

Kvantumszámítás

Vágvölgyi Sándor

SZTE, Számítástudomány Alapjai Tanszék

Szeged, Árpád tér 2

H-6720

E-mail: vagvolgy@inf.u-szeged.hu

1. Bevezetés

A kvantumszámítógépek a számolásokat kvantumalgoritmusok segítségével végzik, melyek véges sok kvantumbites műveletekből építhetők fel. Ezeket az elemi műveleteket és a műveleteket megvalósító fizikai eszközöket is kvantum kapuknak nevezzük. A kvantumszámítógép ezen kvantum kapuk rendszere. A kapuk meghatározott qubiteken hajtanak végre változtatásokat, ami az egész összefonódott állapot megváltozását eredményezi. A qubit hordozóiként elvben minden olyan rendszer alkalmas, amelynek két, jól megkülönböztethető állapota van. Ilyen a foton (a fény részecskéje) két egymásra merőleges polarizációja; alkalmasan előkészített kétállapotú atomok vagy ionok, és spinnel rendelkező részecskékből álló folyadékok.

A kvantumszámítás lehetőségei beláthatatlanok és a közelmúltban elért fejlődés ígéretes, a kvantumszámítógépek kereskedelmi szintű elterjedése mégis messze van. A jelenlegi kvantumszámítógépek csupán laboratóriumi kísérletek tárgyai. Az első működő példányok

feltehetőleg bonyolult matematikai problémák megoldása során jelentkező speciális részfeladatok megoldására fognak majd szolgálni.

2. Vektorterek

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: $a \cdot (b + c) = a \cdot b + a \cdot c$.

$\mathcal{A}$ vektortér három összetevőből áll:

1. $(V, +, \mathbf{0})$ Ábel csoport. V elemeit vektoroknak nevezzük.
2. $(F, +, 0, \cdot, 1)$ test. F a valós számok halmaza vagy a komplex számok halmaza. F tetszőleges 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,

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

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

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

$$1 \cdot \alpha = \alpha.$$

$\mathbf{R}$ a valós számok teste, $\mathbf{C}$ a komplex számok teste. $\mathbf{R}^n$ a valós számok feletti n komponensű vektorok halmaza. $\mathbf{C}^n$ a komplex számok feletti n komponensű vektorok halmaza.

$\mathbf{R}^n$ (és $\mathbf{C}^n$) fölött értelmezzük az összeadást:

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} v_1 + z_1 \\ v_2 + z_2 \\ \vdots \\ v_n + z_n \end{pmatrix}.$$

$\mathbf{R}^n$ (és $\mathbf{C}^n$) fölött értelmezzük a skalárral való szorzást:

$$v \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} vz_1 \\ vz_2 \\ \vdots \\ vz_n \end{pmatrix}$$

Legyen $n \geq 1$. Az $\{\alpha_1, \dots, \alpha_m\} \in \mathbf{R}^n$ vektorhalmaz lineárisan független ha minden $c_1, \dots, c_n \in \mathbf{R}$ esetén,

$$\text{ha } c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n = \mathbf{0}$$

akkor $c_1 = c_2 = \dots = c_n = 0$.

Ha $\{\alpha_1, \dots, \alpha_m\} \in \mathbf{R}^n$ vektorhalmaz nem lineárisan független, akkor az $\{\alpha_1, \dots, \alpha_m\}$ vektorhalmazt lineárisan függőnek nevezzük.

Hasonlóan definiáljuk a komplex számok feletti vektorokra a line-

árisan függetlenség fogalmát. Legyen $n \geq 1$. Az $\{\alpha_1, \dots, \alpha_m\} \in \mathbf{C}^n$ vektorhalmaz lineárisan független ha minden $c_1, \dots, c_n \in \mathbf{C}$ esetén,

$$\text{ha } c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n = \mathbf{0}$$

$$\text{akkor } c_1 = c_2 = \dots = c_n = 0.$$

Ha $\{\alpha_1, \dots, \alpha_m\} \in \mathbf{C}^n$ vektorhalmaz nem lineárisan független, akkor az $\{\alpha_1, \dots, \alpha_m\}$ vektorhalmazt lineárisan függőnek nevezzük.

Legyen $\mathcal{A}$ egy vektortér. Az $S \subseteq V$ részhalmazt résztérnek nevezzük ha S zárt az összeadásra és a skalárral való szorzásra. Azaz (a) két S -beli vektor összege eleme S -nek, és (b) minden S -beli vektorra és minden skalárra, a szorzatuk eleme S -nek.

Állítás 2.1 Legyen $\mathcal{A}$ egy vektortér. Tetszőleges $\mathcal{A}$ -beli vektorhalmaz összes lineáris kombinációinak halmaza $\mathcal{A}$ -nak egy részterét alkotja.

Bizonyítás. Minden $c, c_1, c_2, \dots, c_m, c'_1, c'_2, \dots, c'_m \in F$ esetén,

$$\begin{aligned} (c_1\alpha_1 + c_2\alpha_2 + \dots + c_m\alpha_m) + (c'_1\alpha_1 + c'_2\alpha_2 + \dots + c'_m\alpha_m) &= \\ (c_1 + c'_1)\alpha_1 + (c_2 + c'_2)\alpha_2 + \dots + (c_m + c'_m)\alpha_m &= \\ c(c_1\alpha_1 + c_2\alpha_2 + \dots + c_m\alpha_m) &= \\ (cc_1)\alpha_1 + (cc_2)\alpha_2 + \dots + (cc_m)\alpha_m & \end{aligned}$$

□

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 2.2 Ha $\{b_1, b_2, \dots, b_m\}$ és $\{c_1, c_2, \dots, c_n\}$ bázisai az $\mathcal{A}$ vektortérnek, 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 $\mathbf{R}^3$ vektortérnek. Tehát $\dim(\mathbf{R}^3) = 3$.

Például az $\mathbf{C}^2$ vektorteret kifeszíti a

$$\alpha = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \beta = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

vektorokból álló vektorhalmaz. Mert tetszőleges $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ vektor felírható $\frac{a_1+a_2}{\sqrt{2}}\alpha + \frac{a_1-a_2}{\sqrt{2}}\beta$ alakban.

2.1. Az n -dimenziós valós Euklidészi vektortér

Legyen $n \geq 1$, $\mathbf{R}^n$ jelöli az n -dimenziós valós vektorteret.

Definíció 2.3 Az $\mathbf{R}^n$ vektorteret n -dimenziós valós Euklidészi vektortérnek nevezzük ha minden $\alpha, \beta \in \mathbf{R}^n$ vektorhoz hozzárendelünk egy (α, β) valós számot úgy hogy az alábbi négy feltétel teljesül:

1. $(\alpha, \beta) = (\beta, \alpha)$,
2. $(c\alpha, \beta) = c(\alpha, \beta), \quad c \in \mathbf{R},$

$$3. (\alpha + \gamma, \beta) = (\alpha, \beta) + (\gamma, \beta), \quad \gamma \in \mathbf{R}^n,$$

$$4. (\alpha, \alpha) \geq 0 \text{ és}$$

$$(\alpha, \alpha) = 0 \text{ akkor és csak akkor ha } \alpha = \mathbf{0}.$$

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

Az α vektor hossza $\|\alpha\| = \sqrt{(\alpha, \alpha)}$. Az α, β vektorok által bezárt szög a θ valós szám:

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

Ebből következik hogy

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

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

Állítás 2.4 Egy n -dimenziós Euklidészi vektortérben ha az $\{e_1, \dots, e_n\}$ vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{e_1, \dots, e_n\}$ bázist alkot.

Egy n -dimenziós Euklidészi vektortérben ha az $\{e_1, \dots, e_n\}$ vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{e_1, \dots, e_n\}$ vektorhalmazt ortogonális bázisnak nevezzük. Ha még az is teljesül hogy minden vektor hossza 1, akkor $\{e_1, \dots, e_n\}$ vektorhalmazt ortonormális bázisnak nevezzük. Az $\{e_1, \dots, e_n\}$ 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 2.5 Minden n -dimenziós Euklidészi vektortérnek van ortonormális bázisa.

Legyen $\{e_1, \dots, e_n\}$ ortonormális bázisa az n -dimenziós Euklidészi vektortérnek. Tetszőleges α, β vektorokra, $\alpha = a_1e_1 + a_2e_2 + \dots + a_ne_n$ és $\beta = b_1e_1 + b_2e_2 + \dots + b_ne_n$. Mivel $(e_i, e_j) = \delta_{i,j}$, kapjuk hogy $(\alpha, e_i) = a_i$ és $(\alpha, \beta) = \sum_{i=1}^n a_ib_i$.

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

Definíció 2.6 Legyenek $V_{\mathcal{A}}$ és $V_{\mathcal{B}}$ vektorterek. Az $A : V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ lineáris leképezést operátornak nevezzük.

Az $A : V_{\mathcal{A}} \times V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ leképezést bilineárisnak nevezzük ha teljesül hogy

1. Minden rögzített β esetén, $A(\alpha; \beta)$ az α lineáris függvénye.
2. Minden rögzített α esetén, $A(\alpha; \beta)$ a β lineáris függvénye.

Állítás 2.7 Legyenek $\mathcal{A}$ és $\mathcal{B}$ vektorterek ugyanazon F test felett. Az $A : V_{\mathcal{A}} \times V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ leképezés bilineáris akkor és csak akkor ha

$$A(a\alpha + b\alpha'; \beta) = aA(\alpha; \beta) + bA(\alpha'; \beta)$$

és

$$A(\alpha; c\beta + d\beta') = cA(\alpha; \beta) + dA(\alpha; \beta')$$

Azt mondjuk hogy az A bilineáris függvény szimmetrikus ha $A(\alpha; \beta) = A(\beta; \alpha)$.

Például, az Euklidészi tér felett két vektor belső szorzata szimmetrikus bilineáris függvény.

Legyen $A : V_{\mathcal{A}} \times V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ szimmetrikus bilineáris leképezés. Az $A' : V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ leképezést az $A'(\alpha) = A(\alpha, \alpha)$ egyenlőséggel definiáljuk. Az A' függvényt kvadratikus alaknak nevezzük. Az $A'(\alpha)$ jelölés helyett az $A(\alpha; \alpha)$ jelölést használjuk. Az $A(\alpha; \alpha)$ kvadratikus alakot pozitív definitnek nevezzük ha minden $\alpha \neq \mathbf{0}$ vektorra $A(\alpha; \alpha) > 0$. Az $A(\alpha; \alpha)$ kvadratikus alakhoz hozzárendeljük az $\mathbf{A}(\alpha; \beta)$ bilineáris alakot. Az $\mathbf{A}(\alpha; \beta)$ bilineáris függvényt az $A(\alpha; \alpha)$ kvadratikus alakhoz rendelt poláris alaknak nevezzük. Igazolható hogy $\mathbf{A}(\alpha; \beta)$ bilineáris alakot egyértelműen meghatározza az $A(\alpha; \alpha)$ kvadratikus alak.

Állítás 2.8 $A(\alpha; \alpha)$ kvadratikus alak egyértelműen meghatározza az $\mathbf{A}(\alpha; \beta)$ bilineáris alakot.

Az Euklidészi tér egy másik, ekvivalens definíciója: Az Euklidészi tér egy olyan vektortér ahol egy $A(\alpha; \alpha)$ pozitív definit kvadratikus alak van értelmezve. Az $A(\alpha; \alpha)$ kvadratikus alakhoz hozzárendeljük az egyértelmű $\mathbf{A}(\alpha; \beta)$ bilineáris alakot. Az α, β vektorok belső szorzata az $\mathbf{A}(\alpha; \beta)$ bilineáris alak értéke.

2.2. Operátorok és mátrixok

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

Definíció 2.9 Legyen $V_{\mathcal{A}}$ egy vektortér. Az $A : V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ lineáris leképezést operátornak nevezzük.

Az F test fölötti mátrix egy olyan téglalap alakú táblázat amelynek m sora és n oszlopa van.

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

$A = [a_{ij}]$ jelölést használjuk.

Az A mátrix lineáris leképezést indukál az F^n n dimenziós vektortérből az F^m m dimenziós vektortérbe. Ha az A mátrixot jobbról megszorozzuk egy n komponensű oszlopvektorral, akkor egy m komponensű oszlopvektort kapunk. Minden A lineáris leképezéshez van olyan M mátrix amely az A lineáris leképezést indukálja.

Elemi sorműveletek:

1. Két sor felcserélése.
2. Egy sor valamely $c \in F$ konstanssal való szorzása: a sor minden elemét megszorozzuk a $c \in F$ konstanssal.
3. Egy sor és valamely $c \in F$ szorzatának egy másik sorhoz való hozzáadása.

Azt mondjuk hogy két mátrix sor ekvivalens ha az egyik eláll a másiktól sorműveletek véges sorozatával.

Legyen $n = m$. Az egység mátrix az az $I = [a_{ij}]$ mátrix amelyre teljesül hogy $a_{ii} = 1$, $1 \leq i \leq n$, és $a_{ij} = 0$, $1 \leq i < j \leq n$. A permutációs mátrixot az egység mátrix sorainak és oszlopainak a felcserélésével kapjuk.

