + |0\rangle)|1\rangle\\(|1\rangle - |0\rangle)|1\rangle\end{cases}. \tag{2.2.3}$$

   A lehetséges eredményeket összevetve az (2.2.2) táblázatban szereplő üzenet kódjával látjuk, hogy ha B most megméri a b kubit spinjének z-irányú vetületét, akkor aszerint hogy b-t a $|0\rangle$ vagy az $|1\rangle$ állapotban találja, rekonstruálta az üzenet első bitjének 0 ill. 1 értékét. Jegyezzük meg, hogy b spinjének mérése nem változtatja meg az $\hat{U}_{\mathrm{CNOT}}|\Phi_{\mathrm{K}}\rangle$ állapotot, mert abban b a spin z-irányú vetületének sajátállapotában van.

4. *lépés:* B ezután a Hadamard-kaput alkalmazza az a kubitre:

$$\hat{U}_{\mathrm{H}}\otimes\hat{1}(\hat{U}_{\mathrm{CNOT}}|\Phi_{\mathrm{K}}\rangle) = \frac{1}{2}\begin{cases}(|0\rangle + |1\rangle + |0\rangle - |1\rangle)|0\rangle = 2|0\rangle|0\rangle\\(|0\rangle + |1\rangle - |0\rangle + |1\rangle)|0\rangle = 2|1\rangle|0\rangle\\(|0\rangle - |1\rangle + |0\rangle + |1\rangle)|1\rangle = 2|0\rangle|1\rangle\\(|0\rangle - |1\rangle - |0\rangle - |1\rangle)|1\rangle = -2|1\rangle|1\rangle\end{cases}. \tag{2.2.4}$$

Ezután B megméri az a kubit z-irányú spinvetületét. Ha a dekódolás utáni (2.2.4) állapotot összehasonlítjuk az (2.2.2) táblázatban szereplő üzenettel, akkor látjuk, hogy aszerint, hogy a-t $|0\rangle$ vagy $|1\rangle$ állapotban találja, megállapítja, hogy a kapott üzenet második bitje 0 ill. 1 értékű.

Ezzel befejeződött a 2 klasszikus bitnyi információ dekódolása.

2.3 Kvantumkriptográfia

A *kriptográfia* az üzenetek titkosításával foglalkozik. A feladat a következő. Adott az üzenet, a *forrásszöveg* mint a $(p_1, p_2, \ldots, p_N)$ N darab szimbólumból álló sorozat, ahol N egész szám. Az egyszerűség kedvéért tegyük fel, hogy a szimbólumok digitalizált alakban állnak rendelkezésre, mint $1 \leq p_j \leq B$ egész számok, ahol $B \geq 2$ is egész szám. A forrásszöveg szimbólumai tehát egy B darab ,,betűből" álló ABC betűi közül vannak választva. Ezt a betűsorozatot Alíz valamilyen kulcs segítségével átalakítja egy másik, az eredeti sorozattal azonos N számú szimbólumból álló $(c_1, c_2, \ldots, c_N)$ sorozattá. Ez a titkosított szöveg, az ún. *kriptogram*. Utána Alíz megküldi Bécinek a kriptogramot, aki a titkosításhoz felhasznált kulcs birtokában dekódolja azt, s így megfejti az üzenetet. A fő kérdés a titkosítás biztonsága. A kulcsot is, meg a kriptogramot is általában valamilyen információs csatornán kell Alíznak Bécihez eljuttatnia. Hogyan lehet biztosítani, hogy mondjuk Elemér, aki illetéktelenül próbálja lehallgatja a kriptogramot, vagy a kulcsot, vagy mindkettőt, ne legyen abban a helyzetben, hogy megfejtse az üzenetet?

2.3.1 Klasszikus kriptográfia

Mielőtt arról beszélnénk, hogyan alkalmazhatók a részecskék kvantummechanikai állapotai a kriptográfia céljaira, érdemes néhány alapvető fontosságú klasszikus kriptográfiai eljárással megismerkedni.

1. *Egyszer használatos kulcs módszere (Vernam-eljárás, 1917).* Az üzenetváltást megelőzően Alíz és Béci megegyeznek a kulcsban. A kulcs véletlenszerűen (egyenletes eloszlással) választott egész számok sorozata: $(k_1, k_2, \ldots, k_M)$, ahol $1 \leq k_j \leq B$ és $M \geq N$. Alíz a

$$c_j = p_j + k_j \bmod B, \qquad j = 1, 2, \ldots N \tag{2.3.1}$$

utasítással rendeli hozzá a kriptogramot a forrásszöveghez. Ezután Béci a már korábban, a biztonság kedvéért az üzenettől függetlenül megkapott kulcs birtokában vissza tudja állítani a kriptogramból a forrásszöveget, ami egy ismert számelméleti feladat.

Az eljárás előnye, hogy a kulcs betűinek véletlenszerű választása ,,kimossa" az ismétlődéseket a forrásszövegből. Ugyanakkor nagy hátrány, hogy (a) a kulcsban előzőleg meg kell egyezni, (b) a kulcsnak legalább olyan hosszúnak kell lennie, mint a forrásszövegnek, ami azt jelenti, hogy hosszú szövegek titkosítása nehézkes, (c) ugyanazt a kulcsot nem szabad kétszer felhasználni. Az utóbbit azért nem szabad csinálni, mert két, azonos kulccsal kódolt szó átfedéséből információt lehet kiolvasni a forrásszövegre nézve (Shannon, 1919).

Érdekességképpen, ezt a titkosítási eljárást széleskörben alkalmazták a II. világháborúban, a hidegháború korában és a Fehér Ház és a Kreml közötti ,,forró dróton" történő üzenetváltásban. Ma már ez a módszer csak történeti érdekességű.

2. *Nyilvános kulcs módszere.* Ez a módszer a 70-es években került kifejlesztésre (Diffie, Hellmann, 1976; Rivest, Shamir, Adleman, 1978: RSA-módszer) és azóta világszerte általánosan elterjedtté vált; pl. a világháló is ezt használja. Ennek a módszernek a lényege, hogy Béci, aki másoktól (pl. Alíztól) titkos üzeneteket akar kapni, most

   (a) nyilvánosan közzé tesz egy K_1 kulcsot, ez a *nyilvános kulcs*, amit bárki használhat, és ugyanakkor

   (b) megőrzi ennek a kulcsnak az ún. K_2 inverzét, a *privát kulcsot.*

   Ezután Alíz a nyilvános K_1 kulcs segítségével előállítja a forrásszövegből a kriptogramot, azt elküldi valamilyen klasszikus információs csatornán Bécinek, aki azt a K_2 privát kulcs, az eredeti K_1 inverzének birtokában meg tudja fejteni.

   Az eljárás érdekessége, hogy most a K_1 kulcs és a kódolási algoritmus is nyilvános, egyedül a K_1 kulcs inverzét nem ismeri senki Bécin kívül. A K_2 privát kulcs elvileg meghatározott algoritmus segítségével kiszámolható a K_1 kulcs ismeretében, azonban K_1-et meg lehet úgy választani, hogy az inverzének kiszámolásához szükséges CPU-idő elérhetetlenül nagy legyen. Az eljárás „lelke" éppen az a mód, ahogy meg kell választani a K_1 kulcsot ahhoz, hogy az inverzének a meghatározása gyakorlatilag ne legyen megoldható elérhető CPU-idők alatt. Erre vonatkozik az RSA-módszer, amelynek főbb lépései a következők:

   (a) *lépés: a K_1 kulcs megadása.* Béci választ egy N, kb. 200-300-jegyű egész számot. Ezt azonban nem akárhogyan teszi, hanem úgy, hogy két nagy, egyenként legalább 100-jegyű p_1 és p_2 prímszámot[1] választ véletlenszerűen, és ezeket szorozza össze: $N = p_1 p_2$. Prímszámok keresésére léteznek numerikus eljárások. Utána meghatározza a $[0, N)$ intervallumban az N-hez képest relatív prímszámok[2] $\varphi(N) = (p_1 - 1)(p_2 - 1)$ számát, és választ az $(1, \varphi(N))$ intervallumból egy egész számot, legyen ez d. Utóbbit tekinti a privát kulcsának, $K_2 \equiv d$. Ezután kiszámolja d és $\varphi(N)$ ismeretében a

   $$c\, d = 1 \mod \varphi(N) \tag{2.3.2}$$

   egyenlet megoldását jelentő $c \in (1, \varphi(N))$ számot. A nyilvános kulcs $K_1 \equiv (N, c)$ az N és c egész számokból áll.

   (b) *lépés:* Béci nyilvánosságra hozza azt a kölcsönösen egyértelmű leképezést, amelynek segítségével elő lehet állítani adott $(p_1, p_2, \ldots, p_n)$ $(n < N)$ forrásszövegből a megfelelő $(c_1, c_2, \ldots, c_n)$ kriptogramot:

   $$c_j = p_j^c \mod N. \tag{2.3.3}$$

   (c) Ezek után Alíz a forrásszövegét minél hosszabb, de $n < N$ elemű blokkokra bontja és azokat a nyilvános kulcs és a nyilvános kódolási algoritmus segítségével titkosítja, majd a kapott, blokkokkból álló kriptogramot elküldi Bécinek.

   (d) Béci a kapott blokkokat rendre dekódolja a birtokában lévő d privát kulcs segítségével:

   $$p_j = c_j^d \mod N. \tag{2.3.4}$$

[1] A prímszámok olyan pozitív egész számok, amelyeknek csak triviális osztóik vannak, az 1 és önmaguk.

[2] Két pozitív egész számot relatív prímszámnak nevezünk, ha a legnagyobb közös osztójuk 1.

Célszerűségi szempont, hogy d se legyen túl rövid és a neki megfelelő c szám sem.

Miben áll az eljárás biztonsága? Elvileg a N számot bárki prímtényezőkre bonthatja és ezután meghatározhatja $\varphi(N)$-et, majd pedig c ismeretében d-t, a privát kulcsot is. Ez azonban rendkívül időigényes eljárás a prímtényezőkre történő felbontás miatt. Egy 200 Mips (millió utasítás másodpercenként) számolási sebességű gépen egy 250-jegyű szám prímtényezőkre bontása a ma ismert algoritmusokkal legalább 10^7 év CPU-időt igényel. A nagy kihívást természetesen az jelenti, hogy az algoritmusok tökéletesedhetnek és a számítógépek is fejlődhetnek, aminek következtében lecsökkenhet a prímtényezőkre bontás időigénye. Becsléseket lehet végezni arra nézve, hogy mi várható ilyen tekintetben. Moore-törvénye szerint a számológépek teljesítőképessége 18-havonta megduplázódik, továbbá várhatóan 2020 körülre a hagyományos számítógépek elérik a miniatürizálási határt. Ha a 2000-ben elérhető 800 Mips számolási sebességet vesszük alapul és 1000 munkaállomás párhuzamos munkájával számolunk, akkor egy 2048-bites szám prímtényezőkre bontásához még 2020-ban is több mint 10^{10} CPU-év lesz szükséges.

2.3.2 Kvantumkriptográfia

A *kvantumkriptográfia* a kvantummechanikai módszerek alkalmazása a kriptográfia céljaira. A kvantumkriptográfia új lehetőséget nyit abban a tekintetben, hogy Alíz és Béci úgy egyezzenek meg a közös kulcsban (0-kból és 1-ekből álló bitsorozatban), hogy

1. ne legyen szükségük közvetítőre, és
2. észrevegyék ha a kulcsot illetéktelen fel akarja törni és megfelelő ellenintézkedéseket tehessenek.

Az eljárás lényege, hogy a kulcsot úgy küldi meg mondjuk Alíz Bécinek, hogy pl. optikai szálon meghatározott polarizációs állapotú fotonokat küld. Az alábbiakban ismertetek egy eljárást, a *BB84-protokolt*, amelyet Bennett és Brassard (1984) dolgoztak ki, és amely alkalmas a közös kulcs fenti értelmezésére. Ebben az eljárásban négyféle különböző polarizációs állapotban kell fotonokat előállítani és optikai szálon továbbítani. Legyen a 4 felhasznált polarizációs állapot valamely rögzített irányhoz képest 0^o (H), 45^o (D), 90^o (V) és 135^o (A) szöget bezáró irányban lineárisan poláros fotonállapot. Az eljárás lépései a következők:

1. *lépés:* Alíz a fenti polarizációs irányok közül fotononként véletlenszerűen választva előállít egy fotonsorozatot, és listát, ún. *rekordot* készít az egymás utáni fotonok állapotáról:

$$\begin{array}{cccccccccc} V & V & V & H & A & V & A & A & \dots \\ + & + & + & + & \times & + & \times & \times & \dots \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & \dots \end{array} \tag{2.3.5}$$

   ahol a H és V, ill. a D és A állapotokat közös jellel rendre + ill. $\times$, a H és D állapotokat, ill. a V és A állapotokat pedig rendre 0 ill. 1 jelöli. Ezt a fotonsorozatot Alíz optikai szálon elküldi Bécinek. A fotonok polarizációs állapotának beállításához Alíz kétféle polarizátor, az egyenes állású + és a „keresztezett" állású $\times$ között választ véletlenszerűen.

