Kvantumszámítás

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

1 Bevezetés

A kvantumszámítás egy izgalmas és gyorsan fejlődő kutatási terület. Egyre nő azoknak a kutatóknak a száma, akik érdeklődést mutatnak a téma iránt. A fizikusoktól kezdődően, az informatikusok, matematikusok, de még a filozófia művelői is bekapcsolódnak a kvantum alapú számítás tanulmányozásába.

Eddigi eredmények. Már megalkottak egy 7 qbites kvantum számítógépet amely kiszámította a 15 szám prímtényezős felbontását. Nemrégen egy 16 qbites gépet hoztak létre. Becslések szerint hatékony gyakorlati alkalmazáshoz legalább 3000 qbit és 128 kvantum kapu megvalósítására van szükség.

Az első előadáson az alapfogalmakat (Hilbert tér, qbit, kvantum kapu, kvantumszámítógép) tekintjük át.

A második előadáson Shornak a természetes számok prímtényezős felbontását kiszámító algoritmusát tanulmányozzuk.

A vektortér

A $(G, \cdot, e)$ rendszert csoportnak nevezzük, ahol G halmaz, a $\cdot$ bináris G feletti művelet. $\cdot$ -ot szorzásnak nevezzük. A $\cdot$ szorzás műveletre teljesül az alábbi három feltétel:

1. $\cdot$ asszociatív.

2. $e \in G$ egységeleme G-nek: minden $a \in G$ esetén: $a \cdot e = e \cdot a = a$.

3. Minden $a \in G$ esetén: létezik egy $a^{-1} \in G$ úgy hogy $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Ha $\cdot$ kommutatív, azaz minden $a, b \in G$ esetén, $a \cdot b = b \cdot a$ akkor G Ábel (kommutatív) csoport.

Az $(F, +, 0, \cdot, 1)$ rendszert testnek nevezzük ahol F halmaz, $+$ és $\cdot$ két változós művelek. $+$-t összeadásnak, $\cdot$-t szorzásnak nevezzük. Továbbá teljesülnek az alábbi feltételek:

1. $(F, +, 0)$ Ábel csoport.

2. $(F - \{\, 0 \,\}, \cdot 1)$ Ábel csoport. $0 \neq 1$.

3. a szorzás disztributív az összeadásra: $a \cdot (b + c) = a \cdot b + a \cdot c$.

$\mathcal{A}$ vektor tér három összetevőből áll:

1. $(V, +)$ Ábel csoport. V elemeit vektoroknak nevezzük.

2. $(F, +, 0, \cdot, 1)$ test. F a valós számok halmaza vagy a komplex számok halmaza. F elemét skalárnak nevezzük.

3. $\cdot$ művelet, a skalárral való szorzás művelete. Minden $c \in F$ és $\alpha \in V$ esetén, $c \cdot \alpha \in V$.

Minden $\alpha, \beta \in V$, $c, c' \in F$ esetén,

$c \cdot (\alpha + \beta) = c \cdot \alpha + c \cdot \beta$,

$(c + c') \cdot \alpha = c \cdot \alpha + c' \cdot \alpha$,

$(c \cdot c') \cdot \alpha = c \cdot (c' \cdot \alpha)$,

$1 \cdot \alpha = \alpha$.

$\mathbf{C}$ a komplex számok testét jelöli.

Legyen $n \geq 1$. Az $\{ \alpha_1, \ldots, \alpha_m \}$ vektorhalmaz lineárisan független ha minden $c_1, \ldots, c_n \in F$ esetén,
ha $c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = \mathbf{0}$
akkor $c_1 = c_2 = \cdots = c_n = 0$.
Ha $\{ \alpha_1, \ldots, \alpha_m \} \in \mathbf{C}^n$ vektorhalmaz nem lineárisan független, akkor az $\{ \alpha_1, \ldots, \alpha_m \}$ vektorhalmazt lineárisan függőnek nevezzük.

Tetszőleges $\mathcal{A}$-beli U vektorhalmaz összes lineáris kombinációinak H halmaza $\mathcal{A}$ (a $\subseteq$ relációra nézve) legszűkebb olyan résztere amely tartalmazza U-t. Azt mondjuk hogy U kifeszíti a H részteret. Ha U lineárisan független vektorhalmaz kifeszíti az egész $\mathcal{A}$ teret, akkor azt mondjuk hogy U az $\mathcal{A}$-nak egy bázisa. Azt mondjuk hogy $\mathcal{A}$ véges dimenziós ha van $\mathcal{A}$-nak véges bázisa.

Állítás 1.1 *Ha* $\{ b_1, b_2, \ldots, b_m \}$ *és* $\{ c_1, c_2, \ldots, c_n \}$ *bázisai az* $\mathcal{A}$ *vektortérnak, akkor* $m = n$.

Legyen $\mathcal{A}$ egy véges dimenziós vektortér. $\mathcal{A}$ tetszőleges bázisának az elemszámát $\mathcal{A}$ dimenziójának nevezzük és $dim(\mathcal{A})$-val jelöljük. Például az $\mathbf{R}^3$ vektorteret (kifeszíti a $\{ (1,0,0), (0,1,0), (0,0,1) \}$ lineárisan független vektorhalmaz. Ez a halmaz bázisa az $\mathbf{R}^3$ vektortérnak. Tehát $dim(\mathbf{R}^3) = 3$.

Legyenek $V_\mathcal{A}$ és $V_\mathcal{B}$ vektorterek ugyanazon F test felett. Az $A : V_\mathcal{A} \to V_\mathcal{B}$ leképezést lineárisnak nevezzük ha teljesül hogy $A(\alpha + \beta) = A(\alpha) + A(\beta)$ és $A(c\alpha) = cA(\alpha)$.

Definíció 1.2 *Legyen* $V_\mathcal{A}$ *egy vektortér. Az* $A : V_\mathcal{A} \to V_\mathcal{A}$ *lineáris leképezést operátornak nevezzük.*

Az n-dimenziós komplex vektortér

Definíció 1.3 *Az n-dimenziós komplex vektortér fogalma.*

$V = \mathbf{C}^n$. *Azaz n hosszú vektorokat tekintünk, amelyek komponensei komplex számok.*

$F = C$.