Az A $n \times n$ mátrix determinánsát $|A|$ jelöli. Ha felcseréljük A két sorát, akkor $|A|$ előjele ellentétesre vált. Az A mátrix transzponáltjának a determinánsa megegyezik az A mátrix transzponáltjának a determinánsával: $|A^T| = |A|$. Ha A -nak két sora megegyezik, akkor $|A| = 0$.

Az $\mathbf{A}(\beta; \gamma)$ bilineáris alakot β, γ vektoroknak az $e_1, e_2, \dots, e_n$ ortonormális bázishoz tartozó vetületének függvényében fejezzük ki. Legyen $\beta = b_1e_1 + b_2e_2 + \dots + b_ne_n$ és $\gamma = c_1e_1 + c_2e_2 + \dots + c_ne_n$. Ekkor $\mathbf{A}(\beta; \gamma) = \mathbf{A}(b_1e_1 + b_2e_2 + \dots + b_ne_n; c_1e_1 + c_2e_2 + \dots + c_ne_n)$. Mivel $\mathbf{A}$ bilineáris függvény,

$$\mathbf{A}(\beta; \gamma) = \sum_{i,j=1}^n \mathbf{A}(e_i; e_j) b_i c_j.$$

Itt $\mathbf{A}(e_i; e_j)$ egy valós szám, amelyet a_{ij} -vel jelölünk. Ekkor $\mathbf{A}(\beta; \gamma) = \sum_{i,j=1}^n a_{ij} b_i c_j$. Az $A = [a_{ij}]$ mátrixot az $\mathbf{A}(\beta; \gamma)$ bilineáris alak $e_1, e_2, \dots, e_n$ bázisra vonatkozó mátrixának hívjuk.

2.3. Az n -dimenziós komplex Euklidészi vektortér

Legyen $n \geq 1$, $\mathbf{C}^n$ jelöli az n -dimenziós komplex vektorteret.

Definíció 2.10 Az $\mathbf{C}^n$, vektorteret n -dimenziós komplex Euklidészi vektortérnek nevezzük ha 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. $(c\alpha, \beta) = c^*(\alpha, \beta), \quad c \in \mathbf{C},$
3. $(\alpha + \gamma, \beta) = (\alpha, \beta) + (\gamma, \beta),$
4. $(\alpha, c\beta) = c(\alpha, \beta), \quad c \in \mathbf{C},$

$$5. (\alpha, \beta + \gamma) = (\alpha, \beta) + (\alpha, \gamma),$$

$$6. (\alpha, \alpha) \geq 0 \text{ és } (\alpha, \alpha) = 0 \text{ akkor és csak akkor ha } \alpha = \mathbf{0}.$$

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.

Például, $\mathbf{C}^n$ felett definiáljuk a belső szorzatot az alábbi módon:

$$\left(\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} \right) = \sum_{i=1}^n y_i^* z_i =$$

$$(y_1^*, y_2^*, \dots, y_n^*) \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

Legyen $\alpha \neq \mathbf{0}$ és $\beta \neq \mathbf{0}$. Azt mondjuk hogy α és β merőlegesek (ortogonálisak) ha $(\alpha, \beta) = 0$.

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 $\alpha = \mathbf{0}$.

Állítás 2.11 Egy n -dimenziós komplex Euklidészi vektortérben ha az $\{e_1, \dots, e_n\}$ vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{e_1, \dots, e_n\}$ bázist alkot.

Egy n -dimenziós komplex Euklidészi vektortérben ha az $\{e_1, \dots, e_n\}$ vektorhalmazra teljesül hogy elemei páronként ortogonálisak, akkor $\{e_1, \dots, e_n\}$ vektorhalmazt ortogonális bázisnak nevezzük. Ha még az is teljesül hogy minden vektor hossza 1, akkor $\{e_1, \dots, e_n\}$ vektorhalmazt ortonormális bázisnak nevezzük. Az $\{e_1, \dots, e_n\}$ 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 2.12 Minden n -dimenziós komplex Euklidészi vektortérnek van ortonormális bázisa.

Legyen $\{e_1, \dots, e_n\}$ ortonormális bázisa az n -dimenziós Euklidészi vektortérnek. Tetszőleges α, β vektorokra, $\alpha = a_1e_1 + a_2e_2 + \dots + a_ne_n$ és $\beta = b_1e_1 + b_2e_2 + \dots + b_ne_n$. Mivel $(e_i, e_j) = \delta_{i,j}$, kapjuk hogy $(\alpha, e_i) = a_i$ és $(\alpha, \beta) = \sum_{i=1}^n a_ib_i$.

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

1. Minden rögzített β esetén, $A(\alpha; \beta)$ az α lineáris függvénye.
2. Minden rögzített α esetén, $A(\alpha; \beta)$ a β lineáris függvénye.

Állítás 2.13 Legyenek $\mathcal{A}$ és $\mathcal{B}$ vektorterek ugyanazon F test felett. Az $A : V_{\mathcal{A}} \times V_{\mathcal{A}} \rightarrow V_{\mathcal{B}}$ leképezés bilineáris akkor és csak akkor ha

$$A(a\alpha + b\alpha'; \beta) = aA(\alpha; \beta) + bA(\alpha'; \beta)$$

és

$$A(\alpha; c\beta + d\beta') = cA(\alpha; \beta) + dA(\alpha; \beta')$$

Definíció 2.14 Az $\mathbf{A}$ bilineáris formát Hermite-félének nevezzük ha $A(\alpha; \beta) = (A(\beta; \alpha))^*$.

Állítás 2.15 Az $\mathbf{A}$ bilineáris forma Hermite-féle akkor és csak akkor ha tetszőleges $e_1, e_2, \dots, e_n$ bázisra vonatkozó $A = [a_{ij}]$ mátrixára teljesül hogy $a_{ij} = a_{ji}^*$.

Legyen $\mathcal{A}$ egy bilineáris forma. Legyen $\mathbf{A}^\dagger(\alpha; \beta) = (\mathbf{A}(\beta; \alpha))^*$. Azt mondjuk hogy $\mathbf{A}^\dagger$ az $\mathcal{A}$ adjungáltja.

Állítás 2.16 Az $\mathbf{A}$ bilineáris forma mátrixa legyen A , az $\mathbf{A}^\dagger$ bilineáris forma mátrixa legyen $A^\dagger$. Ekkor teljesül hogy $A^\dagger = (A^*)^T$.

Például a $\begin{pmatrix} 1 - 5i & 1 + i \\ 1 + 3i & 7i \end{pmatrix}$ mátrix adjungáltja a $\begin{pmatrix} 1 + 5i & 1 - 3i \\ 1 - i & -7i \end{pmatrix}$ mátrix.

Az $\mathbf{A}$ bilineáris formát normálisnak nevezzük ha $\mathbf{A}\mathbf{A}^\dagger = \mathbf{A}^\dagger\mathbf{A}$.

Állítás 2.17 Ha $\mathbf{A}$ bilineáris forma Hermite-féle (önadjungált), akkor $\mathbf{A}$ normális.

Definíció 2.18 Az U $n \times n$ -es mátrixot unitérnek nevezzük ha $U^\dagger U = U U^\dagger = I_n$, ahol I_n az $n \times n$ -es egység mátrix, azaz

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Mással az a komplex U unitér mátrix olyan négyzetes mátrix, melynek transzponált konjugáltja ($\dagger$ -rel jelölve) egyben inverze is.

Állítás 2.19 Legyen U $n \times n$ -es unitér mátrix. Tetszőleges $\alpha, \beta \in \mathbf{C}^n$ esetén $(U\alpha, U\beta) = (\alpha, \beta)$.

Definíció 2.20 Legyenek $\mathbf{A}$ és $\mathbf{B}$ operátorok. $\mathbf{A}$ és $\mathbf{B}$ kommutátora: az $[A, B] = \mathbf{AB} - \mathbf{BA}$ operátor.

$\mathbf{A}$ és $\mathbf{B}$ kommutatívak (felcserélhetők) ha $[\mathbf{A}, \mathbf{B}] = \mathbf{0}$. Itt a $\mathbf{0}$ operátor minden vektorhoz a nulla vektort rendeli. Azaz $\mathbf{A}$ és $\mathbf{B}$ kommutatívak ha $\mathbf{AB} = \mathbf{BA}$.

2.4. Az n dimenziós Hilbert tér

Tekintsük a komplex számok feletti n dimenziós vektorteret. A $\| \cdot \| : \mathbf{C} \rightarrow \mathbf{R}$ nemnegatív leképezést normának nevezzük ha kielégíti az alábbi feltételeket:

Az α vektor 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 $\alpha = \mathbf{0}$.

A komplex számok feletti n dimenziós vektortér belső szorzata segítségével definiáltuk a vektor hosszát ami kielégíti a fenti feltételeket, ezért a belső szorzat által származtatott normának nevezzük.

Definíció 2.21 Az n dimenziós $\mathcal{H}_n$ Hilbert tér fogalma.

- $\mathcal{H}_n$ a komplex számok feletti n dimenziós vektortér belső szorzattal és a belső szorzat által származtatott normával,
- $\mathcal{H}_n$ erre a normára nézve teljes, azaz minden $\mathcal{H}_n$ -beli Cauchy-sorozat konvergál.

Igazolható, hogy $\mathcal{H}_n$ izomorf a $\mathbf{C}^n$ vektortérrel. Az n dimenziós $\mathcal{H}_n$ Hilbert tér belső szorzata az előzőekben már megadott belső szorzat. A belső szorzat által származtatott norma a fentiek szerint definiált.

Állítás 2.22 Tetszőleges n dimenziós $\mathcal{H}_n$ Hilbert térnek létezik egy ortonormális bázisa.

Tekintsük az alábbi ortonormális bázist, ahol az ortonormális bázis elemeit írhatjuk ket vektorokként:

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

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

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

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

...

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

Az ortonormális bázis elemeit írhatjuk bra vektorokként:

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

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

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.

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_i|i\rangle + \dots + \alpha_{n-1}|n-1\rangle,$$

ahol $\alpha_1, \dots, \alpha_i, \dots, \alpha_{n-1} \in \mathbf{C}$.

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

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

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

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

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

2.5. A belső szorzat az n dimenziós Hilbert térben

A $|\psi_a\rangle, |\psi_b\rangle$ vektorok belső szorzatát $\langle\psi_a|\psi_b\rangle$ jelöli. Azaz $(|\psi_a\rangle, |\psi_b\rangle) = \langle\psi_a|\psi_b\rangle$. A $\langle\psi_a|\psi_b\rangle$ jelölés rövidítése a $(|\psi_a\rangle, |\psi_b\rangle)$ jelölésnek.

1. $\langle\psi|\psi\rangle \in \mathbf{R}$, $\langle\psi|\psi\rangle = 0$ ha $|\psi\rangle = \mathbf{0}$ és $\langle\psi|\psi\rangle > 0$ különben. Tehát egy tetszőleges vektor önmagával való belső szorzata egy nemnegatív valós szám.

2. Konjugált lineáris az első argumentumban és lineáris a második argumentumban

Minden $|\psi_a\rangle, |\psi_b\rangle, |\psi_c\rangle \in \mathcal{H}_n$, és $a, b, c \in \mathbf{C}$ esetén

$$(c|\psi_a\rangle, |\psi_b\rangle) = c^* \langle\psi_a|\psi_b\rangle,$$

$$(|\psi_a\rangle, c|\psi_b\rangle) = c \langle\psi_a|\psi_b\rangle,$$

$$(a|\psi_a\rangle + b|\psi_b\rangle, |\psi_c\rangle) = a^* (|\psi_a\rangle, |\psi_c\rangle) + b^* (|\psi_b\rangle, |\psi_c\rangle),$$

$$(|\psi_c\rangle, (a|\psi_a\rangle + b|\psi_b\rangle)) = a \langle\psi_c|\psi_a\rangle + b \langle\psi_c|\psi_b\rangle$$

$$3. \langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*.$$

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

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

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

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

$$\begin{aligned} \text{Így } \langle\psi_a|\psi_a\rangle &= \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 + \alpha_2^*\alpha_2 + \alpha_3^*\alpha_3 \\ &= |\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2. \end{aligned}$$

Legyen

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

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

$$\text{Ekkor } \langle\psi_a|\psi_b\rangle = (1-i)(1-2i) + (2+3i)(3+2i).$$

Definíció 2.23 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.