2. *lépés:* Bécinek Alíz polarizátoraival azonos állású + és $\times$ irányú analizátorai vannak. Ez azt feltételezi, hogy Alíz klasszikus csatornán közli Bécivel a használt

polarizátorok irányítására vonatkozó információt továbbá azt is, hogy mely polarizációs irányokhoz rendelt 0-t ill. 1-et. Béci minden beérkező fotont véletlenszerűen választott állású analizátorral analizál. Rekordot készít a használt analizátorokról és a mérés eredményéről. Ha az utóbbi 0^o vagy 45^o ill. 90^o vagy 135^o polarizációs irány, akkor rendre 0-t ill. 1-et ír az eredmények rekordjára (ez ugyanaz a megfeleltetés, mint amit Alíz használ):

$$\begin{array}{cccccccccc} \times & + & \times & + & \times & \times & \times & + & \ldots \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & \ldots \\ D & V & A & H & A & A & A & V & \ldots \end{array} \tag{2.3.6}$$

3. *lépés:* Kölcsönösen megüzenik egymásnak az Alíz által használt polarizátor-állások és a Béci által használt analizátor-állások rekordját valamilyen klasszikus kommunikációs csatornán:

$$\begin{array}{l|cccccccccc} \text{Alíz:} & + & + & + & + & \times & + & \times & \times & \ldots \\ \text{Béci:} & \times & + & \times & + & \times & \times & \times & + & \ldots \end{array} \tag{2.3.7}$$

4. *lépés:* Eldobják a rekordjaikról azokat az eseményeket, amelyek során Béci nem azt az analizátor állást választotta, mint ami Alíz polarizátorának állása volt:

$$\begin{array}{l|cccccccccc} \text{Alíz:} & \not{+} & + & \not{+} & + & \times & \not{+} & \times & \not{\times} & \ldots \\ & \not{1} & 1 & \not{1} & 0 & 1 & \not{1} & 1 & \not{1} & \ldots \\ \text{Béci:} & \not{\times} & + & \not{\times} & + & \times & \not{\times} & \times & \not{+} & \ldots \\ & \not{0} & 1 & \not{1} & 0 & 1 & \not{1} & 1 & \not{1} & \ldots \\ \hline \text{kulcs :} & - & 1 & - & 0 & 1 & - & 1 & - & \ldots \end{array} \tag{2.3.8}$$

A visszamaradó 0-kból és 1-esekből álló sorozatot használják kulcsként a titkosításhoz.

5. *lépés:* Végül Alíz és Béci kicserélik klasszikus kommunikációs csatornán a kapott kulcs egy véletlenszerűen kiválasztott darabját. Ha ez megegyezik mindkettőjüknél, akkor nagy valószínűséggel nem történt lehallgatás. Ekkor a kulcsból a kicserélt darabot eldobják és a maradékot használják fel a titkosítás során.

Az így kapott kulcs hossza kb. az eredeti fotonsorozat hosszának a fele. Az utolsó lépéssel a következőképpen indokolható. Tegyük fel, hogy Elemér le akarja hallgatni az optikai szálon továbbított fotonsorozatot, hogy a kulcs birtokába jusson. Ezért ő is analizálja az Alíz által elküldött fotonokat, majd ezután továbbítja azokat Bécihez. A kvantummechanika törvényei szerint azonban 0,5 valószínűséggel rossz analizátorállást fog használni és ezzel elrontja az Alíz által küldött foton polarizációs állapotát. Emlékezzünk rá, a foton polarizációs állapota csak akkor nem változik meg, ha olyan állású analizátort használunk, amelynek a foton polarizációs állapota éppen a sajátállapota. Annak a valószínűsége, hogy Béci a ,,lehallgatott" foton polarizációját másnak fogja találni, mint amilyennek Alíz beállította, $0,5 \cdot 0,5 = 0,25$. Ha tehát a kapott kulcs egy darabját A és B kicserélik, akkor véges valószínűséggel eltérést fognak benne találni, ami jelzi nekik, hogy lehallgatás történt. Ha nem találnak eltérést, akkor tudni fogják, hogy nem történt lehallgatás.

A kulcs továbbításának tetszőleges térbeli távolságon az szab határt, hogy a kvantummechanikai csatorna mennyire zajos és milyen valószínűséggel abszorbeálja a fotonokat. Nyilvánvalóan a rekordról törölni kell minden olyan eseményt, amikor az Alíz által elküldött foton nem érkezik meg Bécihez. (Annak érdekében, hogy a fotonkimaradást észre lehessen venni, Alíz meghatározott időközönként küldi a fotonokat.)

A kísérleti megvalósítás 1992-ben még levegőben történt és 32 cm távolságon bizonyult sikeresnek, újabban (2003) sikerült optikai szálon, speciálisan érzékeny fotodetektorok alkalmazásával a 100 km távolságra történő kulcs-továbbítás [5].

Jelenleg kifejlesztés alatt áll egy olyan, a világhálóhoz kapcsolódó hálózat kiépítése, amely alkalmas kvantumkulcs folyamatos létrehozására, és annak segítségével titkosított üzenetek folyamatos továbbítására a hálózat tagjai között [6].

3 Az elméleti kvantumszámítógép

A kvantumszámítógépek megvalósításának több lényeges fázisa van:

1. *fázis:* Annak matematikai belátása, hogy a számítási feladat jól definiált és megoldható. Másszóval ez annak a belátása, hogy legalább matematikai értelemben létezik univerzális számítógép, amely elvileg alkalmas a matematikai kérdések egy széles körének a megválaszolására. Ez a fázis napjainkban megoldott, ugyanúgy mint a megfelelő klasszikus számítógépekre vonatkozó matematikai feladat.

2. *fázis:* Annak megmutatása, hogy a matematikai probléma (valamely logikai függvény értékének kiszámolása) alkalmas logikai „körök" segítségével fizikailag elvégezhető. A klasszikus számítógépek esetén logikai áramkörökről van szó, amelyek bemeneti ill. kimeneti feszültségszintjei jelentik a bemenő ill. a kimenő adatokat és a számítási (logikai) „műveleteket" logikai kapuk valósítják meg. Hasonlóképpen a kvantumszámítógépekben a számítógép kezdeti ill. végső kvantumállapota határozza meg, hogy milyen bemenő adatokon végezzük a számolást ill. hogy annak az eredménye milyen kimenő adatokban testesül meg. A logikai műveleteket kvantumlogikai kapuk végzik. Ebben a fázisban tisztázni kell, hogy hányféle logikai kapu alkalmazása szükséges és elégséges az összes lehetséges logikai függvény kiszámításához. Ugyancsak fontos tudni, hogy a logikai függvény bonyolultságának megfelelően hogyan növekszik a számolás megvalósításához szükséges logikai kapuk száma. Ezek hasonló kérdések a klasszikus és a kvantumszámítás megvalósításával kapcsolatban.

3. *fázis:* A klasszikus számítógépben a bitek, a logikai kapuk, a logikai áramkörök tényleges fizikai kivitelezése, majd ezek összeépítése minél kisebb méretben (integrált áramkörök, csipek, ill. ezek összépítése), majd a számítógép összeépítése az adatok be- és kiviteléhez ill. a számolási algoritmus beviteléhez szükséges perifériákkal. Hasonló lépések szükségesek a kvantumszámítógép megvalósításához is. Ebben jelenleg (2003) kb. ott tartunk, hogy ismeretes sokféle módszer, hogyan lehet kubiteket, kvantumlogikai kapukat fizikailag megvalósítani. Eddig azonban nem sikerült még néhány kubitnél többet tartalmazó kvantumszámítógépet építeni. A fizikai megvalósítás terén tehát még nagyon messze vagyunk attól, hogy működő és elvileg tetszőleges számítások elvégzésére alkalmas kvantumszámítógépünk legyen. Azt is érdemes megjegyezni, hogy a kvantumszámítógép megalkotásának eddig említett fázisai semmivel sem egyszerűbbek, mint a klasszikus számítógép létrehozásának megfelelő fázisai, s a várható előnyök nem ezen fázisok valamelyikének egyszerűsödésében jelentkeznek.

4. *fázis:* A számítások elvégzéséhez szükséges algoritmusok kidolgozása. Ezen a területen lehet várni, hogy speciális számolási feladatok elvégzése a kvantumalgoritmusok felhasználásával kvantumszámítógépeken lényegesen felgyorsul (CPU-időben mérve) a megfelelő klasszikus algoritmusokkal, klasszikus számítógépeken történő számolásokhoz képest.

   A számolási idő drasztikus lerövidülését az alábbiak miatt lehet remélni. Egy N kubitből álló kvantumszámítógépnek $\mathcal{O}(e^{N \ln 2})$ bázisállapota van. Ennyiféle kezdeti adatsoron tud számolást végezni. A lineáris szuperpozíció elve miatt azonban be lehet állítani olyan kezdeti állapotot, amely az összes ilyen számolási bázisállapotnak a lineáris kombinációja. Ez akkor azt fogja jelenteni, hogy a kvantumszámítógép automatikusan párhuzamosan végzi el az adott számolást az össze lehetséges bemenő adaton. Azt kell mondjuk, hogy a kvantummechanikai lineáris szuperpozíció elve a kvantumszámítógépek működtetése során abban hasznosul, hogy a kvantumszámítások eredendően *párhuzamosak*, azaz sok adaton egyidejűleg történik ugyanazon utasítás-sorozat végrehajtása. Ez a *kvantumpárhuzamosság elve.*

A megfelelő eredmények a számítógép végállapotában fognak ugyancsak lineáris kombináció alakjában rendelkezésre állni. Persze ott veszíthetünk, hogy a minket érdeklő bemenő adathoz tartozó végeredményt ki kell tudnunk olvasni ebből a végállapoti lineáris kombinációból. A megfelelő kvantumalgoritmus éppen azt a célt szolgálja, hogy ez minél egyszerűbben, pontosabban, a számítógép minél kevesebb CPU-idejének felhasználásával lehetséges legyen. Az ügyesen választott kvantumalgoritmusok a számolási bázisállapotok *erősítő interferenciáját* tudják kihasználni. Az erősítő interferencia segítségével el lehet érni, hogy a végállapot méréséből nagy valószínűséggel azt az információt (számolási eredményt) olvassuk ki, amelyre valóban szükségünk van.

Alább megismerkedünk néhány kvantumalgoritmussal, amelyek segítségével speciális feladatok elvileg lényegesen gyorsabban oldhatók meg, mint a hagyományos számítógépeken. Ilyen pl. adott elem kikeresése adott listáról, ill. egész szám prímtényezőkre bontása. Néhány kubites kvantumszámítógépen mindkét eljárást demonstrálták. Jelenleg bizonyítottnak tekinthető, hogy van valóban néhány olyan számolási feladat, amely kvantumszámítógépeken kvantumalgoritmusok alkalmazásával sokkal gyorsabban elvégezhető lesz, mint a klasszikus számítógépeken. Az ilyen feladatok és algoritmusok keresésében még bizonyára csak az első, kezdeti lépéseket tesszük.

3.1 Matematikai számítógép

A kvantumszámítógépek elvi alapjait matematikai állítások formájában fogalmazták meg. A kvantumszámítógép matematikai modellje az ún. kvantum-Turing-gép. Ez olyan számítógép, amely kubitekből álló végtelen szalagból, egy a szalag valamely kubitjére mutató fejből („cursor") és véges sok kubitből álló vezérlő egységből áll. A gép véges T időtartamú lépésekben működik. Minden lépésben csak a szalag véges sok kubitje és a vezérlő egység hatnak kölcsön a mutatófejjel. A gép adott utasítás végrehajtására szolgál. Az utasítás unitér időfejlesztő operátor, amely a kvantum-Turing-gép kvantumállapotainak Hilbert-terén (a szalag, a fej és a vezérlő egység Hilbert-tereinek direktszorzat terén) hat. Ez az operátor lokálisan hat a szalagon, azaz minden lépésben csak egy kubit állapotát befolyásolja, amelyre a mutatófej mutat és azt mindig eggyel lépteti balra vagy jobbra. Az is fel van tételezve, hogy véges sok lépésben hajtja végre az utasítást. Az egyik jelentős matematikai lépés az volt, hogy belátták, minden véges szabadsági fokú kvantummechanikai rendszeren ható unitér időfejlesztő operátorhoz létezik egy megfelelő kvantum-Turing-gép.

Megmutatták, hogy elvileg lehetséges olyan univerzális kvantum-Turing-gépet szerkeszteni, amelyik tetszőleges utasítást végre tud hajtani, azaz amelyik programozható. Elvileg tehát nem kell minden feladathoz másik számítógépet építeni.

Már a kvantumszámítógép matematikai modellje is tükrözi a kvantumszámítások két nagyon jellegzetes vonását. A kvantumszámítógép kezdeti állapotának megadásával (pontosabban a szalag meghatározott kubitjeinek megfelelő állapotával) vihetjük be azokat az adatokat, amelyeken a számolást (az adott utasítást ill. azok sorozatát) el akarjuk végezni. A kvantummechanika azonban megengedi, hogy a kezdeti állapot ne csak valamelyik számolási bázisállapot lehessen, hanem a számolási bázisállapotoknak tetszőleges lineáris kombinációja. Ez azt jelenti, hogy a számolás párhuzamosan (egyidejűleg) végezhető el akár az összes lehetséges számolási bázisállapoton. Ezt nevezzük *kvantumpárhuzamosságnak*. A kvantumpárhuzamosság alapja nyilvánvalóan a kvantummechanikai lineáris szuperpozíció elve. Természetesen ahhoz, hogy ezt a párhuzamosságot valóban jól tudjuk kihasználni, valahogy ki kell tudjuk olvasni a minket érdeklő bemenő adathoz tartozó számolási eredményt a kvantumszámítógép végállapotából. Utóbbi ugyancsak lineáris kombináció alakjában tartalmazza ugyanis az egyes bemenő adatokhoz tartozó számolási eredményeket.