Minden $\alpha, \beta \in \mathbf{C}^n$ *vektorhoz hozzárendelünk egy* (α, β) *komplex számot úgy hogy az alábbi hat feltétel teljesül:*

1. $(\alpha, \beta) = (\beta, \alpha)^*$,
2. $(c\alpha, \beta) = c^*(\alpha, \beta)$,
3. $(\alpha + \gamma, \beta) = (\alpha, \beta) + (\gamma, \beta)$,
4. $(\alpha, c\beta) = c(\alpha, \beta)$,
5. $(\alpha, \beta + \gamma) = (\alpha, \beta) + (\alpha, \gamma)$,
6. $(\alpha, \alpha) \geq 0$ *és* $(\alpha, \alpha) = 0$ *akkor és csak akkor ha* $\alpha = 0$.

Azt mondjuk hogy (α, β) *az* α *és* β *vektorok belső szorzata.*

Itt a $c = a + ib$ komplex szám konjugáltja a $c^* = a - ib$ szám.

Az α, β vektorok által bezárt szög a θ valós szám:

$$\theta = arccos \frac{(\alpha, \beta)}{\|\alpha\| \|\beta\|} \ .$$

Ebből következik hogy

$$cos\theta = \frac{(\alpha, \beta)}{\|\alpha\| \|\beta\|} \ .$$

Az α vektor hossza (normája) $\|\alpha\| = \sqrt{(\alpha, \alpha)}$. A normára teljesül hogy

minden α vektor esetén, $\|\alpha\| \geq 0$,

minden α, β vektor esetén, $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$,

minden $c \in \mathbf{C}$ és α vektor esetén, $c \cdot \|\alpha\| = |c| \cdot \|\alpha\|$, és

minden α vektor esetén, $\|\alpha\| = 0$ akkor és csak akkor ha $\alpha = \mathbf{0}$.

Legyen $\alpha \neq \mathbf{0}$ és $\beta \neq \mathbf{0}$. Ha $(\alpha, \beta) = 0$, akkor $cos(\theta) = 0$. Tehát $\theta = \frac{\pi}{2}$. Azt mondjuk hogy α és β merőlegesek (ortogonálisak) ha $(\alpha, \beta) = 0$.

Állítás 1.4 *Az n-dimenziós komplex vektortérben ha az*
$\{ e_1, \ldots, e_n \}$
vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{ e_1, \ldots, e_n \}$ *bázist alkot.*

Az n-dimenziós komplex vektortérben ha az $\{ e_1, \ldots, e_n \}$ vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{ e_1, \ldots, e_n \}$ vektorhalmazt ortogonális bázisnak nevezzük. Ha még az is teljesül hogy minden vektor hossza 1, akkor $\{ e_1, \ldots, e_n \}$ vektorhalmazt ortonormális bázisnak nevezzük. Az $\{ e_1, \ldots, e_n \}$ ortonormális bázisra teljesül hogy $(e_i, e_j) = 0$ ha $i \neq j$ és $(e_i, e_j) = 1$ ha $i = j$. Azaz $(e_i, e_j) = \delta_{i,j}$, ahol $\delta_{i,j}$ a Kronecker delta függvény.

Állítás 1.5 *Az n-dimenziós komplex vektortérnek van ortogonális bázisa.*

Az n dimenziós Hilbert tér

Definíció 1.6 *Az n dimenziós $\mathcal{H}_n$ Hilbert tér: a komplex számok feletti n dimenziós vektortér belső szorzattal és a belső szorzat által származtatott normával.*

Állítás 1.7 *Tetszőleges n dimenziós $\mathcal{H}_n$ Hilbert térnek létezik egy ortonormális bázisa.*

Vegyünk egy tetszőleges ortonormális bázist. Az ortonormális bázis elemeit írhatjuk ket vektorokként:

$\{ |0\rangle, |1\rangle, \cdots, |i\rangle, \cdots, |n-1\rangle \}$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$|i\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$\dots$

$$|n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Az ortonormális bázis elemeit írhatjuk bra vektorokként:

$\{ \langle 0|, \langle 1|, \cdots, \langle i|, \cdots, \langle n-1| \}$.

$\langle 0| = (1\ 0\ \dots\ 0\ \dots\ 0)$, $\langle 1| = (0\ 1\ \dots\ 0\ \dots\ 0)$, $\dots$, $\langle i| = (0\ 0\ \dots\ 1\ \dots\ 0)$, $\dots$, $\langle n-1| = (0\ 0\ \dots\ 0\ \dots\ 1)$.

Vegyük észre hogy $\langle i| = |i\rangle^T$, $1 \leq i \leq n$.

Tetszőleges $|\psi\rangle$ ket vektor előáll az ortonormális bázis ket vektorainak a lineáris kombinációjaként.

$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_i|i\rangle + \cdots + \alpha_{n-1}|n-1\rangle$,
ahol $\alpha_1, \dots, \alpha_i, \dots, \alpha_{n-1} \in \mathbf{C}$.

Definíció 1.8 *M mátrix $M^\dagger$ adjungáltját úgy definiáljuk hogy az M transzponáltjában minden elemnek vesszük a konjugáltját.*

Minden $|\psi\rangle$ ket vektornak a duálisa a $\langle\psi|$ bra vektor.

$|\psi\rangle = (\langle\psi|)^\dagger$ és $\langle\psi| = (|\psi\rangle)^\dagger$.

$\langle\psi| = \alpha_0^*\langle 0| + \alpha_1^*\langle 1| + \cdots + \alpha_i^*\langle i| + \cdots + \alpha_{n-1}^*\langle n-1|$.

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_i \\ \vdots \\ \alpha_{n-1} \end{pmatrix}$$

$\langle\psi| = (\alpha_0^*\alpha_1^*\cdots\alpha_i^*\cdots\alpha_{n-1}^*)$.

A $|\psi_a\rangle, |\psi_b\rangle$ vektorok belső szorzatát $\langle\psi_a|\psi_b\rangle$ jelöli.

Példák: Legyen $|\psi_a\rangle, |\psi_b\rangle \in \mathcal{H}_4$. Ekkor

$|\psi_a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$

$|\psi_b\rangle = \beta_0|0\rangle + \beta_1|1\rangle + \beta_2|2\rangle + \beta_3|3\rangle$

$$\langle\psi_a|\psi_b\rangle = (\alpha_0^*\ \alpha_1^*\ \alpha_2^*\ \alpha_3^*)\begin{pmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\end{pmatrix} = \alpha_0^*\beta_0 + \alpha_1^*\beta_1 + \alpha_2^*\beta_2 + \alpha_3^*\beta_3$$

Így $\langle\psi_a|\psi_a\rangle = \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 + \alpha_2^*\alpha_2 + \alpha_3^*\alpha_3$

$= |\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2$.