2.6. Tenzor és külső szorzat

Definíció 2.24 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.

$$\textbf{Definíció 2.25} \text{ Legyen } A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

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

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

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

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

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

3. Szemléletes példa a kvantum rendszerre

Tekintsünk egy egyenes szakaszt, amelyet egyenlő közökre osztják az $\{x_0, x_1, \dots, x_{n-1}\}$ pontok. Azaz, $x_1 = x_0 + \delta$, $x_2 = x_1 + \delta$, $\dots$, $x_{n-1} = x_{n-2} + \delta$. Itt n nagy és δ kicsi. Egy szubatomi részecske az egyenes szakaszon fordul elő, és az $\{x_0, x_1, \dots, x_{n-1}\}$ pontokban észlelhető. Amikor a részecske az x_i pontban van, akkor az $|x_i\rangle$ állapotban van. Az $|x_i\rangle$ állapotokat alapállapotoknak hívjuk. Az $|x_i\rangle$ állapothoz a következő módon rendeljük hozzá egy oszlopvektort a $\mathbf{C}^n$ vektortérben.

$$|x_0\rangle \mapsto \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

$$|x_1\rangle \mapsto \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

$\dots$

$$|x_i\rangle \mapsto \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

$\dots$

$$|x_{n-1}\rangle \mapsto \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

A részecske állapotát egy n dimenziós komplex számok feletti szlopvektorral adjuk meg. Minden oszlopvektor $\mathbf{C}^n$ vektortérben a részecske valamely állapotát írja le. Tetszőleges $|\psi\rangle$ állapot az $|x_0\rangle, |x_1\rangle, \dots, |x_{n-1}\rangle$ állapotok valamely $c_0, c_1, \dots, c_{n-1}$ komplex számokkal képzett lineáris kombinációja. A $c_0, c_1, \dots, c_{n-1}$ számokat komplex amplitúdónak hívjuk. Itt $|\psi\rangle$ -t komplex hullámnak tekintjük. (Az amplitúdó időben változó mennyiségek legnagyobb eltérése az egyensúlyi állapottól. Pl. inga, rugóra függesztett rezgő test esetén az amplitúdó az egyensúlyi vagy nyugalmi helyzettől számított legnagyobb kitérést jelenti.)

$$|\psi\rangle = c_0|x_0\rangle + c_1|x_1\rangle + \dots + c_{n-1}|x_{n-1}\rangle.$$

Eképpen

$$|\psi\rangle \mapsto \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}.$$

$p(x_i)$ annak a valószínűsége, hogy miután megfigyeljük a részecskét az az x_i pontban lesz.

$$p(x_i) = \frac{|c_i|^2}{\|\psi\|^2} = \frac{|c_i|^2}{\sum_j |c_j|^2}. \quad (1)$$

Figyeljük meg, hogy $p(x_i)$ valós szám és $0 \leq p(x_i) \leq 1$. Amikor

megfigyeljük $|\psi\rangle$ -t, mindig valamelyik bázis állapotban találjuk. Jelölés:

$$|\psi\rangle \longrightarrow |x_i\rangle$$

Tekintsük a $2|\psi\rangle$ állapotot. Mi a valószínűsége, hogy a részecskét az x_j helyen pozíción találjuk?

$$\begin{aligned} p(x_i) &= \frac{|2c_i|^2}{\|\psi\|^2} = \frac{|2c_i|^2}{\sum_j |2c_j|^2} = \\ &= \frac{4|c_i|^2}{4\sum_j |c_j|^2} = \frac{|c_i|^2}{\sum_j |c_j|^2}. \end{aligned}$$

Tehát a $2|\psi\rangle$ állapotvektor ugyanazt a fizikai rendszert írja le mint a $|\psi\rangle$ állapotvektor. Figyeljük meg, hogy 2 helyébe tetszőleges $c \in \mathbf{C}$ komplex számot írva ugyanazt az eredményt kapjuk. Tehát $|\psi\rangle$ állapotvektor hossza nem számít a fizikai rendszer reprezentálásakor.

Legyen $|\psi\rangle$ normalizált ket vektor! Ekkor a (1) egyenlőségben a nevező 1 és az egyenlőség $p(x_i) = |c_i|^2$ alakra egyszerűsödik.

Definíció 3.1 Legyenek $\phi = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$ and $|\psi\rangle = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$ nor-

malizált állapotok. A $|\phi\rangle$ és $|\psi\rangle$ közötti – mérés utáni – átmeneti amplitúdót a következő módon definiáljuk. ϕ a kiindulási állapot. Mérünk. A végállapot pedig $\langle\psi|$ lesz. A ϕ és ψ közötti – mérés utáni – átmeneti amplitúdó a $\langle\psi|\phi\rangle$ belső szorzat.

$$\langle \psi | \phi \rangle = (b_0^* \ b_1^* \ \cdots \ b_{n-1}^*) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \sum_i b_i^* a_i$$

Ha két állapotvektor merőleges egymásra, akkor a mérés utáni átmeneti amplitúdó köztük 0. Ha egy elektron fel állapotban van, akkor a mérés után soha sem lesz le állapotban.

Tegyük fel, hogy a kvantum fizikai rendszernek van egy

$$\{ |b_1\rangle, \dots |b_{n-1}\rangle \}$$

ortonormális bázisa, és egy tetszőleges mérés után mindig a $\{ |b_0\rangle, |b_1\rangle, \dots |b_{n-1}\rangle \}$ végállapotok valamelyikében van a rendszer. De tetszőleges mérés után soha sincsen a fenti állapotok valamely szuperpozíciójában. Tegyük fel, hogy normalizált $|\psi\rangle$ kezdőállapotban van a kvantum fizikai rendszer. Fejezzük ki $|\psi\rangle$ kezdőállapotot a $\{ |b_0\rangle, |b_1\rangle, \dots |b_{n-1}\rangle \}$ ortonormális bázisban!

$$|\psi\rangle = b_0|b_0\rangle + b_1|b_1\rangle + \cdots + |b_{n-1}|b_{n-1}\rangle. \quad (2)$$

$$\text{Tehát A } |\psi\rangle = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

Figyeljük meg, hogy tetszőleges i esetén,

$$\langle b_i | \psi \rangle = (0 \ 0 \ \cdots \ 1 \ \cdots \ 0) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = b_i.$$

Mivel $|\psi\rangle$ normalizált, $1 = \langle\psi | \psi\rangle = |b_0|^2 + |b_1|^2 + \dots + |b_{n-1}|^2$. Tehát $|b_0|^2 + |b_1|^2 + \dots + |b_{n-1}|^2 = 1$.

A fentiek alapján természetes a (2) egyenlőségre úgy tekinteni, hogy hogy minden i esetén $|b_i|^2$ a valószínűsége annak hogy a mérés után a kvantum rendszer a $|b_i\rangle$ állapotban van.

3.1. A fizikai mennyiség

A fizikai mennyiség értéke egy kvantummechanikai mérés során meghatározható, s ezek az értékek, mint kvantumszámok jellemzik az illető kvantummechanikai rendszer állapotát.

A kvantumfizikai rendszer egy állapottérből és a fizikai mennyiségek halmazából áll. Az állapottér azon állapotok halmaza, amiket a kvantumfizikai rendszer felvehet. A fizikai mennyiségek halmaza az állapottér minden egyes állapotában megfigyelhető fizikai mennyiségek halmaza.

Posztulátum 3.2 *A fizikai mennyiség az állapottér feletti Hermite operátorként nyilvánul meg.*

A fizikai mennyiség egy lineáris operátor amely állapotokat állapotokba képez. Ha az Ω fizikai mennyiséget alkalmazzuk a $|\psi\rangle$ állapotvektorra, akkor a $\Omega|\psi\rangle$ állapotvektort kapjuk eredményül. Emlékezzünk, hogy a Hermite operátor sajátértékei valós számok.

Posztulátum 3.3 *Az állapottér tetszőleges ψ állapotában megmérve a fizikai mennyiséget, a hozzárendelt Ω Hermite operátor valamely sajátértékét kapjuk eredményül. Az Ω sajátvektorai az állapottérnek egy bázisát alkotják.*

A 3. fejezet szubatomi részecske példájában a pozíció a legnyilvánvalóbb fizikai mennyiség. A pozíció megmondja, hogy hol van a szubatomi részecske. A pozícióhoz rendelt Hermite operátort P -vel jelöljük. Hogyan hat P a bázis állapotokon?

$$P(|x_i\rangle) = x_i|x_i\rangle. \quad (3)$$

P alkalmazása a pozícióval való szorzást eredményezi. Mivel az alapállapotok bázist alkotnak, kiterjesztjük (3) egyenlőséget tetszőleges állapotokra is.

$$P(\sum c_i|x_i\rangle) = \sum x_i c_i|x_i\rangle. \quad (4)$$

A P operátor standard bázis feletti mátrix reprezentációja:

$$P = \begin{pmatrix} x_0 & 0 & \dots & & 0 \\ 0 & x_1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & x_{n-1} \end{pmatrix}$$

A P mátrix átlójában az x_i koordináták vannak. P Hermite és a sajátértékei az x_i értékek. A normalizált sajátvektorok pedig az $|x_0\rangle, |x_1\rangle, \dots, |x_{n-1}\rangle$ alap állapotvektorok.

Tetszőlegesen adott irányban két alap spin állapot van. A függőleges tengely esetén ezeket az állapotokat spin fel $|\uparrow\rangle$ és spin le $|\downarrow\rangle$ névvel illetjük. Az általános állapot a fel és le szuperpozíciója, azaz

$$|\psi\rangle = c_0|\uparrow\rangle + c_1|\downarrow\rangle.$$

Itt a részecske c_0 az amplitúdóval van a fel állapotban és c_1 az amplitúdóval van a állapotban.

3.2. A mérés

Posztulátum 3.4 *Legyen Ω egy fizikai mennyiség és $|\psi\rangle$ egy állapot. Mérjük meg Ω -t a $|\psi\rangle$ állapotban! Ha Ω megmérésekor a λ sajátértéket kapjuk eredményül, akkor a mérés után az állapot mindig egy a λ sajátértékhez tartozó sajátvektor lesz.*

Példa 3.5 Tekintsük az $\Omega = \begin{pmatrix} -1 & -i \\ i & 1 \end{pmatrix}$ fizikai mennyiséget! Számoljuk ki Ω sajátértékeit és a hozzájuk tartozó sajátvektorokat! A sajátértékek $\lambda_1 = -\sqrt{2}$ and $\lambda_2 = \sqrt{2}$. A megfelelő sajátvektorok rendre $|e_1\rangle = \begin{pmatrix} -0,923i \\ -0,382 \end{pmatrix}$ és $|e_2\rangle = \begin{pmatrix} -0,382i \\ 0,923 \end{pmatrix}$ Tegyük fel, hogy megmérjük Ω -t a $|\psi\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ állapotban és λ_1 mérési értéket figyelünk meg. A kvantum fizikai rendszer $|\psi\rangle$ állapotból az $|e_1\rangle$ állapotba roskadt.

3.3. Kvantum fizikai rendszerek összeszerelése

Egy korábbi példában egy egyenes szakaszt tekintettünk, amelyet egyenlő közökre osztják az $\{x_0, x_1, \dots, x_{n-1}\}$ pontok. Azaz, $x_1 = x_0 + \delta$, $x_2 = x_1 + \delta$, $\dots$, $x_{n-1} = x_{n-2} + \delta$. Itt n nagy és δ kicsi. Egy szubatomi részecske az egyenes szakaszon fordul elő, és az $\{x_0, x_1, \dots, x_{n-1}\}$ pontokban észlelhető.

Most két részecskét tekintünk, – amelyek a fenti példához hasonlóan – egy-egy rácson észlelhetők.

Az első részecske az $\{x_0, x_1, \dots, x_{n-1}\}$ pontokban észlelhető. A második részecske az $\{y_0, y_1, \dots, y_{m-1}\}$ pontokban észlelhető.

Posztulátum 3.6 *Legyenek Q és Q' Tekintsünk két egymástól független kvantum fizikai rendszer, amelyeket rendre a $\mathbf{V}$ és $\mathbf{V}'$ vektorterek reprezentálnak. A Q és Q' egyesítésével kapott kvantum fizikai rendszert a $\mathbf{V} \otimes \mathbf{V}'$ tenzorszorzat reprezentálja.*

Mivel a vektorterek tenzorszorzata asszociatív, egyre nagyobb és nagyobb kvantum fizikai rendszereket építhetünk fel egyesítéssel:

$$\mathbf{V}_0 \otimes \mathbf{V}_1 \otimes \dots \otimes \mathbf{V}_k.$$

A fentieket a példánkon szemléltetjük. $n \cdot m$ darab alapállapot van:

$|x_0\rangle \otimes |y_0\rangle$ azt jelenti, hogy az első részecske az x_0 pontban van, a második részecske az y_0 pontban van.

:

$|x_0\rangle \otimes |y_{m-1}\rangle$ azt jelenti, hogy az első részecske az x_0 pontban van, a második részecske az y_{m-1} pontban van.

:

$|x_{n-1}\rangle \otimes |y_0\rangle$ azt jelenti, hogy az első részecske az x_{n-1} pontban van, a második részecske az y_0 pontban van.

:

$|x_{n-1}\rangle \otimes |y_{m-1}\rangle$ azt jelenti, hogy az első részecske az x_{n-1} pontban van, a második részecske az y_{m-1} pontban van.

Az általános állapotvektort a fenti alapállapot vektorok szuperpozíciójaként írjuk fel:

$$|\psi\rangle = c_{00}|x_0\rangle \otimes |y_0\rangle + \dots + c_{ij}|x_i\rangle \otimes |y_j\rangle + \dots + c_{n-1,n-1}|x_{n-1}\rangle \otimes |y_{m-1}\rangle$$

$|\psi\rangle$ egy vektor az $n \cdot m$ dimenziós $\mathbf{C}^{n \cdot m}$ vekortérben.