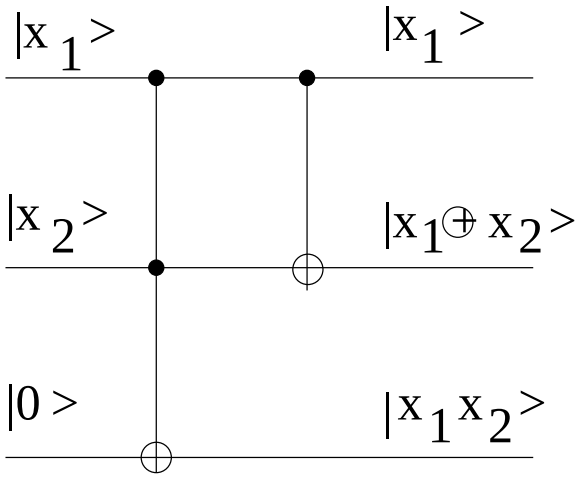

Figure 2: A $\oplus$-összeadás megvalósítása T- és CNOT-kapu segítségével.

Az eredmény kiolvasásában az *erősítő interferencia* lehet segítségünkre. A különböző bemeneti számolási bázisállapotok meghatározott amplitudókkal feljődnek valamilyen állapotba az utasításokat jelentő unitér időfejlesztő operátorok hatására. A ténylegesen kialakuló végállapot ezen amplitudók szuperpozíciójaképpen jön létre. Az amplitudók erősítő interferenciáját kihasználva kierősíthetjük azt az eredményt, amelyet ki szeretnénk olvasni és elnyomhatjuk azokat az eredményeket, amelyekre valójában nincsen szükségünk. Így nagy valószínűséggel a szalag megfelelő kubitjei végállapotának mérésekor a kívánt eredményt fogjuk kiolvasni. Ezen a ponton játszanak szerepet a *kvantumalgoritmusok*, amelyek alkalmas megválasztásával nemcsak azt kell elérni, hogy kiszámoljuk, amit ki akarunk, hanem azt is, hogy nagy valószínűséggel az a számolási eredmény legyen kiolvasható a végállapotból, amelyre kíváncsiak vagyunk.

3.2 Műveletek kvantumlogikai kapukkal

3.2.1 Kvantumaritmetika

Az elemi logikai kapuk, amelyeket egy korábbi fejezetben sorra vettünk, felhasználhatók aritmetikai műveletek végzésére. Az elemi kvantumkapukra bebizonyítottak egy *univerzalitási tételt* (Barenco, 1995). Ennek értelmében az egy-kubites kapuk és a CNOT-kapu az elemi kapuk olyan halmaza, amely elegendő az egzakt kvantumszámításokhoz. A kvantumszámítások elméleti lehetősége mellett azonban fontos technikai kérdés is felmerül. Nevezetesen, hogy egy tetszőleges n-kubites $\hat{U}$ kaput legkevesebb hány elemi kapu felhasználásával lehet adott ϵ pontossággal megközelíteni. A szükséges elemi kapuk száma $> \mathcal{O}(n4^n \log^c(n4^n/\epsilon))$. Ez az alsó korlát a kubitek számától exponenciálisan függ, s ezért technikailag a legtöbb kapu szimulálása reménytelen.

A kvantumaritmetika legfontosabb műveletei, a szorzás (logikai és), az $\oplus$-összeadás és a hatványozás modulo N (N egész szám) azonban beépíthetők a T(offoli)-kapuba. Mint az az 1. ábráról leolvasható, ha a harmadik kubit a $|0\rangle$ bázisállapotban van, akkor $\hat{U}_T$ hatására a harmadik kubit éppen a $|x_1 x_2\rangle = |x_1 \wedge x_2\rangle$ állapotba kerül, ami a szorzásnak, ill. a logikai és-nek felel meg.

A *körplusz- ($\oplus$)-összeadás, azaz a bitenkénti összeadás modulo 2.* a CNOT-kapuval

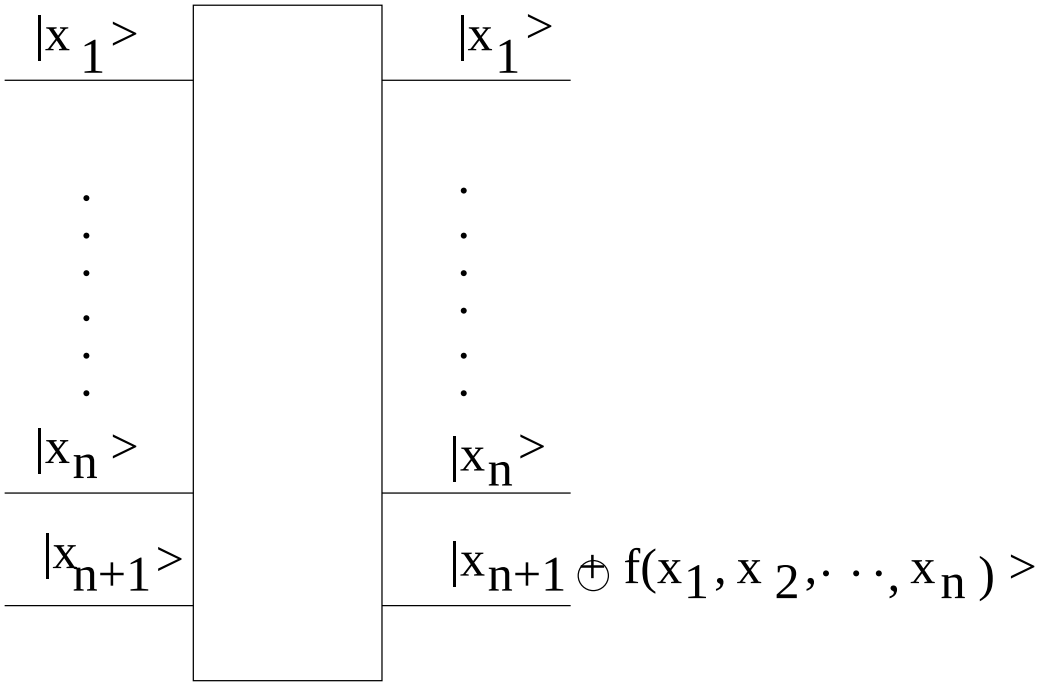

Figure 3: A $f : \{0,1\}^n \mapsto \{0,1\}$ függvényt megvalósító $\hat{U}_f$ orákulum szemléltetése.

kivitelezhető, amelynek hatására a második kubit állapota éppen $|x_1 \oplus x_2\rangle$ lesz. Ez hozzáépíthető a T-kapuhoz, és ha a harmadik kubit bemenő állapota $|0\rangle$, akkor a második kubit kimenő állapota éppen $|x_1 \oplus x_2\rangle$ lesz. A körplusz-összeadás megvalósítását az 2. ábra szemlélteti.

3.2.2 Logikai függvények

Az n-változós Boole-függvények kiszámítása matematikailag elemi logikai műveletek egymás utáni elvégzését jelenti. Utóbbiaknak unitér operátorok felelnek meg. Ezért az f Boole-függvények kiszámítása is elvileg úgy végezhető el, hogy alkalmasan választott $\hat{U}_f$ unitér operátorral hatunk egy megfelelő hosszúságú kvantumregiszter állapotára.

Legyen az egyszerűség kedvéért a kiszámolandó Boole-függvény

$$f : \{0,1\}^n \mapsto \{0,1\}. \tag{3.2.9}$$

Az ilyen, n-változós f Boole-függvények n darab változója értékeinek megadásához n darab kubit szükséges. Ezek alkotják a kvantumregiszter ún. *forrásregiszter* részét. A számolás eredményének, azaz a függvényértéknek a tárolására egy további kubitre van szükség, utóbbi alkotja a kvantumregiszter *targetregiszter* részét. Az n-változós $f(x_1, x_2, \ldots, x_n) \in \{0,1\}$ függvény értékeinek *lekérdezését* olyan $\hat{U}_f$ unitér operátor valósítja meg, amely az $(n+1)$-kubites kvantumregiszter állapotainak Hilbert-terén hat. Az unitaritás következtében a függvényérték nem jelenhet meg mint kimenet, helyette belátható, hogy a targetregiszter végállapota $|x_{n+1} \oplus f(x_1, x_2, \ldots, x_n)\rangle$ alakban kell tartalmazza az eredményt.

Azt könnyű belátni, hogy $|f(x_1, x_2, \ldots, x_n)\rangle$ nem jelenhet meg mint a target regiszter végállapota. Tegyük fel az ellenkezőjét. Vizsgáljuk továbbá azt az esetet, amikor

f nem kölcsönösen egyértelmű leképezés. Akkor létezik a forrásregiszternek legalább két olyan $|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ ill. $|x'_1\rangle \otimes |x'_2\rangle \otimes \cdots \otimes |x'_n\rangle$ egymásra ortogonális állapota, hogy a targetregiszter kimenetén $|f(x_1, x_2, \ldots, x_n)\rangle = |f(x'_1, x'_2, \ldots, x'_n)\rangle$ lenne, úgyhogy a kvantumregiszternek két ortogonális kezdeti állapothoz két nem ortogonális végállapota tartozna, ami ellentmond az $\hat{U}_f$ operátor unitaritásának.

Szokásos szóhasználat, hogy az f függvény értékeinek lekérdezését megvalósító $\hat{U}_f$ unitér operátort, ill. ennek fizikai megvalósítását az f függvényhez tartozó *orákulumnak*, röviden *f-orákulumnak* nevezik.

3.3 Kvantumalgoritmusok

Az alábbiakban ismertetek néhány kvantumalgoritmust, amelyek lehetővé teszik speciális számolási feladatok lényegesen kevesebb CPU-lépésben történő megoldását, mint a megfelelő klasszikus algoritmusok. Részletesen bemutatom

1. a Deutsch-Józsa algoritmust, amely annak eldöntésére szolgál, hogy egy Boole-függvény, amely csak kiegyensúlyozott vagy állandó lehet, a két lehetőség közül melyiket valósítja meg;
2. a Grover-algoritmust, amely egy rendezetlen listában egyetlen elem megkeresésére szolgál;
3. a Shor-algoritmust, amely egész számok relatív prímszámok szorzatára történő felbontására szolgál.

Újabban kidolgoztak egy kvantumalgoritmust klasszikus dinamikai rendszer vizsgálatára, pontosabban az ún. Poincaré-féle visszatérési idők és a periodikus pályák numerikus meghatározására [10]. Arról van ,,durván" szó, hogy a fázistér tetszőlegesen kis tartományának bizonyos pontjai a dinamikai rendszer evolúciója során, meghatározott visszatérési idő után visszatérnek ugyanebbe a tartományba. A periodikus pályák pedig olyan pályák, amelyek mentén a fázispont egzaktul visszatér önmagába. A vissztérési időt ill. a periodikus pályákat csak numerikusan lehet meghatározni. Mindkét jellemző ismerete fontos a Hamilton-i és a disszipatív dinamikai rendszerek fizikai tulajdonságainak megértésében: pl. diffúziós együtthatók meghatározását és a különös attraktor tulajdonságainak meghatározását teszik lehetővé. Mivel a visszatérési idő ill. a periodusidő lehet nagyon nagy, ezért annak numerikus meghatározása klasszikus algoritmussal az elérhető CPU-idők alatt általában nagy nehézségbe ütközik.

3.3.1 Deutsch-Józsa-algoritmus

A Deutsch-Józsa-algoritmus arra alkalmas, hogy egy logikai függvény (Boole-függvény) bizonyos tulajdonságát döntsük el. Legyen f egy n-változós Boole-függvény: f :

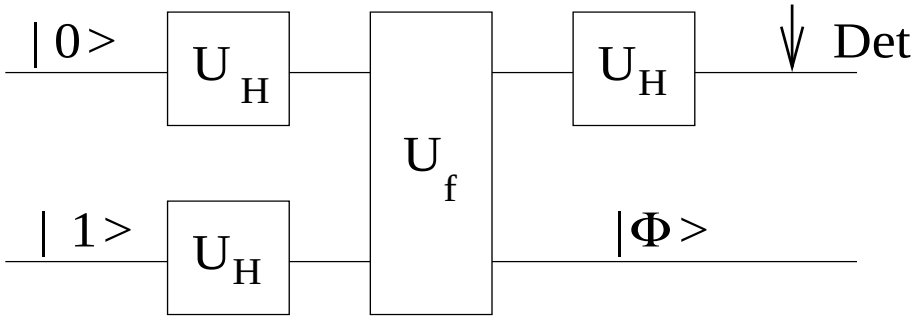

Figure 4: Deutsch-Józsa-algoritmus egy-változós Boole-függvény vizsgálatára. A nyíl az első kubit állapotát mérő detektort (Det) jelöli.

$\{0,1\}^n \mapsto \{0,1\}$, amelyről tudjuk, hogy vagy

1. állandó, azaz bármely x_1 és $x_2 \in \{0,1\}^n$ esetén $f(x_1) = f(x_2)$, vagy
2. kiegyensúlyozott, azaz ugyannyi x helyen vesz fel 0 értéket, mint ahány helyen 1 értéket.

A feladat az, hogy eldöntsük, az f függvény állandó, vagy kiegyensúlyozott? Az algoritmus megadásakor feltételezzük, hogy adott az a fizikai eljárás, amely megvalósítja az f függvénynek megfelelő $\hat{\mathcal{U}}_f$ unitér operátort. Az algoritmus abból áll, hogy véges számú kubitet tartalmazó *kvantumregiszterre* meghatározott sorrendben unitér operátorokkal hatunk, azaz a regiszter állapotát kvantumlogikai kapukon ,,bocsátjuk át".