Legyen

$|\psi_a\rangle = (1+i)|0\rangle + (2-3i)|1\rangle$

$|\psi_b\rangle = (1-2i)|0\rangle + (3+2i)|1\rangle$

Ekkor $\langle\psi_a|\psi_b\rangle = (1+i)^*(1-2i) + (2-3i)^*(3+2i) = (1-i)(1-2i) + (2+3i)(3+2i) = -1+10i$.

Definíció 1.9 *Legyen $|\psi_a\rangle$ és $|\psi_b\rangle$ két vektor a $\mathcal{H}_n$ Hilbert térben. Azt mondjuk hogy $|\psi_a\rangle$ és $|\psi_b\rangle$ merőlegesek egymásra (azaz ortogonálisak) ha a belső szorzatuk* 0.

Az $f : \mathcal{H}_n \to \mathcal{H}_n$ leképezést lineárisnak nevezzük ha teljesül hogy $f(|\psi_a\rangle + |\psi_b\rangle) = f(|\psi_a\rangle) + f(|\psi_b\rangle)$ és $f(c|\psi_a\rangle) = cf(|\psi_a\rangle)$.

Definíció 1.10 *Az $f : \mathcal{H}_n \to \mathcal{H}_n$ lineáris leképezést operátornak nevezzük.*

Az $\mathbf{U}$ operátornak megfeleltetünk egy U mátrixot úgy hogy az $\mathbf{U}$ operátor végrehajtása egy $|\psi_a\rangle$ ket vektoron megfelel az U mátrixszal való szorzásnak:

$\mathbf{U}(|\psi_a\rangle) = U|\psi_a\rangle$.

U mátrixot meg tudjuk konstruálni ha ismerjük $\mathbf{U}$ értékeit a bázisvektorokon. Az operátort azonosítjuk a mátrixával. Így van értelme az $\mathbf{U}$ operátor $\mathbf{U}^\dagger$ adjungáltjának is.

Tenzor és külső szorzat

Definíció 1.11 *A $\mathcal{H}_n$ és $\mathcal{H}_m$ Hilbert terek tenzor szorzata a $\mathcal{H}_{nm}$ Hilbert tér. Azaz, $\mathcal{H}_n \otimes \mathcal{H}_m = \mathcal{H}_{nm}$. Itt $\otimes$ a tenzor szorzat jele.*

Az A $m \times n$-es mátrix és a B $p \times q$-es mátrix $A \otimes B$ tenzor szorzata az alábbi módon definiált.

Definíció 1.12 *Legyen* $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1q} \\ b_{21} & b_{22} & \dots & b_{2q} \\ \vdots & \vdots & \dots & \vdots \\ b_{p1} & b_{p2} & \dots & b_{pq} \end{pmatrix}$$

Ekkor

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \dots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

Minden $1 \leq i \leq n$, $1 \leq j \leq m$ esetén $a_{ij}B$ egy rész mátrix amelyet úgy kapunk a B mátrixból hogy B minden elemét megszorozzuk a_{ij}-vel. Így az $A \otimes B$ mátrix egy $mp \times nq$-es mátrix.

Például az $\begin{pmatrix} a \\ b \end{pmatrix}$ és $\begin{pmatrix} c \\ d \end{pmatrix}$ vektorok tenzor szorzata az

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \text{ vektor.}$$

Így a $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ és a $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

vektorok tenzor szorzata a $|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ vektor.

Egy $\mathcal{H}_p$-beli vektor és egy $\mathcal{H}_q$-beli vektor tenzor szorzata egy $\mathcal{H}_{pq}$-beli vektor. Az előző példában két $\mathcal{H}_2$-beli vektor tenzor szorzata egy $\mathcal{H}_4$-beli vektor.
Egy $m \times 1$ mátrix (ket vektor) és egy $1 \times n$-es mátrix (bra vektor) tenzor szorzataként kapott $m \times n$ mátrixot a két vektor külső szorzatának hívjuk. Például tekintsük a

$$|\psi_a\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

és

$$|\psi_b\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

ket vektorokat. A $|\psi_a\rangle$ ket vektor és $\langle\psi_a|$ bra vektor $|\psi_a\rangle\langle\psi_b|$ külső szorzatára teljesül hogy

$$|\psi_a\rangle\langle\psi_b| = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} (\beta_0^* \ \beta_1^* \ \beta_2^* \ \beta_3^*) = \begin{pmatrix} \alpha_0\beta_0^* & \alpha_0\beta_1^* & \alpha_0\beta_2^* & \alpha_0\beta_3 \\ \alpha_1\beta_0^* & \alpha_1\beta_1^* & \alpha_1\beta_2^* & \alpha_1\beta_3 \\ \alpha_2\beta_0^* & \alpha_2\beta_1^* & \alpha_2\beta_2^* & \alpha_2\beta_3 \\ \alpha_3\beta_0^* & \alpha_3\beta_1^* & \alpha_3\beta_2^* & \alpha_3\beta_3 \end{pmatrix}$$

Kvantum állapotok

Az állapot egy kvantum fizikai rendszer teljes leírása. A kvantum állapotot egy olyan $\mathcal{H}_n$ Hilbert térbeli vektorral ábrázoljuk aminek a normája 1.

$|\psi_a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_i|i\rangle + \cdots \alpha_{n-1}|n-1\rangle$.

Tekintsük a $|\psi_a\rangle$ és $|\psi_{a'}\rangle$ ket vektorokat amelyekre teljesül hogy $|\psi_a\rangle = c|\psi_{a'}\rangle$ és c komplex szám abszolút értéke 1. Azt mondjuk hogy $|\psi_a\rangle$ és $|\psi_{a'}\rangle$ ugyanazt az állapotot ábrázolják. A zéró vektor nem ábrázolja a kvantum fizikai rendszer egyetlen állapotát sem. A hagyományokat követve feltesszük hogy a $|\psi_a\rangle$ állapotvektorra $\langle\psi_a|\psi_a\rangle = 1$. Ezért

$\Sigma_{i=0}^{n-1} |\alpha_i|^2 = 1$.

A $|\psi_a\rangle$ és $|\psi_b\rangle$ állapot vektorok belső szorzata a két állapot által bezárt általánosított szöget ábrázolja. A $\langle\psi_a|\psi_b\rangle = 0$ egyenlőséget úgy értelmezzük hogy $|\psi_a\rangle$ és $|\psi_b\rangle$ egymásra merőleges (ortogonális) állapotokat reprezentálják.

A kvantum fizikai változó

A fizikai rendszer mérhető tulajdonságát fizikai változónak nevezzük. A kvantum fizika formalizmusa a kvantum fizikai változót egy önadjungált (más szóval Hermite-féle) operátorral írja le. A fizikai változó megmérésekor az operátor valamely sajátértékét kapjuk eredményül.