Példa 3.7 Legyen $n = 2$ és $m = 2$ a fenti két részecske példában. Eképpen a $\mathbf{C}^4$ vekortért tekintjük, az

$$\{ |x_0\rangle \otimes |y_0\rangle, |x_0\rangle \otimes |y_1\rangle, |x_1\rangle \otimes |y_0\rangle, |x_1\rangle \otimes |y_1\rangle \}$$

bázissal. Tekintsük a

$$|\psi\rangle = i|x_0\rangle \otimes |y_0\rangle + (1-i)|x_0\rangle \otimes |y_1\rangle + 2|x_1\rangle \otimes |y_0\rangle + (-1-i)|x_1\rangle \otimes |y_1\rangle$$

állapotvektort! Mennyi a valószínűsége annak, hogy az első részecskét az x_1 pontban, a második részecskét az y_1 pontban találjuk? Az egy részecskéből álló rendszerhez hasonlóan járunk el:

$$p(x_1, y_1) = \frac{|-1-i|^2}{|i|^2 + |1-i|^2 + |2|^2 + |-1-i|^2} = \frac{2}{9}.$$

Példa 3.8 Legyen $n = 2$ és $m = 2$ a fenti két részecske példában. Eképpen a $\mathbf{C}^4$ vekortért tekintjük, az

$$\{ |x_0\rangle \otimes |y_0\rangle, |x_0\rangle \otimes |y_1\rangle, |x_1\rangle \otimes |y_0\rangle, |x_1\rangle \otimes |y_1\rangle \}$$

bázissal. Tekintsük a

$$|\psi\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$$

állapotot! Azaz

$$|\psi\rangle = |x_0\rangle \otimes |y_0\rangle + 0|x_0\rangle \otimes |y_1\rangle + 0|x_1\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$$

Vajon fel tudjuk-e írni $|\psi\rangle$ állapotvektort a két rendszer egy-egy állapotvektorának tenzor szorzataként? Látni fogjuk, hogy nem. Indirekt bizonyítást adunk. Tegyük fel, hogy $|\psi\rangle$ állapotvektort fel tudjuk írni a két rendszer egy-egy állapotvektorának tenzor szorzataként. Az első rendszer részecskéjét reprezentáló állapotvektor

$$c_0|x_0\rangle + c_1|x_1\rangle$$

alakú. A második rendszer részecskéjét reprezentáló állapotvektor

$$d_0|y_0\rangle + d_1|y_1\rangle$$

alakú. Feltevésünk szerint

$$\begin{aligned}\psi &= (c_0|x_0\rangle + c_1|x_1\rangle) \otimes (d_0|y_0\rangle + d_1|y_1\rangle) = \\ &= c_0d_0|x_0\rangle|y_0\rangle + c_0d_1|x_0\rangle|y_1\rangle + c_1d_0|x_1\rangle|y_0\rangle + c_1d_1|x_1\rangle|y_1\rangle.\end{aligned}$$

Mivel $|\psi\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$, azt kapjuk, hogy

$$c_0d_0 = 1, c_0d_1 = 0, c_1d_0 = 0 \text{ és } c_1d_1 = 1.$$

Mivel $c_0d_1 = 0$, így $c_0 = 0$ vagy $d_1 = 0$. Ha $c_0 = 0$, akkor $c_0d_0 = 0$. Ha $d_1 = 0$, akkor $c_1d_1 = 0$. Mindkét esetben ellentmondásra jutottunk.

Tekintsük a $|\psi\rangle$ állapotvektort! Mi történik akkor ha az első részecskét megmérjük? 50% az esélye annak, hogy az $|x_0\rangle$ állapotban azaz az x_0 pozíción találjuk és 50% az esélye annak hogy az $|x_1\rangle$ állapotban azaz az x_1 pozíción találjuk. Tegyük fel, hogy az első részecskét az x_0 pozíción találjuk. Mivel az

$|x_0\rangle|y_1\rangle$ kifejezés együtthatója 0, így a második részecske nincsen az y_1 pozíción, azaz az y_0 pozíción van. Tegyük fel, hogy az első részecskét az x_1 pozíción találjuk. Mivel az $|x_1\rangle|y_0\rangle$ kifejezés együtthatója 0, így a második részecske nincsen az y_0 pozíción, azaz az y_1 pozíción van. A két részecskére szimmetrikus a $|\psi\rangle$ állapotvektor.

Szeperálható állapotnak hívjuk azt az állapotot, ami a két alkotó rendszer egy-egy állapotának tenzor szorzataként áll elő. Összefonódott állapotnak hívjuk azt az állapotot, ami nem áll elő a két alkotó rendszer egy-egy állapotának tenzor szorzataként áll elő.

3.4. Kvantum állapotok

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

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

A hagyományokat követve feltesszük hogy a $|\psi_a\rangle$ állapotvektorra

$$\langle\psi_a|\psi_a\rangle = 1. \text{ Ezért}$$

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

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 $|\psi_a\rangle$ 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 $\langle\psi_a|\psi_b\rangle = 1$ egyenlőséget úgy értelmezzük hogy $|\psi_a\rangle$ és $|\psi_b\rangle$ ugyanazokat az állapotokat reprezentálják.

Definíció 3.9 Azt mondjuk hogy egy állapot lineáris kombinációja más állapotoknak ha az őt reprezentáló $|\psi_a\rangle$ ket vektor lineáris kombinációja az ezen állapotokat reprezentáló $|\psi\rangle$ ket vektoroknak.

4. Kvantum fizikai változó

A kvantum fizikai rendszer mérhető tulajdonságát kvantum 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 4.1 Az $\mathbf{U}$ operátor a $\mathcal{H}_n$ Hilbert térben

- Hermite-féle (önadjungált) ha $\mathbf{U} = \mathbf{U}^\dagger$

Ez ekvivalens azzal hogy $\mathbf{U}$ -nak az U mátrixára igaz hogy $U^\dagger = U$.

- unitér ha $\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$.

Ez ekvivalens azzal hogy $\mathbf{U}$ -nak az a U mátrixa unitér. (Az U $n \times n$ -es mátrixot unitérnek nevezzük ha $UU^\dagger = U^\dagger U = I_n$, ahol I_n az $n \times n$ -es egység mátrix.)

- normális ha $[\mathbf{U}, \mathbf{U}^\dagger] = \mathbf{U}\mathbf{U}^\dagger - \mathbf{U}^\dagger\mathbf{U} = \mathbf{0}$

Itt $\mathbf{U}^\dagger$ az $\mathbf{U}$ adjungáltja, $\mathbf{I}$ az azonosság operátor.

Állítás 4.2 Minden Hermite-féle operátor normális.

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.

$$|\psi_b\rangle = \mathbf{U}|\psi_a\rangle$$

$$\langle\psi_b| = \langle\psi_a|\mathbf{U}.$$

Az $\mathbf{U}$ unitér lineáris operátorra:

$$\mathbf{U}(a|\psi_a\rangle + b|\psi_b\rangle) = a\mathbf{U}|\psi_a\rangle + b\mathbf{U}|\psi_b\rangle.$$

A $|\psi_a\rangle$ állapot vektort a $\{|0\rangle, \dots, |i\rangle, \dots, |n-1\rangle\}$ bázis állapotok lineáris kombinációjaként tudjuk kifejezni az alábbi módon:

$$|\psi_a\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle,$$

itt α_i , $0 \leq i \leq n-1$ komplex számot állapot amplitúdónak nevezzük.

Igazoljuk hogy $\alpha_j = \langle j|\psi_a\rangle$. Képezzük a belső szorzatot a $\langle j|$ bra állapot vektorral:

$$\langle j|\psi_a\rangle = \langle j|\sum_{i=0}^{n-1} \alpha_i |i\rangle = \sum_{i=0}^{n-1} \alpha_i \langle j|i\rangle = \alpha_j.$$

Az alábbi feladatnak több, egymással ekvivalens megoldását adjuk.

Feladat: adott egy $\mathbf{A}$ operátor amely az n dimenziós Hilbert térből képez az k dimenziós Hilbert térbe. Határozzuk meg a hozzá tartozó $A_{k \times n}$ mátrixot.

A külső szorzatot operátornak fogjuk fel, definíció szerint. Vegyük észre hogy $\sum_{i=0}^{n-1} |i\rangle\langle i| = \mathbf{I}_{n \times n}$, ahol $\mathbf{I}_{n \times n}$ az identitás (azonosság) leképezés az n dimenziós Hilbert tér felett. Ezért

$$\mathbf{A} = \mathbf{I}_{k \times k} \mathbf{A} \mathbf{I}_{n \times n} =$$

$$\begin{aligned}
&= \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} |j\rangle \langle j|\mathbf{A}|i\rangle \langle i| = \\
&\quad (\text{most megcseréljük a } |j\rangle \text{ ket vektor és a } \langle j|\mathbf{A}|i\rangle \text{ komplex szám sorrendjét}) \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} \langle j|\mathbf{A}|i\rangle |j\rangle \langle i|.
\end{aligned}$$

Ez az A mátrix külső szorzattal való megadása. Az A mátrix j -edik sorában és i -edik oszlopában a $\langle j|\mathbf{A}|i\rangle$ komplex szám van. A $|j\rangle \langle i|$ külső szorzat eredménye egy olyan mátrix amelynek j -edik sorában és i -edik oszlopában 1 van, az összes többi helyén 0. Tehát az $\mathbf{A}$ operátorhoz tartozó mátrix $A = [a_{ji}]$ alakú, ahol $a_{ji} = \langle j|\mathbf{A}|i\rangle$, $0 \leq j \leq k-1$, $0 \leq i \leq n-1$.

Feladat: adott egy $\mathbf{U}$ operátor amely n dimenziós Hilbert térből képez az k dimenziós Hilbert térbe. Határozzuk meg a hozzá tartozó $U_{k \times n}$ mátrixot.

Tekintsük a két dimenziós $\mathcal{H}_2$ Hilbert teret a $|0\rangle, |1\rangle$ bázissal. Tekintsük az alábbi függvényt:

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Tehát $\mathbf{U}$ operátor felcseréli az állapot vektor $|0\rangle$ -ra és $|1\rangle$ -re való vetületét.

$$u_{00} = \langle 0|\mathbf{U}|0\rangle = \langle 0|1\rangle = 0.$$

$$u_{01} = \langle 0|\mathbf{U}|1\rangle = \langle 0|0\rangle = 1.$$

$$u_{10} = \langle 1|\mathbf{U}|0\rangle = \langle 1|1\rangle = 1.$$

$$u_{11} = \langle 1|\mathbf{U}|1\rangle = \langle 1|0\rangle = 0.$$

$$\text{Tehát } U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|\psi_b\rangle = U|\psi_a\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_0 \end{pmatrix} = \alpha_1|0\rangle + \alpha_0|1\rangle$$

Továbbá,

$$\langle \psi_b | = \langle \psi_a | U$$

$$\text{Tehát } (\alpha_0^*, \alpha_1^*) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (\alpha_1^* \ \alpha_0^*) = \alpha_1^* \langle 0 | + \alpha_0^* \langle 1 |$$

Feladat: adott egy $\mathbf{U}$ operátor amely n dimenziós Hilbert térből képez az k dimenziós Hilbert térbe. Határozzuk meg a hozzá tartozó $U_{k \times n}$ mátrixot.

Most megadunk egy másik képletet is. Figyeljük meg hogy $I_{n \times n} = \sum_{j=0}^{n-1} |j\rangle \langle j|$. Szorozzuk meg balról mind két oldalt az $U_{n \times n}$ mátrixszal. Így azt kapjuk hogy

$$U = UI = U(\sum_{j=0}^{n-1} |j\rangle \langle j|) = \sum_{j=0}^{n-1} (U|j\rangle) \langle j|.$$

Tehát

$$U = \sum_{j=0}^{n-1} (U|j\rangle) \langle j|.$$

Sokszor ezt a képletet fogjuk használni a továbbiakban.

Bevezetjük a projekció operátor (projektor) fogalmát.

Definíció 4.3 Tetszőleges $|\psi_a\rangle$ állapot vektor önmagával való külső szorzatát projekció operátornak (projektornak) nevezzük.

$$|\psi_a\rangle \langle \psi_a| = \mathbf{P}_{\psi_a}.$$

Szemléletesen tetszőleges $|\psi_b\rangle$ vektornak a $|\psi_a\rangle$ állapotvektor által kifeszített résztérre való vetületét adja eredményül a $\mathbf{P}_{\psi_a}$ projekció operátor alkalmazása a ψ_b vektorra.

Emlékezzünk hogy tetszőleges $|\psi_a\rangle$ állapotvektor hossza 1. Ezért tetszőleges $|\psi_a\rangle$ állapotvektorra $\langle \psi_a | \psi_a \rangle = 1$. A projekció operátor az alábbi tulajdonsággal rendelkezik:

$$(\mathbf{P}_{\psi_a})^2 = |\psi_a\rangle \langle \psi_a | |\psi_a\rangle \langle \psi_a| = |\psi_a\rangle \langle \psi_a | \psi_a \rangle \langle \psi_a| = |\psi_a\rangle \langle \psi_a| = \mathbf{P}_{\psi_a}.$$

Azt mondjuk hogy a $\mathbf{P}_1$ és $\mathbf{P}_2$ projektorok merőlegesek egymásra (ortogonálisak) ha a Hilbert tér minden $|\psi_a\rangle \in \mathcal{H}_n$ állapotára $\mathbf{P}_1\mathbf{P}_2|\psi_a\rangle = \mathbf{0}$. Ez ekvivalens azzal hogy a projekcióknak rendre megfelelő P_1 és P_2 mátrixok szorzata olyan mátrix amelynek minden eleme 0. Azaz $P_1P_2 = \mathbf{0}$.