Megjegyezzük, hogy a megfelelő klasszikus algoritmus (a legrosszabb esetben) $2^{n-1}+1$ darab függvényérték lekérdezését igényli. Ezzel szemben az alább ismertetésre kerülő kvantumalgoritmus segítségével már egyetlen lekérdezés elegendő a feladat megoldásához. Realisztikusabb a feladat megoldásának felgyorsulásáról alkotott képünk, ha azt nézzük, hogy a függvény értékének hány M helyen történő lekérdezésére lenne klasszikus algoritmus alkalmazása esetén szükség ahhoz, hogy $0 < \epsilon < 1$ hibavalószínűséggel el tudjuk dönteni, melyik eset áll fenn. Ha a függvényértékeket véletlenszerűen választott M helyen kérdeztük le és minden értéket azonosnak találtunk, akkor 2^{-M} hibavalószínűséggel állíthatjuk, hogy a függvény állandó. Ezért az ϵ pontosság eléréséhez $M = \mathcal{O}(-\log_2 \epsilon)$ lépés szükséges klasszikus esetben. Ezzel áll szemben a függvény egyszeri lekérdezése kvantumalgoritmus alkalmazása esetén.

1. *Egy-változós függvény esete:* Először $n = 1$-változós Boole-függvény esetére ismertetjük az algoritmust. Az f függvény akkor és csak akkor kiegyensúlyozott, ha $f(0) \neq f(1)$, egyébként állandó. Az algoritmust a 4. ábra szemlélteti.

(a) *lépés:* Előállítjuk a 2-kubites kvantumregiszter $|\Psi_1\rangle = |01\rangle$ kezdeti állapotát.

(b) *lépés:* Kubitenként hatunk a Hadamard-kapuval:

$$|\Psi_2\rangle = \hat{U}_H|0\rangle \otimes \hat{U}_H|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle). \tag{3.3.10}$$

(c) *lépés:* Az $\hat{U}_f$ operátorral lekérdezzük az f függvény értékét:

$$|\Psi_3\rangle = \hat{U}_f|\Psi_2\rangle = \frac{1}{2}\Big[|0\rangle\otimes\Big(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\Big) + |1\rangle\otimes\Big(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\Big)\Big]. \tag{3.3.11}$$

Felhasználva, hogy

$$\begin{aligned} |0\oplus f(0)\rangle - |1\oplus f(0)\rangle &= \begin{cases} |0\rangle - |1\rangle, & \text{ha} \quad f(0)=0 \\ |1\rangle - |0\rangle, & \text{ha} \quad f(0)=1 \end{cases} = (-1)^{f(0)}(|0\rangle - |1\rangle), \\ |0\oplus f(1)\rangle - |1\oplus f(1)\rangle &= (-1)^{f(1)}(|0\rangle - |1\rangle), \end{aligned} \tag{3.3.12}$$

ennek a lépésnek az eredményeként a

$$|\Psi_3\rangle = \frac{1}{2}\sum_{x=0,1}|x\rangle \otimes (-1)^{f(x)}(|0\rangle - |1\rangle) \tag{3.3.13}$$

állapotba kerül a kvantumregiszter.

(d) *lépés:* A Hadamard-kapuval hatunk az első kubitre:

$$|\Psi_4\rangle = \frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}\hat{U}_H|x\rangle \otimes (|0\rangle - |1\rangle). \tag{3.3.14}$$

Itt

$$\begin{aligned} \sum_{x=0,1}(-1)^{f(x)}\hat{U}_H|x\rangle &= \frac{1}{\sqrt{2}}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(-1)^{f(1)}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}\Big((-1)^{f(0)} + (-1)^{f(1)}\Big)|0\rangle + \frac{1}{\sqrt{2}}\Big((-1)^{f(0)} - (-1)^{f(1)}\Big)|1\rangle \\ &= \frac{1}{\sqrt{2}}\sum_{x=0,1}\Big((-1)^{f(x)}|0\rangle + (-1)^{x+f(x)}|1\rangle\Big), \end{aligned} \tag{3.3.15}$$

úgyhogy az eredményül kapott állapot:

$$|\Psi_4\rangle = \frac{1}{2\sqrt{2}}\sum_{x=0,1}\Big((-1)^{f(x)}|0\rangle + (-1)^{x+f(x)}|1\rangle\Big) \otimes (|0\rangle - |1\rangle). \tag{3.3.16}$$

(e) *lépés:* Végül mérjük az első kubit állapotát. Ha azt $|0\rangle$-nak ill. $|1\rangle$-nek találjuk, akkor az f függvény rendre állandó, ill. kiegyensúlyozott.
Ezt a következőképpen látjuk be:

i. A függvény akkor és csak akkor állandó, ha $f(0) = f(1) = 0$ vagy 1. De ekkor

$$\sum_{x=0,1} (-1)^{f(x)} = 2 \text{ vagy } -2,$$
$$\sum_{x=0,1} (-1)^{x+f(x)} = 0, \tag{3.3.17}$$

azaz a regiszter állapota

$$|\Psi_4\rangle \propto |0\rangle \otimes (|0\rangle - |1\rangle), \tag{3.3.18}$$

és az első kubit állapota bizonyossággal $|0\rangle$.

ii. A függvény akkor és csak akkor kiegyensúlyozott, ha $f(0) \neq f(1)$, de ekkor

$$\sum_{x=0,1} (-1)^{f(x)} = (-1)^{f(0)} + (-1)^{f(1)} = 1 - 1 = 0,$$
$$\sum_{x=0,1} (-1)^{x+f(x)} = (-1)^{f(0)} - (-1)^{f(1)} \neq 0, \tag{3.3.19}$$

úgyhogy

$$|\Psi_4\rangle \propto |1\rangle \otimes (|0\rangle - |1\rangle), \tag{3.3.20}$$

azaz az első kubit állapota bizonyosan $|1\rangle$.

2. $n > 1$ *változós függvény esete:* az algoritmust a 5. ábra szemlélteti.

Jelölje az egyes forráskubitek állapotait rendre $|x_0\rangle$, $|x_1\rangle$, ..., $|x_{n-1}\rangle$. Ekkor egy tetszőleges bemenő állapot $|\underline{x}\rangle = |x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle$, ahol

$$x = \sum_{i=0}^{n-1} x_i 2^i. \tag{3.3.21}$$

A kvantumregiszter kezdeti állapota $\Phi_1\rangle = |\underline{0}\rangle \otimes |1\rangle$. Hassunk ezután minden egyes kubitre Hadamard-kapuval:

$$|\Phi_2\rangle = (\hat{U}_H|0\rangle) \otimes \cdots \otimes (\hat{U}_H|0\rangle) \otimes (\hat{U}_H|1\rangle). \tag{3.3.22}$$

Itt az első n darab tényező $\hat{U}_H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, úgyhogy

$$|\Phi_2\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes \frac{1}{\sqrt{2}} \sum_{y=0,1} (-1)^y |y\rangle. \tag{3.3.23}$$

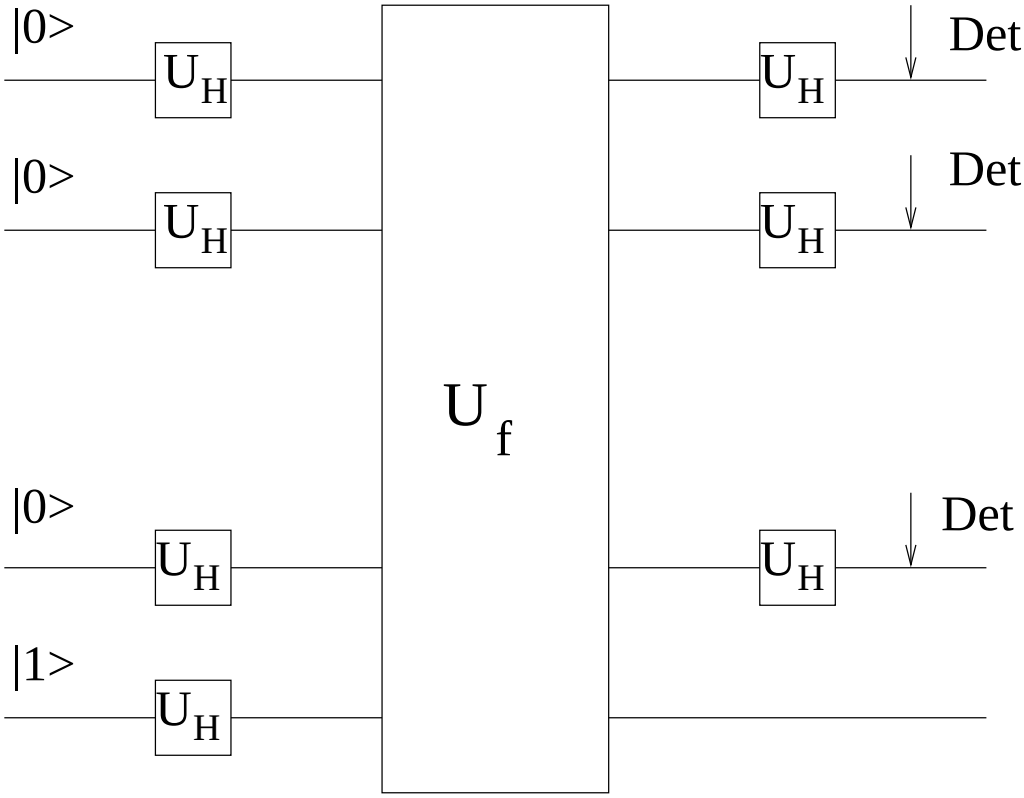

Figure 5: Deutsch-Józsa-algoritmus n-változós Boole-függvény vizsgálatára, ha $n > 1$. A nyilak a megfelelő kubitek állapotát mérő detektorokat (Det) jelölik.

Az f függvény lekérdezésének hatására a kvantumregiszter a

$$|\Phi_3\rangle = \hat{U}_f|\Phi_2\rangle = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|\underline{x}\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^y|y\rangle \tag{3.3.24}$$

állapotba kerül. Ezután az első n darab kubitre Hadamard-kapuval hatunk:

$$\begin{aligned}|\Phi_4\rangle &= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(\hat{U}_H^{\otimes n}|\underline{x}\rangle) \otimes \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^y|y\rangle \\ &= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}\sum_{x'=0}^{2^n-1}(-1)^{x\cdot x'+f(x)}|\underline{x}'\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^y|y\rangle, \end{aligned} \tag{3.3.25}$$

ahol

$$x \cdot x' = \sum_{i=0}^{n-1} x_i x_i' \in \{0,1\}. \tag{3.3.26}$$

Ha az f függvény állandó, akkor a $(-1)^f$ tényező kiemelhető az x-re vonatkozó összegzés alól. Ekkor az x-re vonatkozó összeg akkor és csak akkor nem zérus, ha $x' = 0$, azaz $x_0 = x_1 = \ldots = x_{n-1} = 0$, és ekkor

$$|\Phi_4\rangle = 2^{n/2}(-1)^f|\underline{0}\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^y|y\rangle. \tag{3.3.27}$$

Másrészt, ha f kiegyensúlyozott, akkor $x' = 0$ esetén az x-re vonatkozó összeg zérust ad eredményül, vagyis ekkor a forrásregiszter $|\underline{0}\rangle$ állapota nincsen jelen a $|\Phi_4\rangle$ állapotban. Az f függvény tehát akkor és csak akkor állandó, ha mind az n darab forráskubit az algoritmus befejezésekor $|0\rangle$ állapotban van, egyébként f kiegyensúlyozott. Az első n darab kubit állapotának mérése alapján tehát bizonyossággal eldönthető, hogy f a két lehetséges tulajdonság közül melyikkel rendelkezik.

A fenti feladat az ún. strukturált problémák közé tartozik. Ilyenkor nem a függvény értékeit keressük, hanem azt tudjuk, hogy a függvényre bizonyos igéretek közül valamelyik biztosan teljesül és azt kell eldönteni, hogy melyik. Eléggé kérdéses az ilyen típusú problémák gyakorlati jelentősége, mégis a fenti példa bizonyítja, hogy van olyan probléma, amely kvantumalgoritmus segítségével hatékonyabban oldható meg, mint klasszikus algoritmussal.

A továbbiakban ismertetjük a Grover- és a Shor-algoritmust, amelyek arra példák, hogy a kvantumalgoritmusok a nem strukturált problémák megoldásában is hatékonyabbak bizonyos esetekben, mint a klasszikus algoritmusok.

3.3.2 Grover-algoritmus

A Grover-algoritmus azt a célt szolgálja, hogy N darab elemből álló, rendezetlen listából kiválasszunk (kikeressünk) egy adott elemet. A megfelelő klasszikus algoritmus általában $\mathcal{O}(N)$ számú próbálkozást igényel ahhoz, hogy a keresett elemre rátaláljon. Az alább ismertetésre kerülő Grover-algoritmus alkalmazása ezzel szemben csak $\mathcal{O}(\sqrt{N})$ számú próbálkozást igényel.

A feladat a következő: Legyen adott az $N = 2^n$ darab elemből álló $\mathcal{L} = \{0, 1, 2, \ldots, N-1\}$ lista és legyen $x_0 \in \mathcal{L}$ a keresett elem. Tegyük fel továbbá, hogy a lista rendezetlen, azaz az elemek sorrendje véletlenszerű. A feladat az, hogy megtaláljuk a listában a x_0 keresett elemet.