Definíció 1.13 *Az* $\mathbf{U}$ *operátor a* $\mathcal{H}_n$ *Hilbert térben*
Hermite-féle (önadjungált) ha $\mathbf{U} = \mathbf{U}^\dagger$
unitér ha $\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$

Az $\mathbf{U}$ unitér operátor $\mathcal{H}_n$-beli állapot vektorokhoz $\mathcal{H}_n$-beli állapot vektorokat rendel hozzá. Ezt az alábbi két egyenlőséggel írjuk le.
$|\psi_b\rangle = \mathbf{U}|\psi_a\rangle$
$\langle\psi_b| = \langle\psi_a|\mathbf{U}$.

Definíció 1.14 *Tekintsük a* $\mathcal{H}_n$ *Hilbert teret. A fizikai változó egy olyan Hermite-féle operátor amelynek a sajátvektorai bázist alkotnak.*

Állítás 1.15 *1. A fizikai változó sajátértékei valós számok.*
2. A fizikai változó két különböző sajátértékéhez tartozó sajátvektora merőleges egymásra.
3. A fizikai változó sajátvektorai ortonormális bázist alkotnak $\mathcal{H}_n$*-ben.*

A fentieket újra megfogalmazzuk.

Állítás 1.16 *A* $\mathcal{H}_n$ *Hilbert térben minden* $\mathbf{U}$ *fizikai változónak van* n *sajátvektora:* $|n_i\rangle$, $0 \leq i \leq n-1$. *Továbbá*
$\{\, |n_0\rangle, |n_1\rangle, \ldots, |n_i\rangle, \ldots, |n_{n-1}\rangle \,\}$
egy ortonormális bázis $\mathcal{H}_n$*-ben. Az* $|n_i\rangle$ *sajátvektorhoz tartozik a* λ_i *sajátérték valós szám,* $0 \leq i \leq n-1$. $U|n_i\rangle = \lambda_i|n_i\rangle$.

A kvantum fizikai változó megmérése

A fizikai rendszer mérhető tulajdonságát fizikai változónak nevezzük. A kvantum fizika formalizmusa az $\mathcal{U}$ kvantum fizikai változót az $\mathbf{U}$ önadjungált (más szóval Hermite-féle) operátorral írja le. Az $\mathcal{U}$ fizikai változó megmérésekor az $\mathbf{U}$ operátor valamely λ_i sajátértéket

kapjuk eredményül. A fizikai változók megmérése után azonnal a kvantum állapot **U**-nak az $|u_i\rangle$ sajátvektora és a megmért érték a λ_i sajátérték.

A qbit fogalma és fizikai megvalósítása

A kvantum bit (röviden qbit) egy vektor a két dimenziós Hilbert térben. Ebben a vektortérben a $|\psi\rangle$ vektort

$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

alakban írjuk fel, ahol α_0, α_1 komplex számok $|\alpha_0|^2 + |\alpha_1|^2 = \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 = 1$ és a $|0\rangle$, $|1\rangle$ vektorok ortonormális bázist alkotnak a $\mathcal{H}_2$ térben. Azt mondjuk hogy ψ a $|0\rangle$, $|1\rangle$ bázis vektorok lineáris kombinációja. Amikor megmérünk egy qbitet akkor a $|0\rangle$ eredményt kapjuk $|\alpha_0|^2$ valószínűséggel és az $|1\rangle$ eredményt kapjuk $|\alpha_1|^2$ valószínűséggel.

A qbit a $|0\rangle$ és $|1\rangle$ között végtelen sok állapotben lehet, amíg meg nem mérjük. Például a qbit lehet a

$\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

állapotban és a qbit megmérésekor $\frac{1}{4}$ valszínűséggel a $|0\rangle$ bázis vektort kapjuk eredményül és $\frac{3}{4}$ valószínűséggel a $|1\rangle$ bázis vektort kapjuk eredményül. Azt mondjuk hogy egy kvantum rendszer zárt amíg nincs kölcsönhatásban a külvilággal, azaz amíg nem végzünk mérést a rendszeren.

Választhatunk más ortonormális bázist is. Például tekintsük a

$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

bázis vektorokat.

Ekkor a $|\psi\rangle$ qbitet az alábbi módon reprezentálhatjuk:

$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0\frac{|+\rangle+|-\rangle}{\sqrt{2}} + \alpha_1\frac{|+\rangle-|-\rangle}{\sqrt{2}}.$

Tehát

$|\psi\rangle = \frac{\alpha_0+\alpha_1}{\sqrt{2}}|+\rangle + \frac{\alpha_0-\alpha_1}{\sqrt{2}}|-\rangle$.

A Hadamard mátrixot sokszor fogjuk használni. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

A Hadamard mátrixszal való balról való szorzás a $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ állapothoz milyen ϕ állapotot rendel hozzá ?

$\phi = H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha_0+\alpha_1 \\ \alpha_0-\alpha_1 \end{pmatrix}$. Tehát $\phi = \frac{1}{\sqrt{2}}((\alpha_0+\alpha_1)|0\rangle + (\alpha_0-\alpha_1)|1\rangle)$.

Két qbit által alkotott pár, összefonódás

Tekintsük a $\mathcal{H}_4$ Hilbert teret és a $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, bázis vektorokat. A $|\psi\rangle$ állapotvektor előáll a bázis vektorok lineáris kombinációjaként:

$\psi = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$,

ahol $\alpha_0 0, \alpha_{01}, \alpha_{10}, \alpha_{11}$ komplex számok. Amikor megmérünk két qbit által alkotott $|\psi\rangle$ párt, akkor a kvantum rendszer $|\psi\rangle$ állapotát rávetítjük a négy bázis állapot valamelyikére, az $|\alpha_{00}|^2$ $|\alpha_{01}|^2$, $|\alpha_{10}|^2$, $|\alpha_{11}|^2$ valószínűséggel.

$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

Tekintük az két qbitből álló rendszernek azt a speciális állapotát amikor

$\alpha_{00} = \alpha_{11} = \frac{1}{\sqrt{2}}$ és $\alpha_{01} = \alpha_{10} = 0$. Ezt az állapotot Bell állapotnak nevezzük és a qbit párt pedig EPR párnak hívjuk. Tegyük fel hogy a két qbitből álló rendszer ebben az állapotban van. Amikor megmérjük az első qbitet a két lehetséges eredmény: 0, $\frac{1}{2}$ valószínűséggel és 1, $\frac{1}{2}$ valószínűséggel. A két megfelelő mérés utáni állapot:

$|\psi_0'\rangle = |00\rangle$

és

$|\psi_1'\rangle = |11\rangle$

Amikor megmérjük a második qbitet, a két lehetséges eredmény: 0, $\frac{1}{2}$ valószínűséggel és 1, $\frac{1}{2}$ valószínűséggel. A két megfelelő mérés utáni állapot:

$|\psi_0''\rangle = |00\rangle$

és

$|\psi_1''\rangle = |11\rangle$

A két mérés összefügg egymással. Amikor az első bitet mérjük meg ugyanazt az eredményt kapjuk mint amikor a második bitet mérjük meg. A két qbit lehet különböző helyen, mégis amikor megmérjük a másodikat tudjuk hogy az első milyen állapotban van.