4.1. A fizikai változó spektrális felbontása

Definíció 4.4 Legyen $|\psi\rangle$ egy vektor és legyen $\mathbf{U}$ egy normális operátor $\mathcal{H}_n$ -ben. Azt mondjuk hogy $|\psi\rangle$ az $\mathbf{U}$ sajátvektora és λ az $\mathbf{U}$ -nak a $|\psi\rangle$ -hez tartozó saját értéke ha

$$U|\psi\rangle = \lambda|\psi\rangle.$$

Az I azonosság operátor sajátértéke az 1 szám. $I|\psi\rangle = 1|\psi\rangle$.

Az $U|\psi\rangle = \lambda|\psi\rangle$ egyenlőség az alábbi alakban is írható:

$$U|\psi\rangle = \lambda I|\psi\rangle. \text{ Azaz, } (U - \lambda I)|\psi\rangle = 0. \text{ Legyen}$$

$$\{ |e_0\rangle, |e_1\rangle, \dots, |e_i\rangle, \dots, |e_{n-1}\rangle \}$$

egy ortonormális bázis $\mathcal{H}_n$ -ben, és legyen

$|\psi\rangle = \sum_{i=0}^{n-1} \gamma_i |e_i\rangle$. Ekkor az $(U - \lambda I)|\psi\rangle = \mathbf{0}$ egyenlőség az alábbi alakban is írható:

$$(U - \lambda I) \sum_{i=0}^{n-1} \gamma_i |e_i\rangle = \mathbf{0}$$

Legyen $U = u_{ij}$. Tudjuk hogy $I = \delta_{ij}$. Tehát

$$\sum_{j=0}^{n-1} (u_{ij} - \lambda \delta_{ij}) \gamma_j = 0, \quad i = 1, 2, \dots, n-1.$$

Adott λ sajátértékhez tartozó sajátvektort úgy kapjuk meg hogy megoldjuk a fenti n ismeretlenes n egyenletből álló egyenletrendszert.

Posztulátum 4.5 Tekintsük a $\mathcal{H}_n$ Hilbert teret. A fizikai változó egy olyan Hermite-féle operátor amelynek a sajátvektorai bázist alkotnak.

Posztulátum 4.6 1. A fizikai változó sajátértékei valós számok.

2. Különböző sajátvektorokhoz különböző sajátértékek tartoznak. A fizikai változó két különböző sajátértékéhez tartozó sajátvektora merőleges egymásra.

3. A fizikai változó sajátvektorai ortonormális bázist alkotnak $\mathcal{H}_n$ -ben.

4. Tetszőleges két kommutatív (felcserélhető) fizikai változó sajátvektorainak a halmaza megegyezik egymással. Ezt sajátvektor bázisnak nevezzük.

A fenti 1. 2. 3. pontokat újra megfogalmazzuk.

Posztulátum 4.7 A $\mathcal{H}_n$ Hilbert térben minden U fizikai változónak van n sajátvektora: $|u_i\rangle$, $0 \leq i \leq n-1$. Továbbá $\{|u_0\rangle, |u_1\rangle, \dots, |u_i\rangle, \dots, |u_{n-1}\rangle\}$ egy ortonormális bázis $\mathcal{H}_n$ -ben. Az $|u_i\rangle$ sajátvektorhoz tartozik a λ_i sajátérték valós szám, $U|u_i\rangle = \lambda_i|u_i\rangle$, $0 \leq i \leq n-1$. Minden $1 \leq i < j \leq n$ esetén, $\lambda_i \neq \lambda_j$.

Minden $|\psi_a\rangle \in \mathcal{H}_n$ állapot vektort felírhatunk az

$\{|u_0\rangle, |u_1\rangle, \dots, |u_i\rangle, \dots, |u_{n-1}\rangle\}$ ortonormális bázissal.

$$|\psi_a\rangle = \sum_{i=0}^{n-1} \alpha_i |u_i\rangle.$$

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

$$U|\psi_a\rangle = U \sum_{i=0}^{n-1} \alpha_i |u_i\rangle = \sum_{i=0}^{n-1} \alpha_i U|u_i\rangle = \sum_{i=0}^{n-1} \alpha_i \lambda_i |u_i\rangle.$$

Tekintsük a

$$\mathbf{P}_i = |u_i\rangle\langle u_i|, 0 \leq i \leq n-1.$$

projekció operátorokat. Alkalmazzuk a $\mathbf{P}_i$ projekció operátort a $|\psi_a\rangle$ állapotvektorra.

$$\mathbf{P}_i|\psi_a\rangle = |u_i\rangle\langle u_i|\sum_{j=0}^{n-1}\alpha_j|u_j\rangle = \sum_{j=0}^{n-1}\alpha_j|u_i\rangle(\langle u_i|u_j\rangle) = \alpha_i|u_i\rangle$$

mivel $\langle u_i|u_j\rangle = \delta_{ij}$ $0 \leq i, j \leq n-1$.

$\mathbf{P}_i|\psi_a\rangle$ -t helyettesítjük $\alpha_i|u_i\rangle$ helyébe az $U|\psi_a\rangle$ bal oldalú egyenlőségben:

$$U|\psi_a\rangle = \sum_{i=0}^{n-1}\alpha_i\lambda_i|u_i\rangle = \sum_{i=0}^{n-1}\lambda_i\mathbf{P}_i|\psi_a\rangle.$$

$$\text{Tehát } U = \sum_{i=0}^{n-1}\lambda_i\mathbf{P}_i.$$

A fenti képlet az U fizikai változó spektrális dekompozíciója (felbontása). A fenti képlet teljesül minden $|\psi_a\rangle$ állapotvektorra. Az U fizikai változó spektrális dekompozíciója független a bázis megválasztásától. Az U fizikai változó spektrális dekompozíciója az U fizikai változó kimerítő (teljes) mérését adja meg.

Példa $n = 2$. Tekintsük az U fizikai változót a λ_a és λ_b sajátértékekkel és az ortonormális $|a\rangle, |b\rangle$ sajátvektorral. Itt $|a\rangle, |b\rangle$ sajátvektorok a $\mathcal{H}_2$ tér bázisát alkotják.

$$|a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

$$|b\rangle = \beta_0|0\rangle + \beta_1|1\rangle \mapsto \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$$

A fenti sajátvektorokhoz tartozó projekció operátorokat az alábbi módon írhatjuk fel:

$$\mathbf{P}_a = |a\rangle\langle a| = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} (\alpha_0^* \alpha_1^*) = \begin{pmatrix} |\alpha_0|^2 & \alpha_0 \alpha_1^* \\ \alpha_1 \alpha_0^* & |\alpha_1|^2 \end{pmatrix}$$

$$\mathbf{P}_b = |b\rangle\langle b| = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} (\beta_0^* \beta_1^*) = \begin{pmatrix} |\beta_0|^2 & \beta_0 \beta_1^* \\ \beta_1 \beta_0^* & |\beta_1|^2 \end{pmatrix}$$

Az $\mathbf{U}$ fizikai változó mátrixa:

$$U = \lambda_a \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} (\alpha_0^* \alpha_1^*) + \lambda_b \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} (\beta_0^* \beta_1^*).$$

$$U = \lambda_a \begin{pmatrix} |\alpha_0|^2 & \alpha_0 \alpha_1^* \\ \alpha_1 \alpha_0^* & |\alpha_1|^2 \end{pmatrix} + \lambda_b \begin{pmatrix} |\beta_0|^2 & \beta_0 \beta_1^* \\ \beta_1 \beta_0^* & |\beta_1|^2 \end{pmatrix}.$$

4.2. A 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 $\mathbf{U}$ -nak az $|u_i\rangle$ sajátállapota (sajátvektora) és a megmért érték a λ_i sajátérték. A kvantumfizika állítja hogy a páronként egymást kizáró mérési végeredmények megfelelnek valamely $\{\mathbf{P}_0, \mathbf{P}_1, \dots, \}$ páronként merőleges projekció operátoroknak.

Definíció 4.8 A $\mathcal{H}_n$ Hilbert térben egy

$$\{\mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_i, \dots, \mathbf{P}_{m-1}\}$$

ortogonális projekció operátorok halmazáról azt mondjuk hogy teljes ha $\sum_{i=0}^{m-1} \mathbf{P}_i = \mathbf{I}$.

Itt $\mathbf{I}$ az identitás mátrix.

Igazolható hogy a fenti definícióban $m \leq n$. A kvantum operátor spektrális felbontása alapján amikor az $\mathcal{U}$ fizikai változót megmérjük, akkor a

$$\{ \mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_i, \dots, \mathbf{P}_{m-1} \}$$

teljes ortogonális projekció operátor halmazt mérjük meg. A λ_i sajátértéket a $\mathbf{P}_i$ projekcióval társítjuk, $1 \leq i \leq n$. Annak a valószínűsége hogy λ_i -t kapunk a mérés eredményéül, amikor $|\psi_a\rangle$ állapotban volt a fizikai rendszer közvetlenül a mérés előtt:

$$Prob(\psi_a, \lambda_i) = \langle \psi_a | P_i | \psi_a \rangle.$$

Mivel a projekció halmaz teljes,

$$\sum_{i=0}^{m-1} Prob(\psi_a, \lambda_i) = 1.$$

Ha λ_i a végeredmény, akkor a mérés után kapott állapot:

$$\frac{\mathbf{P}_i |\psi_a\rangle}{\sqrt{\langle \psi_a | \mathbf{P}_i | \psi_a \rangle}}$$

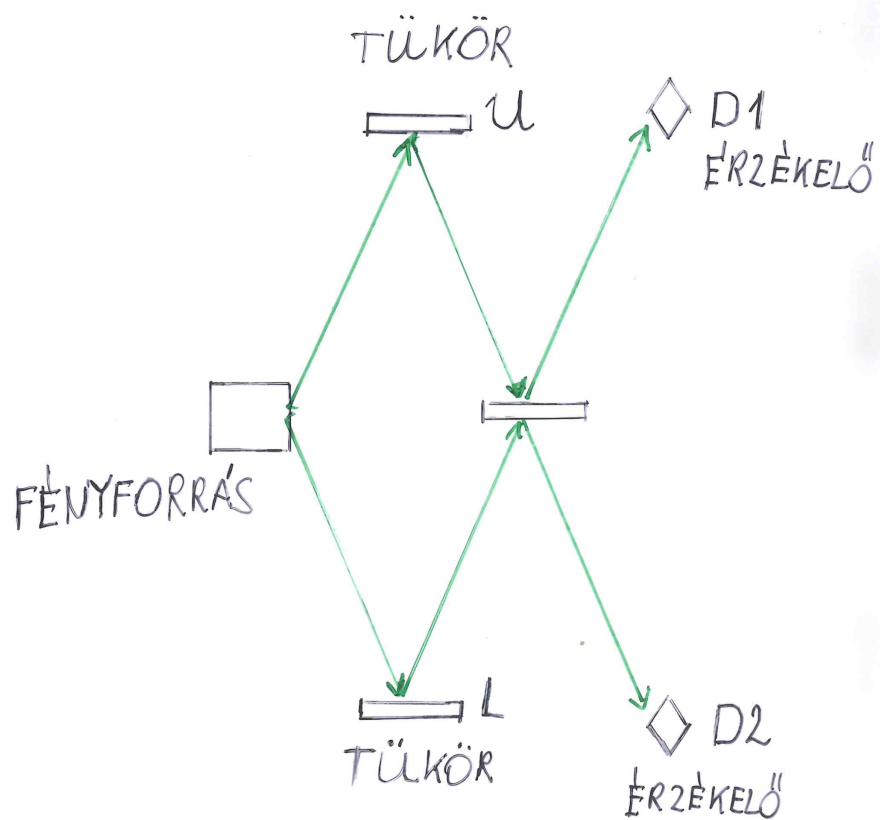
4.3. Két foton viselkedésének véletlen megegyezése, kísérlet

A kísérletet az 1. ábrán mutatjuk be.

Két fotont generálnak egyidejűleg két különböző sugárban. Mind a két sugarat egy-egy visszaverő tükör alkalmazásával ugyanahhoz a fényosztóhoz (beam splitter) irányítják. Amikor a fényosztóhoz ér, minden egyes fotonnak 50% esélye van arra hogy áthaladjon és 50% esélye van arra hogy visszaverődjön.

A klasszikus fizika világában két lehetséges végeredmény van:

1. A két fotonnak különböző a sorsa: az egyik visszaverődik, a másikat átengedi a fényosztó. Mind a két foton a $D1$ érzékelőnél



1. ábra. Két fotont generálnak egyidejűleg két különböző sugárban.

köt ki vagy mind a két foton a $D2$ érzékelőnél köt ki. Amikor az U tükörből érkező fotont visszaveri a fényosztó és az L tükörből érkező fotont átengedi a fényosztó, akkor mind a két foton a $D1$ érzékelőnél köt ki. Fordítva, amikor az U tükörből érkező fotont átengedi a fényosztó és az L tükörből érkező fotont visszaveri a fényosztó, akkor mind a két foton a $D2$ érzékelőnél köt ki.

2. A két fotonnak ugyanaz a sorsa: mind a kettőt visszaveri a fényosztó vagy mind a kettőt átengedi a fényosztó. Ebben az esetben mind $D1$ érzékelő mind $D2$ érzékelő egy fotont érzékel. Amikor mind a két fotont átengedi a fényosztó az akkor az U tükörből érkező foton a $D2$ detektornál köt ki, és az L tükörből érkező foton a $D1$ detektornál köt ki. Amikor mind a két fotont visszaveri a fényosztó akkor az U tükörből érkező foton a $D1$ detektornál köt ki, és az L tükörből érkező foton a $D2$ detektornál köt ki.