A megoldáshoz vezessük be az x_0 elem karakterisztikus függvényét:

$$f_{x_0}(x) = \begin{cases} 1, & \text{ha} \quad x = x_0 \\ 0, & \text{ha} \quad x \neq x_0 \end{cases} . \tag{3.3.28}$$

A keresett elemre úgy fogunk rátalálni, hogy lekérdezzük a hozzá tartozó karakterisztikus függvény értékét, és ha azt 1-nek találjuk, akkor megleltük a keresett elemet.

Építsünk ezért egy n darab forráskubitből és a karakterisztikus függvény értékének kiszámolásához felhasználható 1 darab targetkubitből álló kvantumregisztert. A kvantumregiszter állapotát $|x\rangle \otimes |y\rangle$ jelöli, ahol az első tényező a forráskubitek, a második a targetkubit állapota. A továbbiakban fel fogjuk tételezni, hogy rendelkezésre áll az f_{x_0}-orákulum, $\hat{U}_{f_{x_0}}$, amely lekérdezi a keresett elem $f_{x_0}(x)$ karakterisztikus függvényének értékét:

$$\hat{U}_{f_{x_0}} |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f_{x_0}(x)\rangle. \tag{3.3.29}$$

A Grover-algoritmus fő vonása, hogy

1. a kezdeti $|x\rangle$ állapot olyan, hogy benne lineáris szuperpozíció alakjában a lista valamennyi elemének megfelelő számolási bázisállapot egyidejűleg jelen van;
2. az $\hat{U}_{f_{x_0}}$-orákulum néhányszori alkalmazásával eléri, hogy megtaláljuk a keresett x_0 elemet.

Az algoritmus az alábbi lépésekből áll (ld. 6. ábra):

1. *lépés:* Az induló állapot beállítása:

$$|\Psi_1\rangle = |00\ldots0\rangle \otimes |1\rangle. \tag{3.3.30}$$

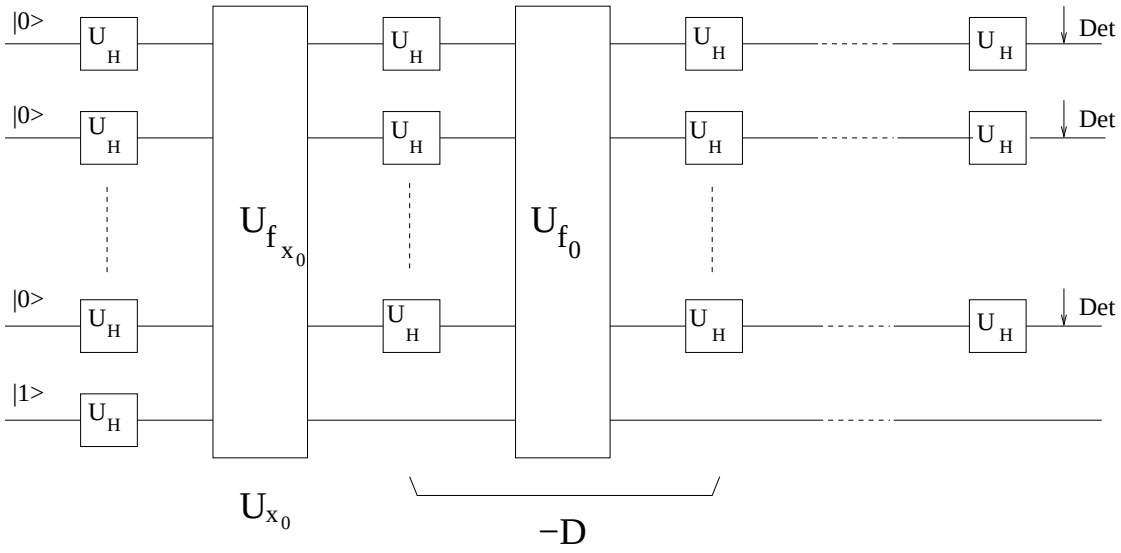

Figure 6: A Grover-algoritmus szemléltetése. A nyilak a megfelelő kubitek állapotát mérő detektorokat (Det) jelölik.

2. *lépés:* A tulajdonképpeni kezdőállapot beállítása. Ez olyan állapot, amely a lista valamennyi elemének megfelelő számolási bázisállapotot azonos amplitudóval tartalmazó lineáris szuperpozíció. Előállítása úgy történik, hogy a forrásregiszter minden kubitjére Hadamard-kapuval hatunk:

$$|\Psi_2\rangle = 2^{-\frac{1}{2}(n+1)} \sum_{x=0}^{2^n-1} |x\rangle \otimes \sum_{y=0,1} (-1)^y |y\rangle. \tag{3.3.31}$$

A targetregiszter kubitjére is hatottunk egy Hadamard-kapuval.

3. *lépés:* az x_0 elem karakterisztikus függvényének lekérdezése:

$$|\Psi_3\rangle = \hat{U}_{f_{x_0}} |\Psi_2\rangle = 2^{-\frac{1}{2}(n+1)} \sum_{x=0}^{2^n-1} (-1)^{f_{x_0}(x)} |x\rangle \otimes \sum_{y=0,1} (-1)^y |y\rangle. \tag{3.3.32}$$

Itt felhasználtuk, hogy

$$(-1)^{y \oplus f_{x_0}(x)} = (-1)^{y + f_{x_0}(x)}. \tag{3.3.33}$$

Mi is történt valójában ebben a lépésben? Csak annyi, hogy a lineáris szuperpozícióban egyedül az $|x_0\rangle$ állapot amplitudója változott $+1$-ről -1-re. Az $\hat{U}_{f_{x_0}(x)}$ orákulum lekérdezése tehát egyenértékű az $|x_0\rangle$ állapot előjelét megfordító $\hat{U}_{x_0}$ operátor hatásával:

$$\hat{U}_{x_0}|x\rangle = (1 - 2|x_0\rangle\langle x_0|)|x\rangle = \begin{cases} -|x_0\rangle, & \text{ha} \quad x = x_0 \\ |x\rangle, & \text{ha} \quad x \neq x_0 \end{cases}. \tag{3.3.34}$$

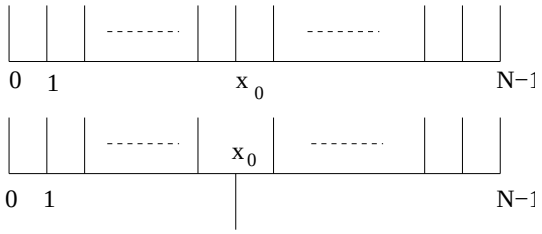

Figure 7: Az x_0 elem megjelölésének szemléltetése.

Ennek segítségével írhatjuk azt is, hogy

$$|\Psi_3\rangle = \hat{U}_{x_0}|x\rangle \otimes \hat{1}|y\rangle = (\hat{U}_{x_0} \otimes \hat{1})|\Psi_2\rangle. \tag{3.3.35}$$

Szemléletesen úgy lehet ezt ábrázolni, hogy elképzelünk egy fésűt, amelynek fogai a lista egyes elemeinek megfelelő állapotok és a fogak hossza és iránya ezen állapotok amplitudója. Azt tettük, hogy az x_0 fogat átfordítottuk (ld. 7. ábra)

4. *lépés:* Az amplitudóknak a várható értékükre történő inverziója, amelyet a

$$\hat{D} = -(\hat{U}_H^{\otimes n} \otimes \hat{1})\hat{U}_{f_0}(\hat{U}_H^{\otimes n} \otimes \hat{1}) \tag{3.3.36}$$

operátor valósít meg, ahol $\hat{U}_{f_0} \equiv \hat{U}_{f_{x_0=0}}$. Ennek hatására a kvantumregiszterállapota

$$\begin{aligned}
&\hat{D}\sum_{x}^{2^n-1}\alpha_x|x\rangle \otimes \sum_{y=0,1}(-1)^y|y\rangle \\
&= -2^{-\frac{1}{2}n}\sum_{x}^{2^n-1}\alpha_x(\hat{U}_H^{\otimes n} \otimes \hat{1})\hat{U}_{f_0}\sum_{x'}^{2^n-1}(-1)^{x\cdot x'}|x'\rangle \otimes \sum_{y=0,1}(-1)^y|y\rangle \\
&= -2^{-\frac{1}{2}n}\sum_{x}^{2^n-1}\alpha_x\sum_{x'}^{2^n-1}(-1)^{x\cdot x'+f_0(x')}(\hat{U}_H^{\otimes n} \otimes \hat{1})|x'\rangle \otimes \sum_{y=0,1}(-1)^y|y\rangle \\
&= -2^{-n}\sum_{x}^{2^n-1}\alpha_x\sum_{x'}^{2^n-1}\sum_{x''}^{2^n-1}(-1)^{x\cdot x'+x''\cdot x'+f_0(x')}|x''\rangle \otimes \sum_{y=0,1}(-1)^y|y\rangle \\
&= \sum_{x''=0}^{2^n-1}\left[2^{-n}\sum_{x}^{2^n-1}\alpha_x - 2^{-n}\sum_{x}^{2^n-1}\alpha_x\sum_{x'=1}^{2^n-1}(-1)^{x\cdot x'+x''\cdot x'}\right]|x''\rangle \otimes \sum_{y=0,1}(-1)^y|y\rangle
\end{aligned} \tag{3.3.37}$$

lesz. Itt felhasználtuk, hogy

$$\hat{U}_H|x_i\rangle = 2^{-\frac{1}{2}}(|0\rangle + (-1)^{x_i}|1\rangle) \tag{3.3.38}$$

és

$$\begin{aligned}\hat{U}_H^{\otimes n}|x\rangle &= (\hat{U}_H|x_0\rangle)\otimes(\hat{U}_H|x_1\rangle)\otimes\cdots\otimes(\hat{U}_H|x_n\rangle)\\ &= 2^{-\frac{1}{2}n}(|0\rangle+(-1)^{x_0}|1\rangle)\otimes(|0\rangle+(-1)^{x_1}|1\rangle)\otimes\cdots\otimes(|0\rangle+(-1)^{x_n}|1\rangle)\\ &= 2^{-\frac{1}{2}n}\sum_{x'=0}^{2^n-1}(-1)^{x\cdot x'}|x'\rangle. \qquad (3.3.39)\end{aligned}$$

A (3.3.37) utolsó egyenletének jobb oldalán a szögletes zárójel második tagjában az x'-re végzett összegzés nullát ad, kivéve ha $x = x''$:

$$\begin{aligned}&\hat{D}\sum_{x}^{2^n-1}\alpha_x|x\rangle\otimes\sum_{y=0,1}(-1)^y|y\rangle\\ &\quad=\sum_{x''=0}^{2^n-1}\Big[2^{-n}\sum_{x}^{2^n-1}\alpha_x-2^{-n}\alpha_{x''}\sum_{x'=1}^{2^n-1}\Big]|x''\rangle\otimes\sum_{y=0,1}(-1)^y|y\rangle\\ &\quad=\sum_{x''=0}^{2^n-1}\Big[2^{-n}\sum_{x}^{2^n-1}\alpha_x-\frac{1}{2}\alpha_{x''}\Big]|x''\rangle\otimes\sum_{y=0,1}(-1)^y|y\rangle\\ &\quad=\frac{1}{2}\sum_{x=0}^{2^n-1}\Big[2\langle\alpha\rangle-\alpha_x\Big]|x\rangle\otimes\sum_{y=0,1}(-1)^y|y\rangle,\end{aligned} \qquad (3.3.40)$$

ahol

$$\langle\alpha\rangle = 2^{-\frac{1}{2}n}\sum_{x=0}^{2^n-1}\alpha_x \qquad (3.3.41)$$

jelöli az α_x amplitudók várható értékét.

Mi is történik tehát a várható értékre vonatkozó inverzió következtében? A 3. lépés után minden $\alpha_x = +1$ kivéve x_0 amplitudóját, amelyik -1. A várható érték tehát

$$\langle\alpha\rangle = \frac{(2^n-1)\cdot 1 - 1\cdot 1}{2^n} = 1-\frac{1}{2^{n-1}}. \qquad (3.3.42)$$

Ezért a D inverziót követően az új amplitudók:

$$\begin{aligned}&2\Big(1-\frac{1}{2^{n-1}}\Big)-1 = 1-2^{-n+2}, \qquad \text{ha } x\neq x_0,\\ &2\Big(1-\frac{1}{2^{n-1}}\Big)+1 = 3-2^{-n+2}, \qquad \text{ha } x = x_0.\end{aligned} \qquad (3.3.43)$$

A várható értékre történő inverzió tehát kierősíti a keresett x_0 elemnek megfelelő számolási bázisállapot amplitudóját. Ha a lista sok elemű, azaz $n \gg 1$, akkor az amplitudó kb. 3-szoros abszolút értékűvé válik.

A későbbiek szempontjából nevezzük a 3. és 4. lépés unitér operátorát $\hat{K} = -\hat{P}_s\hat{D}\hat{U}_{f_{x_0}}\hat{P}_s$ operátornak, ahol $\hat{P}_s$ a forráskubitek alterére ortogonálisan vetítő operátor.