A Bell állapotok. Négy speciális állapotot hívunk Bell állapotoknak. A Bell állapotokegy ortonormális bázist alkotnak.

1. $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$,
2. $|\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$,
3. $|\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$,
4. $|\beta_{01}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$,

A két qbitből álló rendszer lehet szuperpozíció állapotban vagy összefonódott állapotban. A szuperpozíció állapotban mindegyik (mind a kettő) qbitnek jól definiált állapota van, két állapot tenzor szorzata a rendzser állapota. Az összefonódott állapotban a két qbitből álló rendszernek jól definiált állapota van, de egyik qbitnek sincsen jól definiált állapota. Például tekintsük azt az esetet amikor az első qbit az $|1\rangle$ állapotban van, a második qbit pedig a $\sqrt{\frac{1}{2}}(|0\rangle + |1\rangle)$ állapotban van. Ekkor a rendszer állapota előáll a két qbit állapotának a tenzor szorzataként.

$\sqrt{\frac{1}{2}}|1\rangle(|0\rangle + |1\rangle) = \sqrt{\frac{1}{2}}(|10\rangle + |11\rangle) =$

Tekintsük a $\sqrt{\frac{1}{2}}(|00\rangle + |11\rangle) =$ összefonódott állapotot. Ezt az

állapotot nem lehet két qbit állapotának a tenzor szorzataként felírni. Általában is igaz, hogy az összefonódott állapotot nem lehet két qbit állapotának a tenzor szorzataként felírni.

Általában az n qbitből álló rendszert a 2^n dimenziós $\mathcal{H}_{2^n}$ Hilbert térben egy 1 (egység) hosszú vektor reprezentálja. Teljesül hogy $\mathcal{H}_{2^n}$ a tenzor szorzata n darab két dimenziós Hilbert térnek.

A qbit megvalósítása az elektron spinjével

A kvantum részecske (mint például az elektron) nem rendelkezik definiált forgás tengellyel. Az elektron töltése változó térbeli eloszlással rendelkezik. Ennek a töltés eloszlásnak az időbeli változása társul az elektron benső forgásával a térben véletlenszerű irányokban. Az elektron benső forgásához rendelünk egy fizikai mennyiséget, a "spin szög mozgásmennyiséget"-ot. A spin leírja az elektron benső szög mozgásmennyiséget. A kísérletek azt igazolták hogy az elektron spinje 'felfelé mutat' vagy 'lefelé mutat értéket' veszi fel a mérés tengelye mentén, függetlenül attól hogy hogyan választjuk meg a mérés tengelyét.

A $|0\rangle$ és $|1\rangle$ qbit állapotok megfelelnek a spin fel $|\uparrow\rangle$ és spin le $|\downarrow\rangle$ állapotoknak egy általunk választott tengely mentén, ilyen lehet például a z tengely. A spin állapotokat ortogonális egység vektorokkal reprezentáljuk:

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ és } |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Kvantum kapu és kvantum áramkör

A kvantum kapukból építjük fel a kvantum számítógépet. A kvantum kapu az inputját az outputba transzformálja át az igazságtáblája alapján. A kvantum kapu a kvantum rendszer állapotát transzformálja át egy új állapotba. A kvantum kapuk (és a belőlük felépített kvantum áramkörök) által megvalósított állapot tran-

szformációkat unitér operátorokkal írjuk le. Az állapot transzformációt leíró mátrixot áthelyező mátrixnak nevezzük.

Az áthelyező mátrix unitér és az általa indukált transzformáció megfordítható. Az unitér transzformáció megfelel egy hossz megőrző és információ megőrző forgatásnak a vektortérben.

A kvantum kapunak a bemenete és a kimenete ugyanannyi véges sok qbitből áll. Tehát a bemenet állhat $1, 2, 3$ stb qbitből, a kimenet is ugyanannyi qbitből áll mint a bemenet. A bemeneti állapotot és a kimeneti állapotot egy-egy Hilbert térbeli vektorral írjuk le A Hilbert tér dimenziójának a száma 2 hatványa ahol a kitevő a bemeneti qbitek száma. Azaz a Hilbert tér $\mathcal{H}_2$ amikor a bemenet 1 qbitből áll, $\mathcal{H}_4$ amikor a bemenet 2 qbitből áll, $\mathcal{H}_8$ amikor a bemenet 3 qbitből áll, stb. Az n-qbites kvantum kapu bemeneti állapota az egyes input qbitek $\mathcal{H}_2$-beli állapotvektorainak a tenzori szorzata.

Például ha ϕ és ψ a 2-qbites kvantum kapu bemeneti qbitjeinek az állapotvektorai akkor $\phi \otimes \psi$ a kvantum kaput inputjának az állapotvektora. Az n-qbites kvantum kapu elemzésekor használt ortonormális bázis:

1. $|0\rangle$ és $|0\rangle$ $\mathcal{H}_2$ -ben amikor $n = 1$
2. $|00\rangle$ és $|01\rangle$ $|10\rangle$ és $|11\rangle$ $\mathcal{H}_4$ -ben amikor $n = 2$
3. $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ és $|111\rangle$ $\mathcal{H}_8$ -ban amikor $n = 3$ stb.

Tegyük fel hogy $|V\rangle$ a kvantum rendszer kezdeti állapota amely a kapu inputja. A kapu által indukált állapot transzformációt a $\mathbf{G}$ operátor írja le. A $\mathbf{G}$ operátort a G mátrix reprezentálja. Ekkor az eredményül kapott $|W\rangle$ kimeneti állapotra teljesül hogy $|W\rangle = G|V\rangle$.