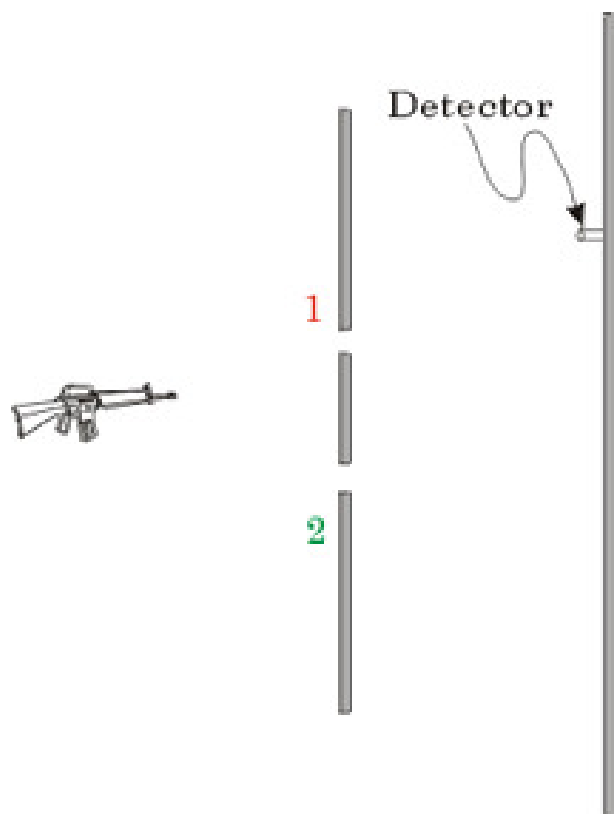
A valóságban a második végeredmény nem fordul elő. Gondosan elvégzett laboratóriumi kísérleteknél a második végeredményt mintegy 10^{-4} valószínűséggel észlelték.

Amikor egy fotont bocsátunk ki akkor ugyanannyi a valószínűsége hogy $D1$ érzékeli mint annak a valószínűsége hogy $D2$ érzékeli.

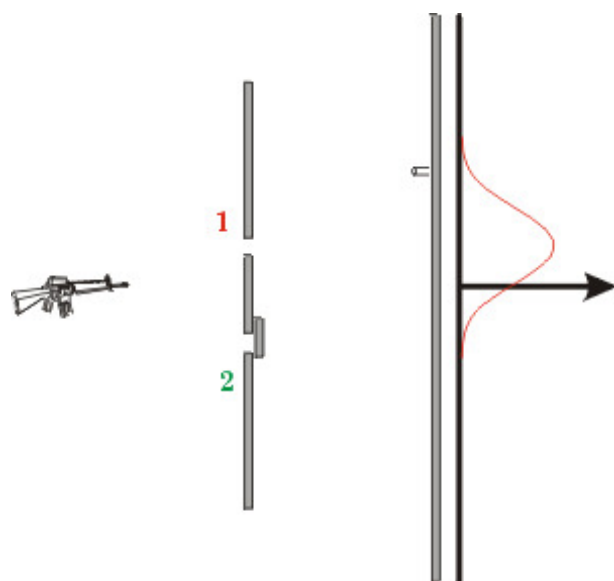
4.4. Kétrés kísérlet

Kettő darab kétrés kísérletet tekintünk. Az elsőben golyók, a másodikban víz hullámok szerepelnek.

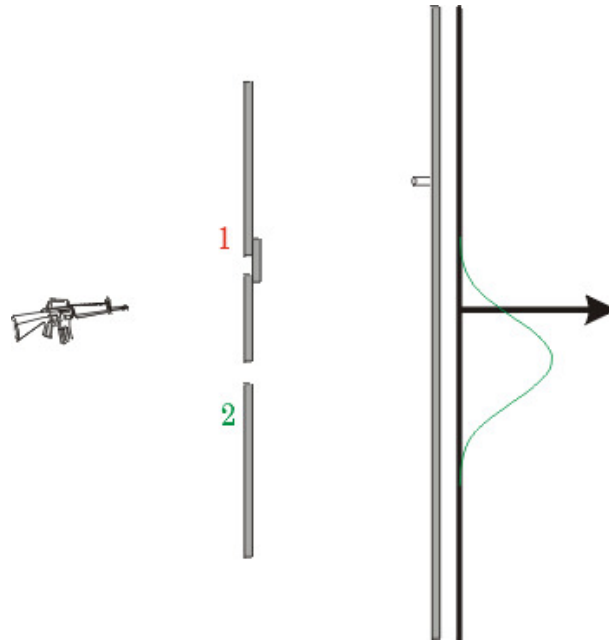
Az első kísérletben egy puska lő golyókat véletlenszerűen,
Két rés van a falon 1 és 2. A golyók átmennek a két résen,



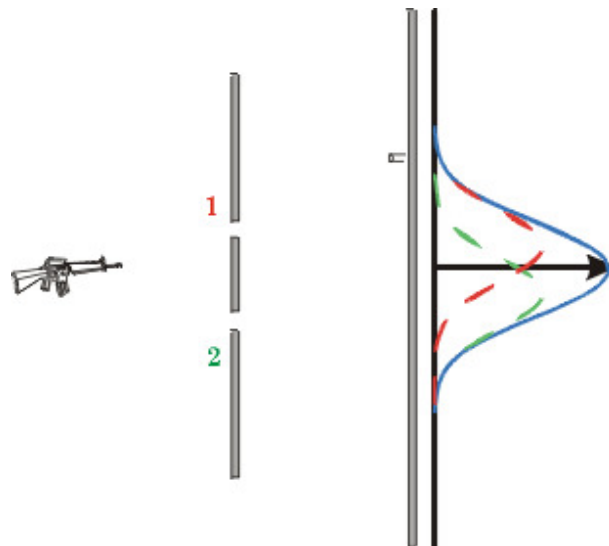
2. ábra. Kétrés kísérlet puskával [7]



3. ábra. Kétrés kísérlet puskával, első rés nyitva van [7]



4. ábra. Kétrés kísérlet puskával, második rés nyitva van [7]



5. ábra. Kétrés kísérlet puskával, mindkét rés nyitva van [7]

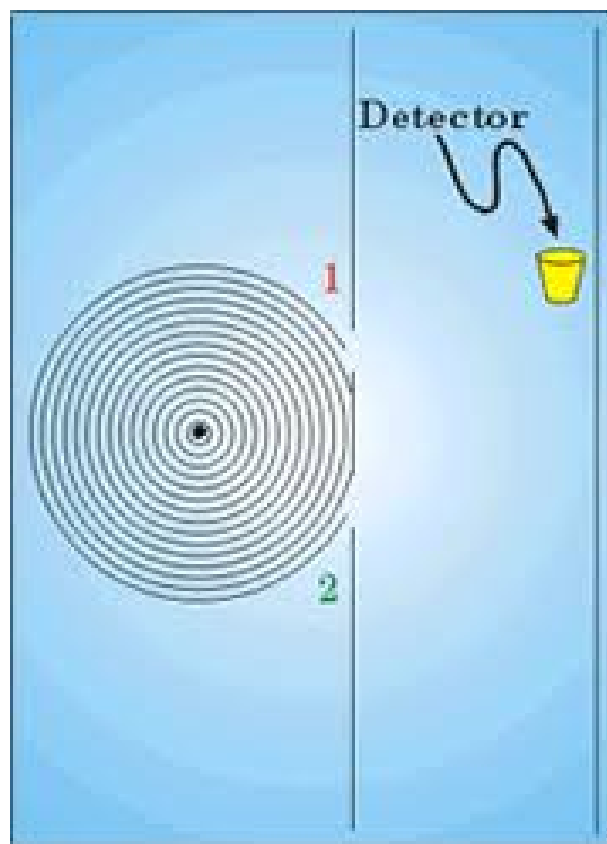
némelyik megpattan a rések falán. Mindegyiket felfogja a hátsó fal. Három alkalommal végezzük el a kísérletet. Az első alkalommal az 1 (első) rés van nyitva. A második alkalommal a 2 Egy elektron puska elektronokat lő ki. (második) rés van nyitva. A harmadik alkalommal mind a kettő rés nyitva van. Mind a három kísérletnél egy mozgatható érzékelőt helyezünk el a hátsófal aljánál, (a hátsófal alja az $x = x_{min}$ helyen van), és n golyót lövünk ki. Majd megszámloljuk hogy hány golyó érte el az érzékelőt. Utána az érzékelőt egy új helyre mozgatjuk, és n golyót lövünk ki, majd megszámloljuk hogy hány golyó érte el az érzékelőt. Ezt az eljárást addig folytatjuk amíg a hátsó fal tetejét el nem érjük. A hátsó fal teteje az $x = x_{max}$ helyen van.

$I_1(x)$, $I_2(x)$, és $I_{1+2}(x)$ jelöli az x helyen egységnyi idő alatt érzékelt golyók számát rendre amikor az 1 nyílás nyitva van, amikor a 2 nyílás nyitva van, és amikor mind a két nyílás nyitva van.

Megfigyeljük hogy minden $x_{min} \leq x \leq x_{max}$ esetén, $I_{1+2}(x) = I_1(x) + I_2(x)$. Az x helyen egységnyi idő alatt érzékelt golyók számát elosztjuk az egységnyi idő alatt kilőtt golyók számával. Az így kapott számok $P_1(x)$, $P_2(x)$, és $P_{1+2}(x)$ jelölik annak a valószínűségét hogy x helyen golyót érzékelünk amikor egy golyót kilövünk, rendre amikor az 1 nyílás nyitva van, amikor a 2 nyílás nyitva van, és amikor mind a két nyílás nyitva van. Megfigyeljük hogy minden $x_{min} \leq x \leq x_{max}$ esetén, $P_{1+2}(x) = P_1(x) + P_2(x)$. A valószínűségek összeadódnak.

A második kísérletünknel egy hullámforrás hullámokat kelt a

vizen, lásd 6, 7, 8 és 9 ábrák.



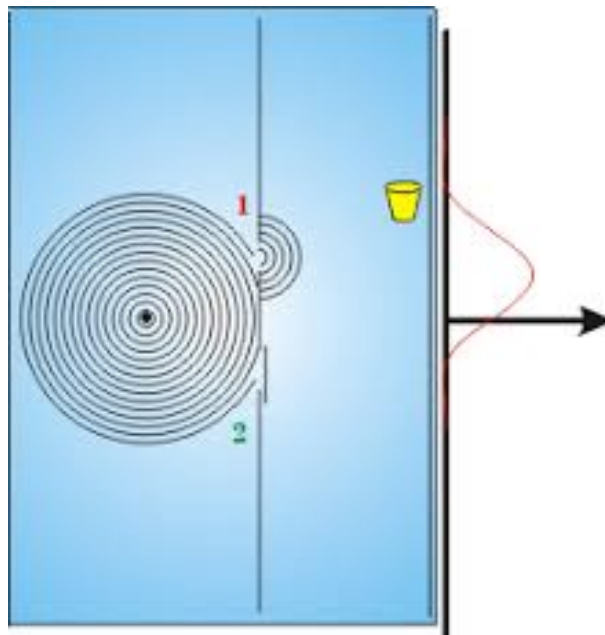
6. ábra. Kétrés kísérlet vízzel [7]

A hullámok elérik az akadályfalat, áthatolnak a réseken és elérik a mozgó érzékelőt. A második fal elnyeli a hullámokat. Az érzékelő a második fal mögött van. Így elkerüljük a hullámvisszaverődést.

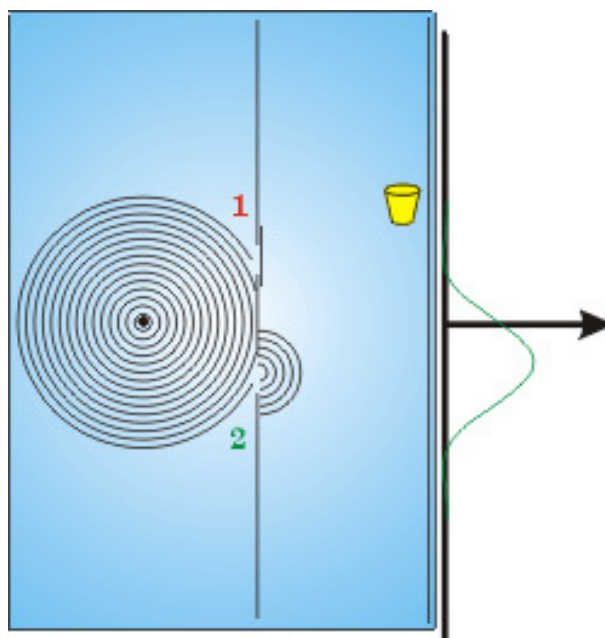
Ha nincsen akadályfal, akkor az érzékelőt x helyen elérő víz magassága egyenlő az alábbi kifejezés valós részével:

$$magas(t) = \beta e^{i\omega t} = \beta(\cos \omega t + i \sin \omega t).$$

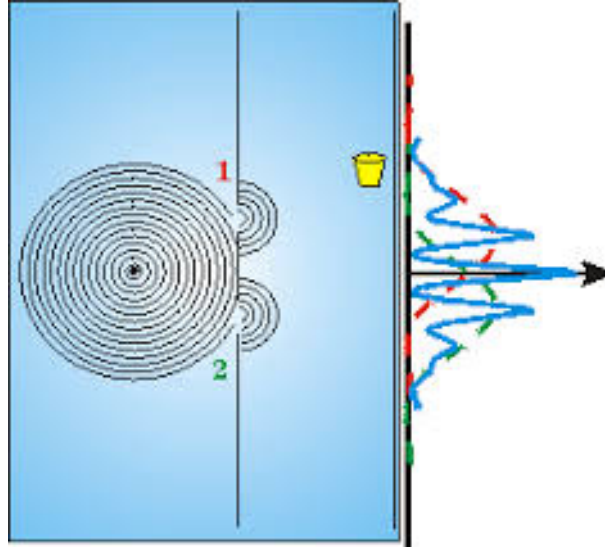
Itt β jelöli az amplitúdót, ω a hullám szögfrekvenciája, t az idő. A fenti függvény az x helytől függ, és komplex számot vesz fel értékül. A hullám intenzitása: $I = |\beta|^2$, azaz a komplex szám abszolút értékének a négyzete.