5. *lépés:* a 3. és 4. lépés többszöri, mondjuk m-szeri ($m > 1$) megismétlése. Az ismétlések m számának alkalmas megválasztásával el tudjuk érni, hogy annak a $p(x_0)$ valószínűsége, hogy az $|x_f\rangle$ végállapotban megtaláljuk a keresett $|x_0\rangle$ állapotot,

$$p(x_0) = |a(x_0)|^2 > \epsilon, \qquad a(x_0) \equiv \langle x_0|x_f\rangle \tag{3.3.44}$$

nagyobb legyen mint egy tetszőleges előre megadott $0 < \epsilon < 1$ valószínűség, pl. mint $\epsilon = 0,5$. A végállapot itt $|x_f\rangle = \hat{K}^m|x_{in}\rangle$, ahol $|x_{in}\rangle = 2^{-\frac{1}{2}n}\sum_{x=0}^{2^n-1}|x\rangle$.

A Grover-algoritmus optimalizációs lépését az alábbiak szerint elemezhetjük. Vezessük be a *Grover-operátor* fogalmát. Definíció szerint a $\hat{G}$ unitér, a forrásregiszter állapotainak Hilbert-terén ható operátort Grover-operátornak nevezzük, ha legfeljebb 2 különböző sajátértékkel rendelkezik. Nevezzük a $\hat{K}$ unitér operátort *Grover-magnak*, ha 2 különböző Grover-operátor szorzata.

Észrevesszük, hogy a 3.és 4. lépest együttesen leíró operátor is Grover-mag, amelynek általánosítása:

$$\hat{K} = \hat{G}_2\hat{G}_1, \tag{3.3.45}$$

ahol

$$\begin{aligned}
&\hat{G}_1 = \alpha\hat{P}_{x_0} + \beta\hat{Q}_{x_0}, \qquad \hat{P}_{x_0} = |x_0\rangle\langle x_0|, \qquad \hat{P}_{x_0} + \hat{Q}_{x_0} = \hat{1};\\
&\hat{G}_2 = \gamma\hat{\tilde{P}} + \delta\hat{\tilde{Q}}, \qquad \hat{\tilde{P}} = \frac{1}{N}\begin{pmatrix} 1 & \cdots & 1\\ \vdots & & \vdots\\ 1 & \cdots & 1\end{pmatrix} \equiv |k_0\rangle\langle k_0|, \quad \hat{\tilde{P}} + \hat{\tilde{Q}} = \hat{1},
\end{aligned} \tag{3.3.46}$$

ahol

$$|k_0\rangle = N^{-\frac{1}{2}}\begin{pmatrix} 1\\ \vdots\\ 1\end{pmatrix} \tag{3.3.47}$$

és α, β, γ és δ egységnyi abszolút értékű komplex számok.

Valóban, könnyű meggyőződni róla, hogy

$$\alpha = \gamma = -1, \qquad \beta = \delta = +1 \tag{3.3.48}$$

választás esetén

$$\begin{aligned}
\hat{G}_1 &= -\hat{P}_{x_0} + \hat{Q}_{x_0} = 1 - 2\hat{P}_{x_0} \equiv \hat{G}_{x_0},\\
\hat{G}_2 &= -\hat{\tilde{P}} + \hat{\tilde{Q}} = 1 - 2\hat{\tilde{P}} = -\hat{D},
\end{aligned} \tag{3.3.49}$$

úgyhogy $\hat{K} = -\hat{D}\hat{G}_{x_0}$, ami pontosan a korábbi $-\hat{D}\hat{U}_{f_{x_0}}$ operátor ortogonális projekciója a forrásregiszter állapotterére.

Most az ismétlések m számának megválasztásához tekintsük a Grover-magot az $|x_0\rangle$ és a rá merőleges $|x_\perp\rangle = (N-1)^{-\frac{1}{2}}\sum_{x\neq x_0}|x\rangle$ vektorok redukált, 2-dimenziós

terében. Ebben a Grover-operátoroknak 2×2-es mátrixok felelnek meg:

$$\hat{G}_1 = \begin{pmatrix} \langle x_0|\hat{G}_1|x_0\rangle & \langle x_0|\hat{G}_1|x_\perp\rangle \\ \langle x_\perp|\hat{G}_1|x_0\rangle & \langle x_\perp|\hat{G}_1|x_\perp\rangle \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$
$$\hat{G}_2 = \begin{pmatrix} \langle x_0|\hat{G}_2|x_0\rangle & \langle x_0|\hat{G}_2|x_\perp\rangle \\ \langle x_\perp|\hat{G}_2|x_0\rangle & \langle x_\perp|\hat{G}_2|x_\perp\rangle \end{pmatrix} = \begin{pmatrix} \delta & 0 \\ 0 & \gamma \end{pmatrix} + \frac{\gamma-\delta}{N}\begin{pmatrix} 1 & \sqrt{N-1} \\ \sqrt{N-1} & -1 \end{pmatrix}. \tag{3.3.50}$$

Ha most $\alpha = \gamma = -1$, ahogy azt korábban választottuk, akkor

$$\hat{K} = \hat{G}_2\hat{G}_1 = \frac{1}{N}\begin{pmatrix} 1+\delta(1-N) & -\beta(1+\delta)\sqrt{N-1} \\ (1+\delta)\sqrt{N-1} & \beta(1+\delta-N) \end{pmatrix}, \tag{3.3.51}$$

és a kezdeti állapot

$$|x_{in}\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_\perp\rangle. \tag{3.3.52}$$

A $p(x_0)$ valószínűség kiszámolása érdekében a Grover-magot spektrálisan felbontjuk. Legyen a Grover-mag 2 sajátvektora $|\kappa_j\rangle$ az $e^{i\omega_j}$ sajátértékekkel,

$$\hat{K}|\kappa_j\rangle = e^{i\omega_j}|\kappa_j\rangle, \qquad j = 1, 2. \tag{3.3.53}$$

Ekkor a kezdeti állapotból a Grover-mag m-szeri alkalmazása után az $|x_0\rangle$ állapotba történő átmenet amplitudója:

$$\begin{aligned} a(x_0) &= \langle x_0|\hat{K}^m|x_{in}\rangle \\ &= \sum_{j=1}^{2} e^{im\omega_j}\langle x_0|\kappa_j\rangle\langle\kappa_j|x_{in}\rangle \\ &= e^{im\omega_1}\left[\sum_{j=1}^{2}\langle x_0|\kappa_j\rangle\langle\kappa_j|x_{in}\rangle + (e^{im\Delta\omega}-1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{in}\rangle\right] \\ &= e^{im\omega_1}\left[\frac{1}{\sqrt{N}} + (e^{im\Delta\omega}-1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{in}\rangle\right], \end{aligned} \tag{3.3.54}$$

ahol $\Delta\omega = \omega_2 - \omega_1$. A Grover-mag invariánsai:

$$\det\,\hat{K} = \beta\delta, \qquad \mathrm{Tr}\,\hat{K} = -(\beta+\delta) + (1+\beta)(1+\delta)\frac{1}{N}, \tag{3.3.55}$$

úgyhogy a sajátértékek a

$$\begin{aligned} &\det\,(\hat{K} - \zeta\hat{1}) = 0, \\ &\zeta^2 - \zeta\,\mathrm{Tr}\,\hat{K} + \det\,\hat{K} = 0 \end{aligned} \tag{3.3.56}$$

szekuláris egyenletből a másodfokú egyenlet megoldó képletének felhasználásával:

$$\begin{aligned}\zeta_{1,2} = e^{i\omega_{1,2}} &= \frac{1}{2}\ \mathrm{Tr}\ \hat{K} \mp \sqrt{\frac{1}{4}(\ \mathrm{Tr}\ \hat{K})^2 -\ \det\ \hat{K}} \\ &= -\frac{1}{2}(\beta+\delta) + \frac{(1+\beta)(1+\delta)}{2N} \\ &\mp \sqrt{(1+\beta)^2(1+\delta)^2 - 2N(\beta+\delta)(1+\beta)(1+\delta) + N^2(\beta-\delta)^2}.\end{aligned} \tag{3.3.57}$$

A sajátvektorok közül

$$|\kappa_2\rangle = \begin{pmatrix} v_0^{(2)} \\ v_\perp^{(2)} \end{pmatrix} \tag{3.3.58}$$

meghatározására van szükségünk a $p(x_0)$ valószínűség kiszámolásához. Ennek komponensei az alábbi homogén lineáris egyenlet megoldásai:

$$\begin{aligned}\Big[1+\delta - \frac{1}{2}(1+\beta)(1+\delta) + \frac{1}{2}(\beta-\delta)N \\ - \frac{1}{2}\sqrt{N^2(\beta-\delta)^2 - 2N(\beta+\delta)(1+\beta)(1+\delta) + (1+\beta)^2(1+\delta)^2}\Big] v_0^{(2)} \\ = (1+\delta)\beta\sqrt{N-1}\, v_\perp^{(2)}.\end{aligned} \tag{3.3.59}$$

Az egyszerűség kedvéért foglalkozzunk csak a sokelemű lista esetével, amikor $N \gg 1$. A β és δ paraméterek megválasztásának két esetét vizsgáljuk meg:

1. $\underline{\beta > \delta}$: Ekkor a négyzetgyökös kifejezést sorba fejtve:

$$\begin{aligned}\frac{1}{2}N|\beta-\delta|\sqrt{1 - \frac{2(\beta+\delta)(1+\beta)(1+\delta)}{N(\beta-\delta)^2} + \frac{(1+\beta)^2(1+\delta)^2}{N^2(\beta-\delta)^2}} \\ \approx \frac{1}{2}N|\beta-\delta|\Big[1 - \frac{(\beta+\delta)(1+\beta)(1+\delta)}{N(\beta-\delta)^2} + \mathcal{O}(\frac{1}{N^2})\Big],\end{aligned} \tag{3.3.60}$$

adódik, amit behelyettesítve a sajátvektor egyenletébe kapjuk, hogy

$$\begin{aligned}\Big[1+\delta - \frac{1}{2}(1+\beta)(1+\delta) + \frac{1}{2}(\beta-\delta)N \\ - \frac{1}{2}|\beta-\delta|N + \frac{1}{2}\frac{(\beta+\delta)(1+\beta)(1+\delta)}{|\beta-\delta|} + \mathcal{O}(\frac{1}{N})\Big] v_0^{(2)} \\ = (1+\delta)\beta\sqrt{N-1}\, v_\perp^{(2)}.\end{aligned} \tag{3.3.61}$$

Ez azt jelenti, hogy

$$v_0^{(2)} = v_\perp^{(2)}\mathcal{O}(\sqrt{N}), \tag{3.3.62}$$

azaz hogy a sajátvektor transzverzális komponense el van nyomva. Közelítőleg írhatjuk tehát, hogy $|\kappa_2\rangle = |x_0\rangle$. Ekkor viszont

$$a(x_0) \approx e^{im\omega_1}\left[\frac{1}{\sqrt{N}} + (e^{im\Delta\omega} - 1)\frac{1}{\sqrt{N}}\right] = \mathcal{O}(\frac{1}{\sqrt{N}}), \tag{3.3.63}$$

aminek az abszolútérték négyzete sosem éri el a 0,5-et.

2. $\underline{\beta = \delta}$: Az algoritmuson azonban változtathatunk azáltal, ha megváltoztatjuk a Grover-mag spektrumát. Ha megköveteljük, hogy $\beta = \delta$, akkor a $|\kappa_2\rangle$ sajátvektor komponenseire vonatkozó egyenlet

$$\begin{aligned}&\left[1 + \delta - \frac{1}{2}(1+\delta)^2 - \frac{1}{2}\sqrt{(1+\delta)^4 - 4N\delta(1+\delta)^2}\right]v_0^{(2)} \\ &\quad = (1+\delta)\delta\sqrt{N-1}v_\perp^{(2)}\end{aligned} \tag{3.3.64}$$

alakot ölt, ahonnan

$$v_0^{(2)} = \left(i\delta^{\frac{1}{2}} + \mathcal{O}(\frac{1}{\sqrt{N}})\right)v_\perp^{(2)}. \tag{3.3.65}$$

Ilyenkor a sajátvektor komponensei nincsenek egymáshoz képest elnyomva, úgyhogy a sajátvektor normálási tényezője $\mathcal{N} = \mathcal{O}(1)$. Ekkor

$$\begin{aligned}|a(x_0)| &= \left|\left[\frac{1}{\sqrt{N}} + (e^{im\Delta\omega} - 1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{in}\rangle\right]\right| \\ &= \left|\left[\frac{1}{\sqrt{N}} + (e^{im\Delta\omega} - 1)\mathcal{N}^2 i\delta^{\frac{1}{2}}\left(\frac{i\delta^{\frac{1}{2}}}{\sqrt{N}} + \sqrt{\frac{N-1}{N}}\right)\right]\right| \\ &= \mathcal{N}^2\delta^{\frac{1}{2}}\left|e^{im\Delta\omega} - 1\right| + \mathcal{O}(\frac{1}{\sqrt{N}}) \\ &\sim \left|\sin\left(\frac{1}{2}m\Delta\omega\right)\right|.\end{aligned} \tag{3.3.66}$$

Ebből látszik, hogy $\beta = \delta$ esetén találhatunk olyan algoritmusokat, amelyekre a $p(x_0)$ valószínűség maximális. Az a legkisebb $m = M$ ismétlési szám, amelynél a keresett állapotnak az algoritmus végén a megtalálási valószínűsége a legnagyobb,

$$M = \left[\left|\frac{\pi}{\Delta\omega}\right|\right], \tag{3.3.67}$$

ahol a szögletes zárójel egész részt jelöl. A maximum értéke $p(x_0)|_{m=M} \approx 1$. Mivel, az ismert sajátértékek alapján, $\Delta\omega = \omega_2 - \omega_1 = \mathcal{O}(\frac{1}{\sqrt{N}})$, ezért az optimális kereséshez szükséges lépésszám $M = \mathcal{O}(\sqrt{N})$.