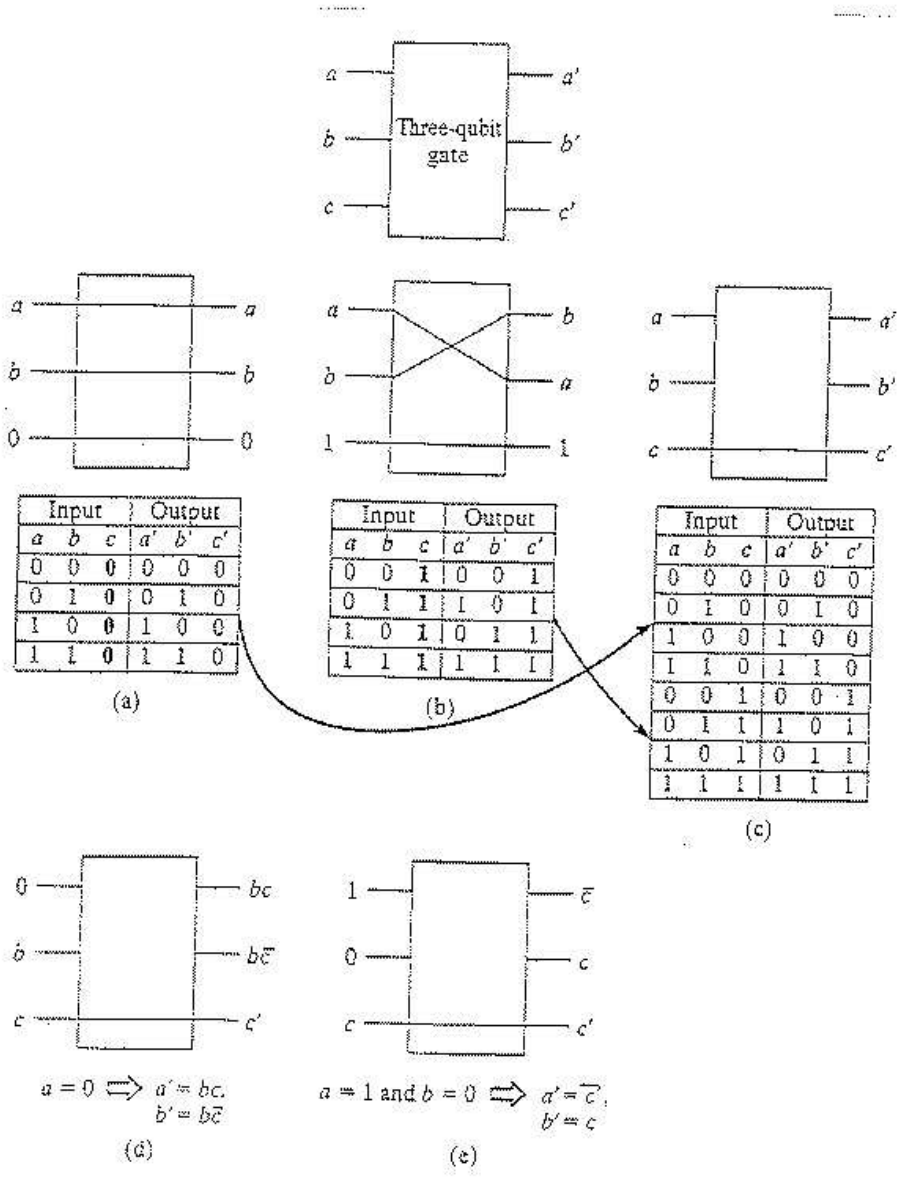
$\oplus$ jelöli az összeadást modulo 2; az output 1 amikor a két input

különbözik egymástól, és 0 amikor a két input egyenlő egymással. Ha $y = 0$, akkor $x+y = x$. Az az összeadást modulo 2 igazságtáblája megegyezik az XOR igazságtáblájával.

Ismert hogy minden logikai függvény kifejezhető AND és NOT kapuk felhasználásával. Tehát tetszőleges logikai függvényt kiszámító logikai áramkört fel tudunk építeni AND és NOT kapuk felhasználásával. Minden
$f : \{ 0, 1 \}^n \rightarrow \{ 0, 1 \}^m$, $n, m \geq 0$
leképezés kiszámítható olyan hagyományos logikai áramkörrel amely AND és NOT kapukból épül fel. Az AND, $NAND$, XOR hagyományos kapuk nem megfordíthatók. Ha ismerjük az outputot akkor nem tudjuk megállapítani hogy mi az input. Például ha tudjuk hogy az AND kapu outputja 0, akkor nem tudjuk hogy mi az input. A NOT kapu megfordítható. Két NOT kapu egymás utáni alkalmazása kiadja az első inputját. A klasszikus logikai kapuk nem megfordítható tulajdonsága azt eredményezi hogy információt veszítünk az alkalmazásukkor.

A Fredkin kapu

Az első ábrán látható a hagyományos Fredkin kapu.



1. ábra

1. A c kontrol input közvetlenül áthelyezi az outputba: $c' = v$.

2. Amikor $c = 0$, akkor a két cél inputot módosítás nélkül áthelyezi az outputba: $a' = a$, és $b' = b$

3. Amikor $c = 1$, a két cél input értékét felcseréljük: $a' = b$ és $b' = a$.

A hagyományos Fredkin kapu univerzális, azaz utánozni tudja az AND és NOT kapukat. Minden
$f : \{ 0, 1 \}^n \to \{ 0, 1 \}^m$, $n, m \geq 0$
leképezés kiszámítható olyan hagyományos logikai áramkörrel amely hagyományos Fredkin kapukból épül fel.

A klaszikus Fredkin kapu megfordítható. Ha a klasszikus Fredkin kapu outputjára ismét alkalmazzuk a klasszikus Fredkin kaput, akkor visszakapjuk az első kapu inputját.

Definiáljuk a kvantum Fredkin kaput! A klasszikus Fredkin kapu és a kvantum Fredkin kapu igazság táblája megegyezik. A Fredkin kapu áthelyező mátrixa:

$$G_{Fredkin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$|W_{Fredkin}\rangle = G_{Fredkin}|V_{Fredkin}\rangle$.

Kvantum áramkörök

Definíció 1.17 *Kvantum számítógépnek nevezzük az n qbitből álló rendszert amelyre az alábbi műveletek hajthatók végre:*

1. Minden qbitnek a kezdőértékét beállíthatjuk a $|0\rangle$ *értékre.*

2. Minden qbitet megmérhetünk a $\{ |0\rangle, |1\rangle \}$ *bázisban.*

3. Véges sokszor, tetszés szerint alkalmazhatunk kvantum kaput a qbitek tetszöleges, rögzitett nagyságú, részhalmazára.

4. A qbitek a kizárólag a fenti transzformációk szerint fejlődnek.

Ha több kaput alkalmazunk egyszerre, párhuzamosan, akkor az eredő transzformáció áthelyező mátrixa az egyes kapuk áthelyező mátrixainak tenzor szorzata.