7. ábra. Kétrés kísérlet vízzel, első rés nyitva van [7]



8. ábra. Kétrés kísérlet vízzel, második rés nyitva van [7]



9. ábra. Kétrés kísérlet vízzel, mindkét rés nyitva van [7]

Három alkalommal végezzük el a kísérletet. Az első alkalommal az 1 rés van nyitva. A második alkalommal a második rés van nyitva. A harmadik alkalommal mind a kettő rés nyitva van.

1. kísérlet: Az 1 résen keresztül jövő víznek a detektornál a magassága $\beta_a e^{i\omega t}$ és az intenzitása $I_1 = |\beta_a|^2$. 2. kísérlet: A 2 résen keresztül jövő víznek a detektornál a magassága $\beta_b e^{i\omega t}$ és az intenzitása $I_2 = |\beta_b|^2$.

3. kísérlet: Amikor mind a két rés nyitva van, az érzékelőt elérő víz magassága $(\beta_a + \beta_b) e^{i\omega t}$ és az intenzitása $I_{1+2} = |\beta_a + \beta_b|^2$. Itt

$$|\beta_a + \beta_b|^2 = |\beta_a|^2 + |\beta_b|^2 + |\beta_a||\beta_b| \cos \delta$$

ahol δ a fáziskülönbség β_a és β_b között. Eképpen,

$$I_{1+2} = I_1 + I_2 + 2\sqrt{I_1 I_2} \cos \delta.$$

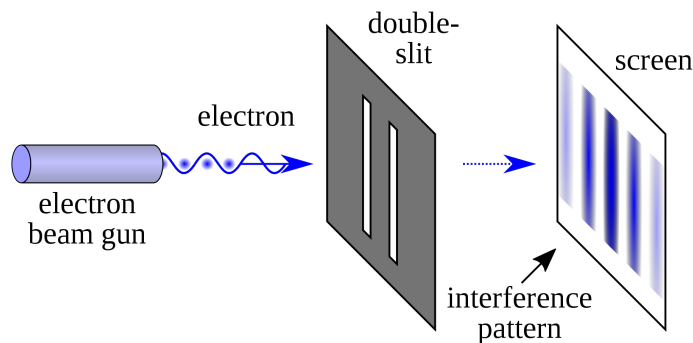
és

$$I_{1+2} \neq I_1 + I_2.$$

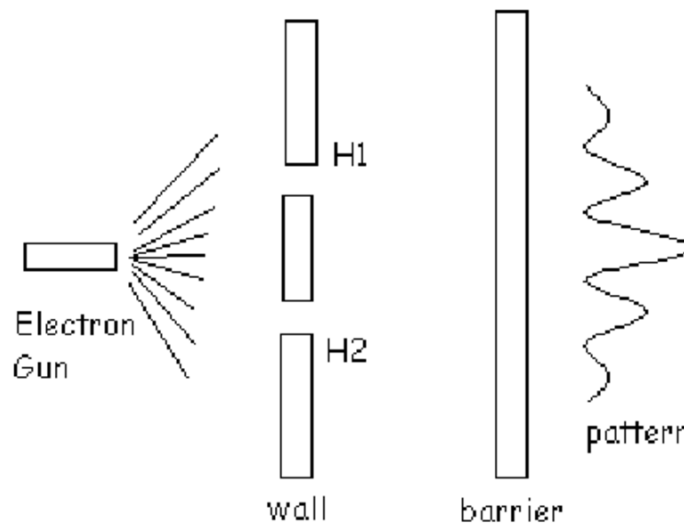
Ebben a kísérletben az 1 és 2 résen áthaladó hullámok inter-

ferenciáját figyeltük meg.

Kísérlet elektronokkal, lásd az 10, 11, ábrákat.



10. ábra. kétrés kísérlet elektronokkal [10]



11. ábra. kétrés kísérlet elektronokkal [2]

Egy elektron puska elektronokat lő ki. Az 1 rés nyitott és az elektronok áthaladhatnak az 1 résen.

A 2 rés nyitott és az elektronok áthaladhatnak a 2 résen

Mind a két rés nyitott és az áthaladhatnak mind a két résen.

A hátsófalán Geiger-számlálóval érzékeljük az elektronokat. Az elektronok egyenként, a golyókhoz hasonlóan érkeznek a Geiger

számlálóhoz. A Geiger számláló kibocsát egy hangot (katt) amikor megérkezik egy elektron a Geiger számlálóhoz, a kattánás erőssége arányos az elektron elektromos töltésével. Különálló kattánást hallunk. Minden kattánás egyformán erős. Ez azt jelenti hogy az elektronok egyenként érkeznek a számlálóhoz, nem pedig csapatosan sem pedig töredék darabokban.

Az első alkalommal az 1 rés van nyitva. A második alkalommal a 2 rés van nyitva. A harmadik alkalommal mind a kettő rés nyitva van.

$I_1(x)$, $I_2(x)$, és $I_{1+2}(x)$ jelöli az x helyen egységnyi idő alatt érzékelt elektronok számát rendre amikor az 1 nyílás nyitva van, amikor a 2 nyílás nyitva van, és amikor mind a két nyílás nyitva van.

Megfigyeljük a kísérlet során hogy $I_{1+2} \neq I_1 + I_2$. Bizonyos helyeken azt látjuk hogy $I_{1+2} < I_1$ és $I_{1+2} < I_2$.

Magyarázat: Az elektronok úgy érkeznek meg mint részecskék. Ezeknek a részecskéknek az érkezése úgy oszlik meg mint a hullámok intenzitása. Mintha minden egyes elektron mindkét résen egyszerre haladna át, és azután sajátmagával interferálna az érzékelőhöz való megérkezésekor.

Az érzékelt elektronok számából kiszámíthatjuk a valószínűségeket. Az x helyen egységnyi idő alatt érzékelt elektronok számát elosztjuk az egységnyi idő alatt kilőtt golyók számával. Az így kapott számok $P_1(x)$, $P_2(x)$, és $P_{1+2}(x)$ jelölik annak a valószínűségét hogy x helyen elektront érzékelünk amikor egy elektront kilövünk, rendre amikor az 1 nyílás nyitva van, amikor a 2 nyílás nyitva van,

és amikor mind a két nyílás nyitva van. Megfigyeljük hogy

$P_{1+2}(x) \neq P_1(x) + P_2(x)$, $x_{min} \leq x \leq x_{max}$ esetén, A valószínűségek nem adódnak össze.

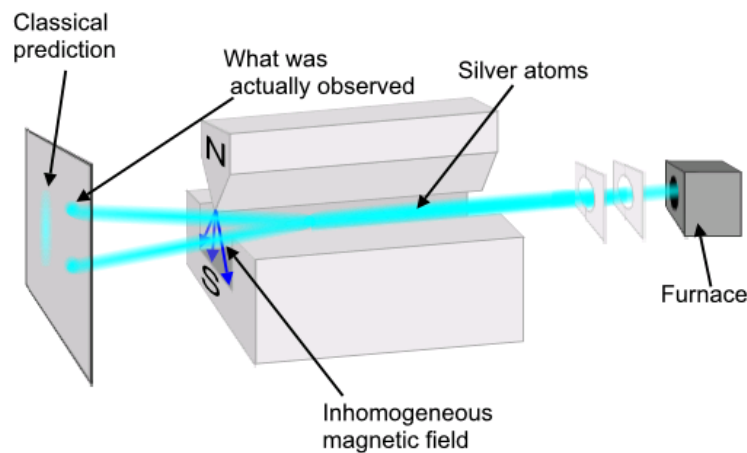
A kvantum kísérlet során valamely esemény bekövetkezésének a valószínűsége: $P = |\alpha|^2$. Itt α egy komplex szám, α -t valószínűségi amplitúdónak nevezzük. Amikor egy esemény több különböző alternatív módon történhet meg, akkor az esemény valószínűségi amplitúdója egyenlő az egyes módok valószínűségi amplitúdójának az összegével. Tegyük fel hogy $P_1 = |\alpha_1|^2$ és $P_2 = |\alpha_2|^2$, ahol α_1 és α_2 komplex számok. Ekkor $P_{1+2} = |\alpha_1 + \alpha_2|^2 \neq P_1 + P_2$.

4.5. Stern-Gerlach kísérlet

Az atommag körül forgó elektron elektromos áramlatot kelt. Ennek az áramlat hatására az atomnak mágneses mezeje van. A Stern-Gerlach kísérleti elrendezésben egy mágnes, asszimetrikus pólusok segítségével, egy inhomogén (nem egységes) mágneses teret kelt. Az egyik pólus közel sík, míg a másik formája ék alakú. Ez az elrendezés olyan inhomogén mágneses teret kelt, melynek z komponense merőleges a majdnem sík alakú pólusra. A mágneses mező x és y tengely menti komponensei elhanyagolhatóak.

Semleges ezüst atomokat lövünk át a mágneses mezőn a mágneses mező gradiensére (irányvektorára) merőlegesen. Minden egyes atom menet közbeni elhajlása az atom mágneses nyomatékától és a mágneses mezőtől függ. Azt várták hogy az atomok mágneses nyomatéka véletlenszerűen minden irányban irányítottak. Ezért

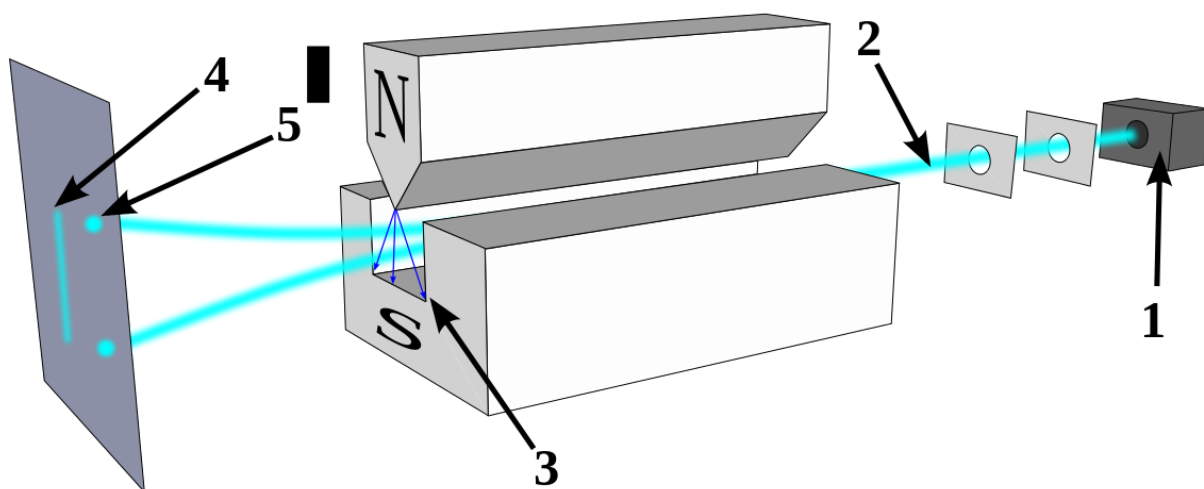
azt várták hogy az atomokat a mágneses mező mindenféle szögben eltéríti, és az ezüst atomok egy folytonos eloszlását kapjuk az elhajlási szög függvényében. Ehelyett csak diszkrét (egymástól elkülönülő) szög halmazban térnek el az atomok. A semleges ezüst atomokat két sugárra választja a mágneses tér. Az egyik sugár felfelé, a másik lefelé tér el. Az érzékelőként használt fényérzékeny lapon két egymástól elkülönülő folt keletkezik, amelyek között nincsen semmi. Ha az atomok klasszikus részecskéként viselkednének, akkor a kép egyetlen nagy folt lenne.



12. ábra. Stern-Gerlach kísérlet elrendezése [15]

A kísérletet megismételték olyan hidrogén atomokkal amelyeknek csupán egy elektronja mozgott az atommag körül. A hidrogén atomok két sugárban (irányban) tértek el a röppályájuktól. Az egyik sugárt felfelé térítette el, a másik sugárt lefelé térítette el a mágneses mező.