Az első kvantumszámítógép, amelyen a Grover-algoritmust sikerült kísérletileg megvalósítani [7], acetonban oldott, C^{13} izotóppal megjelölt kloroform molekulákból

állt. A logikai kapukat NMR-módszerrel működtették. A feladat egy darab elem megkeresése volt egy 4-elemű listában. A lista elemeinek ábrázolásához 4 darab kvantumállapot, azaz egy 2-kubites rendszer szükséges. A 2 kubitet a kloroform molekulában található szén és hidrogén atommmag spinje jelentette. Az algoritmus egyetlen iterációs lépésben megtalálta a keresett elemet.

Amíg a Grover-algoritmus szerkezet nélküli adatbázison hajt végre keresést, addig fontos lehet a gyakorlat számára olyan algoritmusok kidolgozása is, amelyek saját, belső szerkezettel rendelkező adatbázison hajtanak végre keresést. Újabban ilyen kvantumalgoritmus kifejlesztése is folyamatban van [8]. Az ilyen kereső algoritmusok ki tudják használni az adatbázisban eleve meglevő strukturáltságot.

3.3.3 Shor-algoritmus

A Shor-féle algoritmus (1994) [9] nagy egész számok faktorizálására szolgál. Mint ilyen, a kriptográfiában forradalmi változást eredményezhet. Hatékonyságával veszélyezteti ugyanis a jelenleg elfogadottan használatos, korábban ismertetett titkosítási algoritmust. Az utóbbiban a személyes kulcs hozzáférhetetlensége nem elvi alapokon nyugszik, hanem azon a gyakorlati tényen, hogy az ismert klasszikus algoritmusokkal még akkor sem lehet majd elérhető CPU-idők alatt nagy egész számokat faktorizálni, ha a hagymányos számítógépeink el fogják érni a miniatürizálás fizikai határát. A Shor-algoritmus lehetővé teszi elvileg nagy egész számok ,,gyors" faktorizálását[3]. Érdekes módon a kvantummechanika egyszerre ássa alá a kriptográfia azon módszerét, amelynek biztonsága a nagy számok faktorizálásának ,,lassúságán" múlik, és nyit új utat a kvantumkulcsban történő biztonságos megegyezés másféle lehetőségének megteremtésével.

A Shor-algoritmus több mindent épít magába:

1. használja a periodikus függvény fogalmát;
2. kihasználja a kvantum-párhuzamosságot és az átmeneti amplitudók erősítő interferenciáját;
3. használja a kvantum-Fourier-transzformációt;
4. használja a kvantummechanikai mérést;
5. felhasználja a két egész szám legnagyobb közös osztójának megkeresésére vonatkozó klasszikus, Euklidesz-i algoritmust.

Mielőtt rátérhetnénk a Shor-algoritmus tárgyalására, némi számelméleti alapismeret szükséges. Legyen $N \geq 3$ egész szám, amelyet faktorizálni akarunk. Legyen

[3]Az $N > 0$ egész szám faktorizálásán azt értjük, hogy N-et nem-triviális ($\neq 1$ és $\neq N$), természetes számok közé tartozó tényezők szorzatára bontjuk.

$a \in (1, N)$ egész szám, amelyre $\gcd(N, a) = 1$, azaz N és a legnagyobb közös osztója 1, azaz N és a relatív prímszámok. Az a egész szám egész hatványai, a^x ciklikus csoportot[4] alkotnak Z_N-ben[5]. Az a^x tehát periodikus függvény a mod N egész számok csoportjában. Létezik továbbá olyan legkisebb $r \in (1, N)$ egész szám, amelyre $a^r = 1_N$, ahol $1_N = 1 \bmod N$ a Z_N csoport egységeleme. Definíció szerint ekkor r az a szám rendje modulo N. A következő esetek fordulhatnak elő [6]:

1. r páratlan szám;
2. r páros szám és $a^{\frac{r}{2}} \equiv -1 \in Z_N$;
3. r páros szám és $a^{\frac{r}{2}} \not\equiv -1 \in Z_N$.

Egyedül az utóbbi eset érdekes, mert ekkor $\gcd(N, a^{\frac{r}{2}} \pm 1)$ az N egész szám nem-triviális tényezői.

Ha N nem tiszta prímszámnak a hatványa, akkor annak a valószínűsége, hogy az $(1, N)$ intervallumból véletlenszerűen olyan a számot választunk, amely N-hez relatív prím és amely eleget tesz a 3. követelménynek, nagyobb vagy egyenlő mint $\frac{1}{2 \log N}$. Ezért elég $\mathcal{O}(\log(\frac{1}{\epsilon}) \log N)$ darab véletlenszerűen választott a számot megvizsgálni ahhoz, hogy $1-\epsilon$-nál nagyobb valószínűséggel megtaláljuk az N egésznek egy nem triviális osztóját.

Pl.: Ha $N = 21824$, $a = 12084$, akkor $r = 3588$ és $12083^{1794} \equiv 4866 \bmod 21823$, úgyhogy $\gcd(12083^{1794} \mp 1, 21823) = \{139, 157\}$, amelyek nem-triviális osztói $N = 21824$-nek.

A tulajdonképpeni nehéz feladat az a szám r rendjének (mod N) kiszámítása, ha N nagy szám. Erre vállalkozik a Shor-algoritmus [9].

A Shor-algoritmushoz szükség van egy forrásregiszterre, amely K kubitből áll és $Q \equiv 2^K \in (N^2, 2N^2)$ és egy targetregiszterre, amelynek legalább N bázisállapota van, azaz legalább $[\log_2 N]$ kubites. A Shor-algoritmus, melyet sematikusan a 8. ábra szemléltet, a következő lépésekből áll:

1. *lépés:* A forrás- és targetregiszter kezdeti állapotának a beállítása:

$$|\Psi_1\rangle = |0\rangle \otimes |0\rangle. \tag{3.3.68}$$

[4] A ciklikus csoport olyan csoport, amely valamely elemének összes egészkitevős hatványaiból áll.

[5] Z_N azon egész számok halmaza, amelyeket úgy kapunk, hogy vesszük mindazokat a maradékokat, amelyek tetszőleges egész szám modulo N eredményeként előállnak.

[6] Az alábbiakban $a \equiv b \bmod N$ azt jelenti, hogy a kongruens b-vel modulo N, azaz N-nel osztva mind a, mind b ugyanazt a maradékot adja.

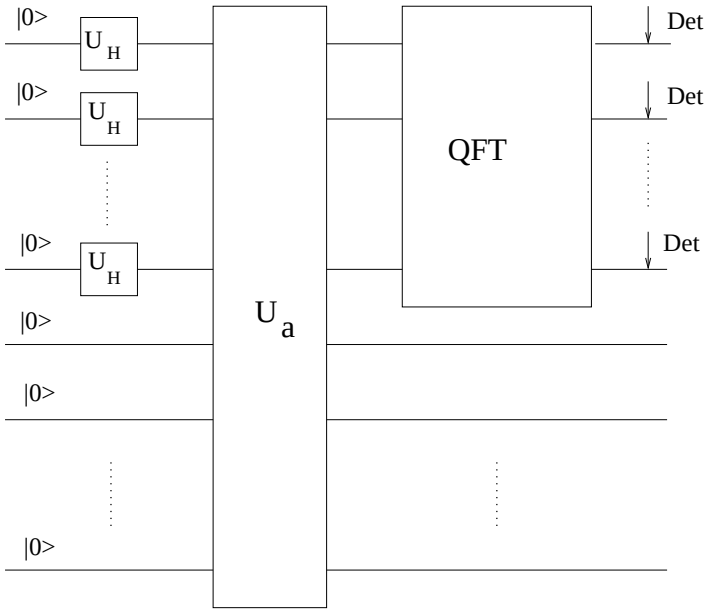

Figure 8: A Shor-algoritmus szemléltetése. A nyilak a megfelelő kubitek állapotát mérő detektorokat (Det) jelölik, az U_a kapu az a alapú moduláris hatványozást, a QFT jelű kapu pedig a kvantum Fourier-transzformációt végzi.

2. *lépés:* A forrásregiszterre a *kvantum-Fourier-transzformációt* alkalmazzuk, ami nem más mint a diszkrét F_Q Fourier-transzformáció Z_Q-ban:

$$\hat{U}_{F_Q}: \qquad |q\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{q'=0}^{Q-1} e^{i2\pi qq'/Q} |q'\rangle. \tag{3.3.69}$$

Itt $q = \sum_{j=0}^{Q-1} q_j 2^j$, $q_j = 0, 1$ és $|q\rangle = |q_{Q-1} \dots q_1 q_0\rangle$. Ennek hatására a következő állapot áll elő:

$$|\Psi_2\rangle = (\hat{U}_{F_Q} \otimes \hat{1})|\Psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0}^{Q-1} |q\rangle \otimes |0\rangle. \tag{3.3.70}$$

A csupa $|0\rangle$ állapotú kubitekből álló forrásregiszterre a kvantum-Fourier-transzformáció ugyanúgy hat, mint a kubitenként külön-külön alkalmazott Hadamard-kapuk (ld. a Deutsch-Józsa-algoritmust).

3. *lépés:* a moduláris hatványozás $\hat{U}_a$ függvényének az alkalmazása:

$$\hat{U}_a: \qquad q \mapsto a^q \bmod N, \tag{3.3.71}$$

azaz

$$|\Psi_3\rangle = \hat{U}_a|\Psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0}^{Q-1} |q\rangle \otimes |a^q \bmod N\rangle. \tag{3.3.72}$$

A kvantumpárhuzamosság abban nyilvánul meg, hogy ez a lépés egyszerre előállítja ($a^q \bmod N$)-et minden q-ra.

4. *lépés:* ismételten alkalmazzuk a kvantum Fourier-transzformációt a forrásregiszterre. Ekkor az alábbi állapotot kapjuk:

$$\begin{aligned}|\Psi_4\rangle &= (\hat{U}_{F_Q} \otimes \hat{1})|\Psi_3\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0}^{Q-1} (\hat{U}_{F_Q}|q\rangle) \otimes |a^q \bmod N\rangle \\ &= \frac{1}{Q} \sum_{q=0}^{Q-1} \sum_{q'=0}^{Q-1} e^{i2\pi qq'/Q} |q'\rangle \otimes |a^q \bmod N\rangle \\ &= \frac{1}{Q} \sum_{q=0}^{Q-1} \sum_{q'=0}^{Q-1} e^{i2\pi qq'/Q} |q\rangle \otimes |a^{q'} \bmod N\rangle. \end{aligned} \tag{3.3.73}$$

5. *lépés:* a forráskubiteket mérjük a számolási bázisban. Az egyszerűség kedvéért mérjük a targetkubiteket is. Annak a prob (q) valószínűsége, hogy a forrásregisztert a $|q\rangle$ állapotban találjuk, a targetregisztert pedig a $|a^k \bmod N\rangle$ állapotban:

$$\begin{aligned}\text{prob}\ (q) &= \left|\langle a^k \bmod N|\langle q|\psi_4\rangle\right|^2 \\ &= \left|\frac{1}{Q} \sum_{q' \in [0,Q-1], a^{q'} \equiv a^k \bmod N} e^{i2\pi qq'/Q}\right|^2. \end{aligned} \tag{3.3.74}$$

Mivel a-nak a rendje modulo N r-rel egyenlő, azért az összegzés azokra a q' egészekre terjed ki, amelyek r-rel osztva k-t adnak maradékul, vagyis amelyek kongruensek k-val modulo r,

$$q' \equiv k \bmod r. \tag{3.3.75}$$

Ezekhez létezik olyan b egész szám, hogy

$$q' = br + k, \qquad b \in [0, B], \tag{3.3.76}$$

ahol $B = \left[\frac{Q-1-k}{r}\right]$ és a (3.3.74) egyenlet jobb oldalán a q'-re vonatkozó összegzés átírható ezen b-kre történő összegzéssé:

$$\begin{aligned}\text{prob}\ (q) &= \left|e^{i2\pi qk/Q}\right|^2 \left|\frac{1}{Q} \sum_{b=0}^{B} e^{i2\pi brq/Q}\right|^2 \\ &= \left|\frac{1}{Q} \sum_{b=0}^{B} e^{i2\pi brq/Q}\right|^2. \end{aligned} \tag{3.3.77}$$

A további lépések, amelyek már nem kvantum-algoritmust igényelnek:

1. Ha megmértük a prob (q) valószínűséget q függvényében, akkor ebből ki kell még olvasni r értékét, azaz a rendjét mod N. Ehhez észrevesszük, hogy a prob (q) valószínűségnek éles maximumai vannak azoknál a q értékeknél, amelyek esetén az (3.3.74) geometriai sor minden tagja a komplex számsík egyazon félsíkján helyezkedik el, vagyis amikor a tagok konstruktív interferenciája valósul meg.

   Vizsgáljuk tehát a (3.3.77) valószínűséget. Legyen rq-nak a Q-val történő osztásból származó maradéka $\{rq\}_Q$, amelyre

$$-\frac{1}{2}Q \geq \{rq\}_Q = rq - q'Q \leq \frac{1}{2}Q \tag{3.3.78}$$

   teljesül valamilyen alkalmas q' egész számmal. A (3.3.77) valószínűséget átírhatjuk

$$\text{prob } (q) = \left|\frac{1}{Q}\sum_{b=0}^{B} e^{i2\pi b\{rq\}_Q/Q}\right|^2 \tag{3.3.79}$$

   alakba. Vegyük azt az esetet, amikor az $\{rq\}_Q$ maradék kicsi. Ekkor az összeg valamennyi tagjának közel azonos a fázisa, azaz erősítő interferencia lép fel. Most megkeressük az erősítő interferencia feltételét.