Ha egymás után alkalmazunk két kaput, akkor az eredő transzformáció áthelyező mátrixa az egyes kapuk áthelyező mátrixainak mátrix szorzata. A szorzásban fordított sorrendben vannak a mátrixok.

A kvantum kapuk összekötésével építjük fel a kvantum áramköröket. Megszorítások:

1. Az áramkörök nem tartalmaznak kört. Nincsen visszacsatolás.

2. Nem tudunk ismeretlen qbitet másolni (klónozni) úgy hogy az eredeti példány állapota változatlan. Szemléletesen: a kvantum rendszer állapotának két példánya szigorúan több információt tartalmaz mint egy példány. Ezért nem lehet másolni az ismeretlen kvantum állapotot.

A kvantum számítógép matematikai modellje.
A kvantum számítógép bemeneti és kimeneti kvantum vezetékekből és kvantum áramkörből áll. A kvantum áramkör kvantum kapukból épül fel. A kvantum áramkör n darab input qbitet képez n darab output kvantum bitbe. Ez a megfordíthatóság szükséges és elegendő feltétele.

A kvantum számítógép áthelyező mátrixa egy G unitér márix amely 2^n darab sorból és 2^n darab oszlopból áll. A kvantum kapu a $|V\rangle$ input vektort a $|W\rangle$ vektorba transzformálja át: $|W\rangle = G|V\rangle$.

A kvantum számítógép inputja k hagyományos bitből álló bináris sztring, ahol $k \leq n$. Ezt az inputot kiegészítjük n hosszú hagyományos bináris sztringre, az utolsó $n-k$ bitet 0-ra állítjuk. Legyen $b' = b_0 b_1 \dots b_{k-1} 00 \dots 0$. Tekintsük a fenti sztringnek megfelelő $|V_{b'}\rangle$ $\mathcal{H}_{2^n}$ Hilbert térbeli vektort. A kvantum számítógép outputja

$$|W\rangle = G|V_{b'}\rangle = \sum_{j=0}^{2^n-1} \alpha_j |u_j\rangle$$

itt $|u_j\rangle$-t a $\mathcal{H}_{2^n}$ tér j-edik bázisvektora. Az α_j komplex számot, $1 \leq i \leq 2^n - 1$ valószínűségi amplitúdónak nevezzük. Az α_j komplex számok kielégítik a

$$\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1.$$

feltételt.

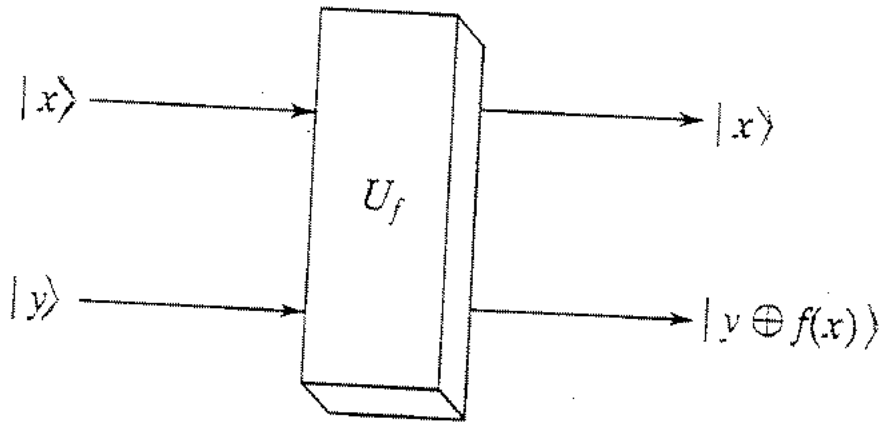
Ha megmérjük a kvantum számítógép outputját akkor $|u_j\rangle$-t (a $\mathcal{H}_{2^n}$ tér j-edik bázisvektorát) kapjuk $|\alpha_j|^2$ valószínűséggel, $1 \leq j \leq 2^n - 1$. Az $|u_j\rangle$ eredmény előáll n darab $\mathcal{H}_2$-beli qbit tenzor szorzataként. Ennek megfeleltetünk n darab hagyományos bitet.

Állítás 1.18 *Tekintsünk egy tetszőleges hagyományos logikai áramkört, amely valamely $f(x)$ függvényt számít ki. Fel tudunk*

építeni egy megfordítható kvantum áramkört amely szintén az $f(x)$ *függvényt számítja ki.*

Bizonyítás: a Fredkin hagyományos kapu univerzális, utánozni tudja az AND kapu számítását és a NOT kapu számítását. Segéd qbiteket használunk fel a számolás során.

□



2. ábra

A második ábrán látható két qbites kvantum áramkör egy adott $f : \{0, 1\} \to \{0, 1\}$