   Írjuk ehhez kis $\{rq\}_Q$ esetén az (3.3.79) egyenlőség jobb oldalán szereplő összeget integrál alakjába:

$$\frac{1}{Q}\int_0^B dbe^{i2\pi b\{rq\}_Q/Q} + \mathcal{O}(\frac{B}{Q}\Big(e^{i2\pi\{rq\}_Q/Q} - 1\Big)), \tag{3.3.80}$$

   ahol a hibát az $\int_0^1 db$ integrállal becsültük. Ha $|\{rq\}_Q| \leq \frac{1}{2}r$, azaz a maradék kicsi, akkor az integrál hibájában szereplő kerek zárójeles kifejezés nagyságrendje $\frac{r}{2Q}$, úgyhogy az összeg integrállal történő közelítésének a hibája $\leq \mathcal{O}(\frac{1}{Q})$.

   Most megmutatjuk, hogy ha teljesül a

$$|\{qr\}_Q| = |qr \bmod Q| \leq \frac{1}{2}r \tag{3.3.81}$$

   feltétel, akkor erősítő interferencia lép fel, azaz a (3.3.79) valószínűség értéke nagynak adódik. Ekkor tehát nagy lesz annak a valószínűsége, hogy a forrásregisztert a $|q\rangle$ állapotban találjuk, függetlenül a targetregiszter állapotától. Utóbbit azért mondhatjuk, mert a (3.3.81) nem függ k-tól.

   A bizonyításhoz vezessük be az $u = \frac{rb}{Q}$ integrálási változót és írjuk az (3.3.80) integrált

$$I \approx \frac{1}{r}\int_0^{\frac{rB}{Q}} du e^{i2\pi\frac{\{rq\}_Q}{r}u} \tag{3.3.82}$$

   alakba. Mivel $k < r$, csak $\mathcal{O}(\frac{1}{Q})$ hibát követünk el, ha az integrálás felső határát 1-re változtatjuk. Ekkor az

$$I = \frac{1}{r}\int_0^1 du e^{i2\pi\frac{\{rq\}_Q}{r}u} \tag{3.3.83}$$

integrált kell vizsgálnunk $|\{rq\}_Q| \leq \frac{1}{2}r$ esetén. Nyilvánvaló, hogy az integrál abszolút értéke $\{rq\}_Q = \pm\frac{1}{2}r$ esetén minimális, ekkor $|I|_{\min} = \frac{2}{\pi r}$és a megfelelő valószínűség $\text{prob}(q) \geq \frac{4}{\pi^2 r^2} > \frac{1}{3r^2}$. A (3.3.81) feltétel teljesülése esetén tehát az erősítő interferencia miatt a keresett $\text{prob}(q)$ valószínűség meghalad egy alsó korlátot.

Belátható, hogy a konstruktív interferencia feltétele az, hogy minden $q > 0$ egész számhoz létezik olyan $q' \in (0, r)$, hogy

$$\left|\left(\frac{q}{Q}\right) - \left(\frac{q'}{r}\right)\right| \leq \frac{1}{2Q}. \tag{3.3.84}$$

Miután (3.3.81) érvényes, létezik olyan q', hogy

$$\begin{aligned} |qr - q'Q| &\leq \frac{1}{2}r, \\ \left|q - \frac{q'Q}{r}\right| &\leq \frac{1}{2}, \\ \left|\frac{q}{Q} - \frac{q'}{r}\right| &\leq \frac{1}{2Q}. \end{aligned} \tag{3.3.85}$$

A következő lépés az, hogy az erősítő interferencia (3.3.81) feltételéből meghatározzuk r értékét. Kiindulunk egy olyan q értékből (olyan q értékekből), amely(ek)re a $\text{prob}(q)$ valószínűség éles maximummal rendelkezik. A (3.3.81) azt jelenti, hogy létezik olyan q' egész szám, hogy

$$-\frac{1}{2}r \leq rq - q'Q \leq \frac{1}{2}r, \tag{3.3.86}$$

azaz

$$-\frac{1}{2Q} \leq \frac{q}{Q} - \frac{q'}{r} \leq \frac{1}{2Q}. \tag{3.3.87}$$

Miután $Q > N^2$ és $r < N$, létezik olyan egyértelműen meghatározott q', amellyel képzett $\frac{q'}{r}$ hányadosra az egyenlőtlenség kielégül. Utóbbi azt jelenti, hogy a konstruktív interferencia, azaz a $\text{prob}\,(q)$ valószínűség éles maximumai $q = \left[\frac{q'Q}{r}\right]$ egészek közelében vannak, ahol q' is egész. A $\frac{q'}{r}$ racionális számokat úgy határozhatjuk meg, hogy az adott $\frac{q}{Q}$ törtet kerekítjük a hozzá legközelebb eső olyan törtre, amelynek nevezője kisebb mint N. Ez numerikusan a $\frac{q}{Q}$ emeletes törtkifejtése[7] alapján tehető meg. Ha az így talált $\frac{q'}{r}$ a $\frac{q_1}{r_1}$

[7]
$$\frac{q}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{3.3.88}$$

irreducibilis tört, akkor előfordulhat, hogy $a^{r_1} = 1 \bmod N$, akkor tudjuk, hogy $r = r_1$ és befejeződött r keresése. Más esetekben csak annyit tudtunk meg, hogy r_1 az r-nek osztója. Ekkor tovább keresünk egy másik, a konstruktív interferenciához tartozó q értéket, stb. Meg lehet mutatni, hogy $\mathcal{O}(\frac{1}{\log\log r})$ annak a valószínűsége, hogy megfelelő q értéket választunk. Ez azt jelenti, hogy általában $\mathcal{O}(\log\log N)$ választási kísérlet után nagy valószínűséggel rátalálunk r-re.

2. Végül r ismeretében meg kell keresni N osztóit a legnagyobb közös osztó megkeresésére szolgáló Euklidesz-i algoritmus[8] segítségével.

Példák:

1. $N = 15$ faktorizálása. Válasszuk $a = 7$-et. Ilyenkor közvetlenül is meggyőződhetünk róla, hogy $r = 4$:

$$\begin{array}{lll} 7 & \equiv 7 \bmod 15 & = 7 \\ 7^2 & \equiv 49 \bmod 15 & = 4 \\ 7^3 & \equiv 343 \bmod 15 & = 13 \\ 7^4 & \equiv 2401 \bmod 15 & = 1 \\ 7^5 & \equiv 7 \bmod 15 & = 7 \\ 7^6 & \equiv 7^2 \bmod 15 & = 4 \\ \vdots & \vdots & \vdots \end{array} \tag{3.3.89}$$

Másrészről $N^2 = 15^2 = 225$, $2N^2 = 450$, úgyhogy $Q = 2^K \in (225, 450)$ megoldása $K = 8$ és $Q = 256$. Ekkor $B = [(255 - k)/4] = 63$, ha $k = 0, 1, 2, 3$, úgyhogy pl. $q = 0$, 64, 128, 192 esetén $\text{prob}(q = 0) = 0,25$. A megfelelő $\frac{q}{Q}$ racionális számokra:

$$\frac{0}{256}, \quad \frac{64}{256} = 0 + \frac{1}{4}, \quad \frac{128}{256} = 0 + \frac{1}{2}, \quad \frac{192}{256} = 0 + \frac{1}{1 + \frac{1}{3}} = \frac{3}{4}, \tag{3.3.90}$$

úgyhogy az emeletes törtkifejtés konvergensei $(\frac{q'}{r})$ rendre $\frac{1}{4}$, $\frac{2}{4}$, $\frac{3}{4}$. Ezek pontosabban közelítik $\frac{q}{Q}$-t mint $\frac{1}{2Q}$. Az első számot, amely nulla és nem alkalmas az r rend meghatározására, elhagytuk. A konvergensekből látszik, hogy 4 osztója r-nek, tehát r lehetséges értékei 4, 8, 12, stb. Közvetlen ellenőrzéssel kapjuk, hogy $r = 4$. Tehát $r = 4$ a 7 rendje modulo 15.

Mivel $7^{\frac{4}{2}} \not\equiv -1 \bmod 15$, azért $\gcd(49 \pm 1, 15) = \{5, 3\}$, s így 15 tényezői 5 és 3.

[8]Ez az algoritmus azon az észrevételen alapul, hogy ha $a = bq + r$, akkor $\gcd(a, b) = \gcd(b, r)$, ahol a, b, q, r nem negatív egész számok. Ilyen módon bármely két $a > b$ szám legnagyobb közös osztójának megkeresése visszavezethető két kisebb szám legnagyobb közös osztójának megkeresésére, $a = b \cdot 1 + b'$ esetén $\gcd(a, b) = \gcd(b, b')$, ahol $b > b'$, majd $b = b' \cdot 1 + b''$ miatt $\gcd(b, b') = \gcd(b', b'')$, stb. A maradékok a fenti eljárásnál egyre kisebb nem-negatív számok. Az eljárás tehát véges sok lépésben befejeződik. A legnagyobb közös osztót az utolsó nullától különböző maradék adja.

2. Legyen $N = 25397$ és $a = 71$. Ekkor $Q = 2^{30} = 1\ 073\ 741\ 824$. Sok olyan q értéket találunk, amelyekre prob (q) jelentős és közel azonos érték. Egyikük pl. $q = 6\ 170\ 930$, amelyre prob $(q) \approx 2 \cdot 10^{-3}$. Az $\frac{1}{174}$ konvergens az egyetlen olyan közelítése $\frac{q}{Q}$-nak, amelynek a nevezője kisebb mint N és ez az alábbi emeletes törtkifejtést szolgáltatja: $\{a_0, a_1, \ldots\} = \{0, 174, 1\ 542\ 732, 2\}$. Ezért 71-nek a rendje modulo $N = 25397$ olyan r egész, amely 174-nek többszöröse. Közvetlen ellenőrzés mutatja, hogy $r = 522$.

   Mivel $a^{\frac{1}{2}r} \not\equiv -1 \bmod N$, azért gcd $(71^{261} \pm 1, 25397) = \{109, 233\}$ az $N = 25397$ osztói.

Ha feltételezünk egy hipotetikus kvantumszámítógépet 100 MHz frekvenciával, akkor a Shor-algoritmus látványos hatékonyságát az mutatja, hogy egy kb. 40000 számjegyű egész szám tényezőkre bontása kb. 20 évet venne csak igénybe. Ezt kell egybevetni a klasszikus számológépekkel a miniatürizálási határon elérhető 10^{10} CPU-év nagyságrenddel. Általában az algoritmus becsült ,,költsége" $\mathcal{O}(\log_2^3 N)$.

Az algoritmus technikai megvalósítása szempontjából fontos, hogy a kvantum-Fourier transzformációt megvalósító kaput fel lehet építeni ismert kapuk egymás utáni alkalmazásával, mint billentő-kapu, Hadamard-kapu és feltételes fázis-kapu.

2001 decemberében az IBM Almadenben lévő kutatóközpontjában sikerült kvantumszámítógép segítségével a 15-öt nem-triviális tényezőire, $15 = 3 \cdot 5$ alakban felbontani (ld. [2]-t és az abban megadott irodalmat). A kvantumszámítógép 7-kubites molekulákból áll. Ezt a molekulát külön erre a célra tervezték és hozták létre kémiai úton. Benne 2 darab szénatom és 5 darab fluoratom magspinje hat kubitenként egymással kölcsön. A kvantumlogikai kapukat külső mágneses térrel, meghatározott ideig történő kölcsönhatással valósították meg. A külső mágneses tér homogén és rádiofrekvenciás komponenst tartalmazott. A molekulák ezekkel a rádiofrekvenciás impulzusokkal ,,programozhatók". A programozás azt jelenti, hogy meghatározott ütemben egymás utáni meghatározott sorrendben logikai kapuk (a külső tértől és annak impulzushosszától függő unitér időfejlesztő operátorok) hatnak a kb. 10^{18} darab, független molekulából álló rendszerre. A logikai kapuk meghatározott sorrendje éppen úgy lett választva, hogy a Shor-algoritmust valósítsa meg.

References

[1] N. Gershenfeld, I.L. Chuang, Sci. Am. (1998, June, pp. 50-55)

[2] Papp Gy., Természettudományi Közlöny, 2003, 134. évf., 3. füzet, 103-106.

[3] A. Galindo, M.A. Martín-Delgado, Rev. Mod. Phys. 2002.; quant-ph/0112105

[4] 'Entanglement bridges the Danube', http://physicsweb.org/article/news/7/6/20

[5] 'Cryptography breaks 100 km barrier', http://physicsweb.org/article/news/7/6/6

[6] C. Elliott, D. Pearson, G. Troxel, 'Quantum Cryptography in Practice', quant-ph/0307049

[7] I.L. Chuang, N. Gershenfeld, M. Kubinec, Phys.Rev. Lett. **80** (1998) 3408.

[8] H. Zaraket, V. Bagnulo, J. Kettner, R. Kobes, G. Kunstatter, 'A new adiabatic quantum search algorithm', quant-ph/0308060

[9] P.W. Shor, 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', quant-ph/9508027.

[10] B. Georgeot, 'Quantum Computing of Poincaré Recurrences and Periodic Orbits', quant-ph/0307233