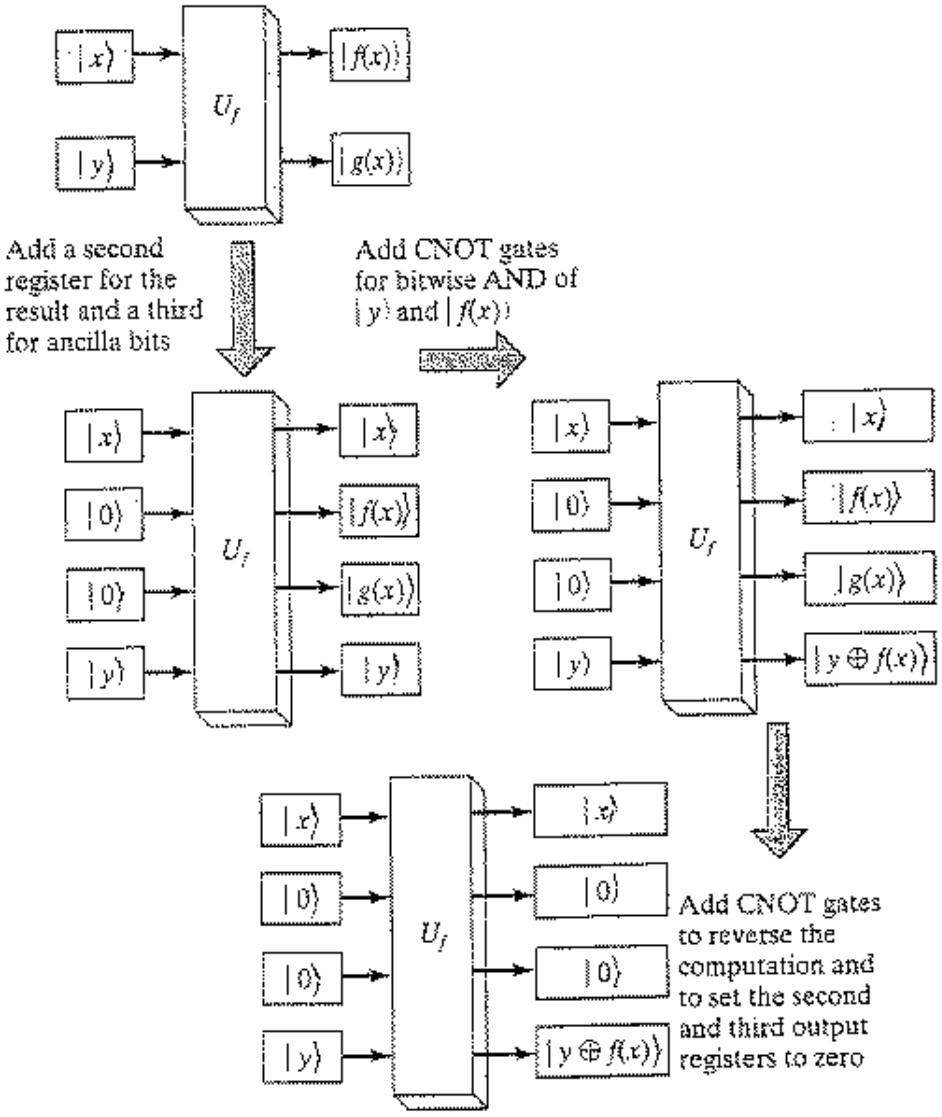
függvényre az

$U_f : |x\, y\rangle \rightarrow |x\, y \oplus f(x)\rangle$

leképezést valósítja meg. Tehát az $|x\rangle$, $|y\rangle$ qbiteket rendre az $|x\rangle$, $|f(x) \oplus y\rangle$ qbitekbe transzformálja át. Amikor $|y\rangle = |0\rangle$, akkor a transzformáció: $|x\, 0\rangle \mapsto |x\, f(x)\rangle$. Az ábrán látható kvantum áramkör megfordítható. Az $|x\, y \oplus f(x)\rangle$ output egyértelműen meghatározza $|x\, y\rangle$ input értékét.

Tetszőleges $f(x)$ függvényre meg tudjuk konstruálni a második ábrán látható kvantum áramkört úgy hogy csupán kvantum Fredkin kapukat tartalmaz. Hangsúlyozzuk hogy az $f(x)$ függvény be van huzalozva a kvantum áramkörbe.

A fentieket természetes módon lehet általánosítani több qbitre. Továbbá szükségünk van munka qbitekre amelyek kezdőértéke $|0\rangle$ és amelyek értékét a számolás végén vissza kell állítanunk $|0\rangle$-ra. Lásd a harmadik ábrát.


$|x\rangle$
$|y\rangle$
U_f
$|f(x)\rangle$
$|g(x)\rangle$
Add a second register for the result and a third for ancilla bits
Add CNOT gates for bitwise AND of $|y\rangle$ and $|f(x)\rangle$
$|0\rangle$
$|x\rangle$
$|f(x)\rangle$
$|g(x)\rangle$
$|y\rangle$
$|y \oplus f(x)\rangle$
Add CNOT gates to reverse the computation and to set the second and third output registers to zero

3. Idea

Nem tudunk ismeretlen qbitet másolni (klónozni)

Állítás 1.19 *Nem tudunk ismeretlen qbitet másolni (klónozni).*

Bizonyítás. Tegyük fel hogy van egy olyan két qbites kapu amely képes valamelyik inputját másolni. A kapu által megvalósított transzformáció egy lineáris leképezés. A $|V\rangle$ input vektort a $|W\rangle$ vektorba transzformálja át: $|W\rangle = G|V\rangle$, ahol G a kapu áthelyező mátrixa. $\mathbf{G}$ jelöli a kapu által megvalósított unitér transzformációt.

Legyen $|\psi\rangle$ és $|\phi\rangle$ két egymára merőleges qbit állapot. Az első input előbb a $|\psi\rangle$ és azután a $|\phi\rangle$ állapot lesz, mindkét esetben a második input a $|0\rangle$ qbit állapot lesz.

Feltettük hogy a kapu klónozza az első inputját. Tehát

$\mathbf{G}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle|\psi\rangle$.

Azaz

$\mathbf{G}(|\psi 0\rangle) = |\psi\psi\rangle$.

Hasonlóan:

$\mathbf{G}(|\phi\rangle \otimes |0\rangle) = |\phi\rangle|\phi\rangle$.

Azaz

$\mathbf{G}(|\phi 0\rangle) = |\phi\phi\rangle$.

Most tekintsük a $|\xi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ állapotot. Mivel $\mathbf{G}$ lineáris leképezés,

$\mathbf{G}(|\xi 0\rangle) = \mathbf{G}(\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)|0\rangle) =$

$\frac{1}{\sqrt{2}}[\mathbf{G}(|\psi 0\rangle) + \mathbf{G}(|\phi 0\rangle)] = \frac{1}{\sqrt{2}}(|\psi\psi\rangle + |\phi\phi\rangle)$.

Most $|\xi\rangle$ legyen a másoló kapu első inputja. Ekkor $\mathbf{G}(|\xi 0\rangle) = |\xi\xi\rangle$. $\mathbf{G}$ és $|\xi\rangle$ definíciója szerint:

$\mathbf{G}(|\xi 0\rangle) = |\xi\xi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) \otimes \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) =$

$\frac{1}{2}(|\psi\psi\rangle + |\psi\phi\rangle + |\phi\psi\rangle + |\phi\phi\rangle)$.

$\neq \frac{1}{\sqrt{2}}(|\psi\psi\rangle + |\phi\phi\rangle)$.

Ellentmondás. (Az ellentmondás még jobban látszik a $\psi = |1\rangle$ és $\phi = |0\rangle$ érték választásra.)

A fenti bizonyítást természetes módon általánosíthatjuk tetszőleges kvantum számítógépre.

□

Irodalom

• M. Le Bellac, A Short Introduction to Quantum Information and Quantum Computation Cambridge, 2006.

• A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, Classical and Quantum Computation, Graduate Studies in Mathematics, volume 47, AMS 2002.

• D. C. Marinescu, G. M. Marinescu, Approaching Quantum Computing, Pearson Prentice Hall, 2005.

• M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge, 2007.

• W. H. Steeb, Y. Hardy, Problems & Solutions in Quantum Computing & Quantum Information, Word Scientific, 2004.