Magyarázat. A hidrogén atom elektronjához hozzárendelünk egy fizikai mennyiséget, a spint. A spin az elektron saját, belső impulzusmomentuma. Az elektron mágneses nyomatékának két



13. ábra. Stern-Gerlach kísérlet: ezüst atomok repülnek inhomogén mágneses mezőn keresztül, felfelé vagy lefelé térülnek el a spinjük szerint; (1) tűzhely, (2) ezüst atomok sugara, (3) inhomogén mágneses mező, (4) klasszikus elmélet alapján várt eredmény, (5) megfigyelt eredmény [23]

komponense van. Az elektron atommag körüli forgása okozza az egyik összetevőt. A másik összetevőt az elektron belső forgása, a spin okozza. Az elektron belső mágneses nyomatékát okozza a spin. Az elektron spinje az elektromos töltésének keringése. Ez a mozgás mágneses mezőt gerjeszt amely párhuzamos a keringés tengelyével. A spin véletlenszerűen oszlik el a térben.

A kísérlet során a mágneses mező irányvektora lefelé mutatott és az elektronok kezdeti iránya vízszintes volt. Az inhomogén mágneses tér a mágneses tér irányával párhuzamos erővel hat az elektron belső mágneses momentumára. Az erő nagysága arányos a tér gradiensével (irányvektorával) és a mágneses momentumnak a tér gradiensének irányára eső vetületével. A kísérlet során azok az elektronok tértek el felfelé amelyek spinjének függőleges komponense felfelé mutatott. Azok az elektronok tértek el lefelé amelyek spinjének függőleges komponense lefelé mutatott.

A Stern-Gerlach kísérletben a mérés tengelyét azaz a spin megmérésének a tengelyét az alkalmazott mágneses mező iránya és a részecskék haladási iránya határozta meg. A kísérletben semleges ezüst atomokat használtak. A semleges ezüst atom elektronjainak mágneses nyomatéka páronként nullára összegződnek (páronként semlegesítik egymást) a kimaradó egyetlen (pár nélküli) elektron mágneses nyomatéka lesz az eredő mágneses nyomaték. Ennek az elektronnak a spinje az egész ezüst atom spinje.

A semleges ezüst atomokat két sugárra választja a mágneses tér. Az egyik sugár felfelé, a másik lefelé tér el. Az érzékelőként használt fényérzékeny lapon két egymástól elkülönülő folt keletkezik,

amelyek között nincsen semmi. Ha az atomok klasszikus részecskékként viselkednének, akkor a kép egyetlen nagy folt lenne. A két folt megfelel a spinnek a z tengely mentén lévő két megengedett értékének, amiket '*spin fel*' és '*spin le*' kifejezésekkel jelölhetünk.

Az atom vagy a részecske spinjét leírja az s *spin kvantum szám*. Itt s lehet egy pozitív egész szám vagy egy pozitív egész számnak a fele. Tegyük fel hogy az atomnak vagy a részecskének a spinje s . Vetítsük a részecske spinjét egy tetszőleges tengelyre! A vetület értéke lehet: a

$$-s, -s + 1, \dots, 0, \dots, s - 1, s$$

$2s + 1$ darab szám bármelyike. Az elektron spinje $s = \frac{1}{2}$. A spin vetülete lehet $-\frac{1}{2}$ és $\frac{1}{2}$. A $-\frac{1}{2}$ értéket „*spin le*” a $\frac{1}{2}$ értéket „*spin fel*” -nek nevezzük.

5. A qubit fogalma és fizikai megvalósítása

A kvantum bit (röviden qubit) egy vektor a két dimenziós Hilbert térben. Ebben a vektortérben a ψ vektort

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

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 qubitet akkor a $|0\rangle$ eredményt kapjuk $|\alpha_0|^2$ valószínűséggel és az $|1\rangle$ eredményt kapjuk $|\alpha_1|^2$ valószínűséggel.

A qubit a $|0\rangle$ és $|1\rangle$ között végtelen sok állapotban lehet, amíg

meg nem mérjük. Például a qubit lehet a $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ állapotban és a qubit megmérésekor $\frac{1}{4}$ valószínűséggel 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 $|\psi\rangle$ qubitet 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 Pauli mátrixok által reprezentált operátoroknak a qubitre gyakorolt hatását tanulmányozzuk a következőkben.

1. Az I egység mátrixszal balról való szorzás saját magát rendeli mindkét bázis vektorhoz. σ_0 operátort rendeljük hozzá az I egység mátrixhoz.

2. Az X mátrixszal balról való szorzás a $|0\rangle$ qubithez a $|1\rangle$ qubitet rendeli és az $|1\rangle$ qubithez a $|0\rangle$ qubitet rendeli. Ezt így írhatjuk fel:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0 \ 1) + \begin{pmatrix} 0 \\ 1 \end{pmatrix} (1 \ 0).$$

Eképpen

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

σ_X operátort rendeljük hozzá az X mátrixhoz.

3. Az Y mátrixszal balról való szorzás a $|0\rangle$ qubithez a $i|1\rangle$ qubitet rendeli és az $|1\rangle$ qubithez a $-i|0\rangle$ qubitet rendeli. Ezt így írhatjuk fel:

$$Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = -i \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0 \ 1) + i \begin{pmatrix} 0 \\ 1 \end{pmatrix} (1 \ 0).$$

Eképpen

$$Y = -i \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + i \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

σ_Y operátort rendeljük hozzá az Y mátrixhoz.

4. A Z mátrixszal balról való szorzás a $|0\rangle$ qubithez a $|0\rangle$ qubitet rendeli és az $|1\rangle$ qubithez a $-|1\rangle$ qubitet rendeli. Ezt így írhatjuk fel:

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1 \ 0) - \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0 \ 1).$$

Eképpen

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

σ_Z operátornak a mátrixa a Z mátrix.

A Hadamard mátrixot sokszor fogjuk használni.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Tekintsük át az egyes mátrixokra hogy a balról való szorzás a $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ állapothoz milyen ϕ állapotot rendel hozzá.

$$1. \phi = \sigma_0|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \text{ Tehát } \phi = \alpha_0|0\rangle + \alpha_1|1\rangle.$$

$$2. \phi = \sigma_X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_0 \end{pmatrix} \text{ Tehát } \phi = \alpha_1|0\rangle + \alpha_0|1\rangle.$$

$$3. \phi = \sigma_Y|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = i \begin{pmatrix} -\alpha_1 \\ \alpha_0 \end{pmatrix} \text{ Tehát } \phi = -i\alpha_1|0\rangle + i\alpha_0|1\rangle.$$

$$4. \phi = \sigma_Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ -\alpha_1 \end{pmatrix} \text{ Tehát } \phi = \alpha_0|0\rangle - \alpha_1|1\rangle.$$

A qubit reprezentálható a foton polarizációjával.

A qubit egy másik reprezentálása az elektron spinje: az állapot fel vagy le.

5.1. A qubit ábrázolása a Bloch gömb felszínén

Legyen $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ egy qubit. A qubit állapotát a θ , ϕ és γ valós számok felhasználásával fejezzük ki. $\psi = e^{i\gamma}[\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle]$ ahol

$$\alpha_0 = e^{i\gamma}\cos\frac{\theta}{2}$$

$$\alpha_1 = e^{i\gamma}e^{i\phi}\sin\frac{\theta}{2}.$$

Itt $e^{i\gamma}$ komplex számot átfogó fázis faktornak hívjuk. $e^{i\gamma}$ értéke nem mutatható ki kísérleti eszközzel, és ezért $e^{i\gamma}$ -t általában figyelmen kívül hagyjuk. A γ különböző értékeihez tartozó qubitek nem különböztethetők meg és a Bloch gömbfelszínnek ugyanazon

pontjával reprezentáljuk őket.

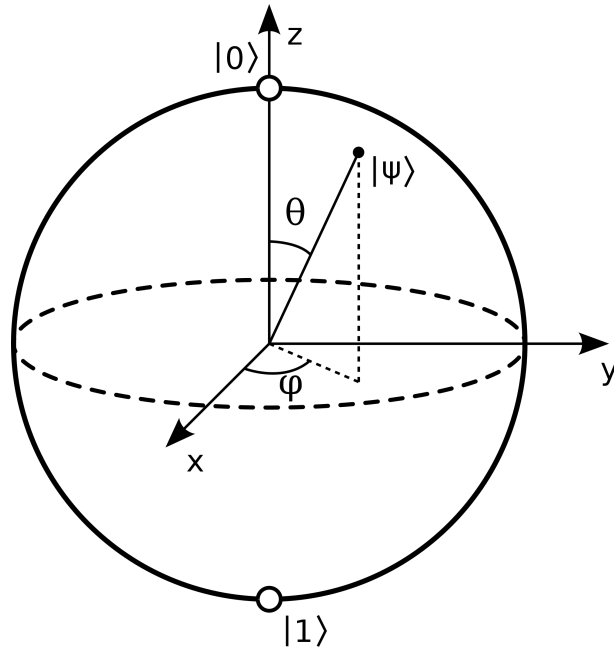
Igazoljuk hogy $|\alpha_0|^2 + |\alpha_1|^2 = 1$!

$$|\alpha_0|^2 + |\alpha_1|^2 = |e^{i\gamma} \cos \frac{\theta}{2}|^2 + |e^{i\gamma} e^{i\phi} \sin \frac{\theta}{2}|^2 =$$

$$|e^{i\gamma}|^2 \cos^2 \frac{\theta}{2} + |e^{i\gamma}|^2 |e^{i\phi}|^2 \sin^2 \frac{\theta}{2} = \cos^2 \frac{\theta}{2} + \sin^2 \frac{\theta}{2} = 1.$$

Itt felhasználtuk az Euler-képletet. Euler-képlet: minden x valós számra, $e^{ix} = \cos x + i \sin x$.

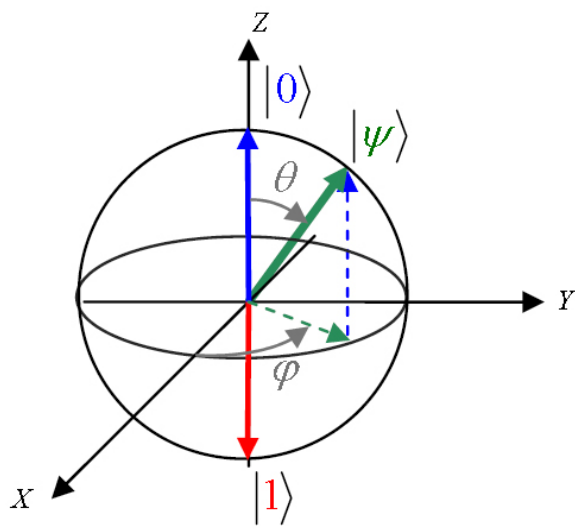
Ezért $|e^{i\gamma}|^2 = |e^{i\phi}|^2 = 1$.



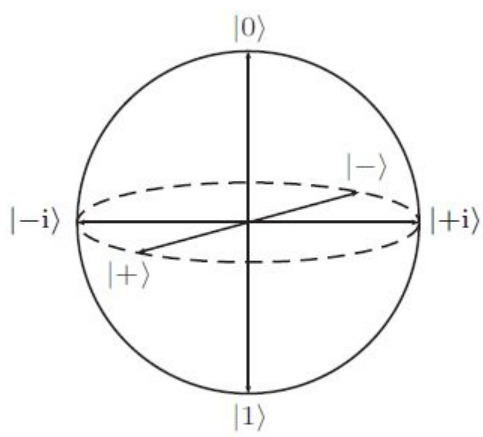
14. ábra. Bloch gömbfelszín [19]

A fenti reprezentációt lerajzoljuk, lásd 14. és 15. ábrák. A $|\psi\rangle$ qubit az origóból kiinduló egy 1 hosszú $\vec{r}$ vektor. Az r és a z tengely által bezárt szöget θ -val jelöljük. Az $\vec{r}$ vektornak az xy síkra eső vetülete és a x tengely által bezárt szöget ϕ -vel jelöljük.

Példa: Tekintsük a 16. ábrát. Először tekintsük a $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ qubitet amely a $|0\rangle, |1\rangle$ bázis vektorok lineáris kombinációja. Most $\alpha_0 = \alpha_1 = \frac{1}{\sqrt{2}}$. Most



15. ábra. Bloch gömbfelszín [1]



16. ábra. Bloch gömbfelszín, [6]

$$\alpha_0 = \cos \frac{\theta}{2} = \frac{1}{\sqrt{2}} \Rightarrow \frac{\theta}{2} = \frac{\pi}{4} \Rightarrow \theta = \frac{\pi}{2}$$

és

$\alpha_1 = e^{i\phi} \sin \frac{\theta}{2} = \frac{1}{\sqrt{2}}$. Mivel $\frac{\theta}{2} = \frac{\pi}{4}$, így $\sin \frac{\theta}{2} = \frac{1}{\sqrt{2}}$. Tehát kapjuk hogy $e^{i\phi} = 1$. Ezért $\phi = 0$.

Másodszorra tekintsük a $|-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ qubitet amely a $|0\rangle$, $|1\rangle$ bázis vektorok lineáris kombinációja. Most $\alpha_0 = \frac{1}{\sqrt{2}}$ és $\alpha_1 = -\frac{1}{\sqrt{2}}$. Most

$$\alpha_0 = \cos \frac{\theta}{2} = \frac{1}{\sqrt{2}} \Rightarrow \frac{\theta}{2} = \frac{\pi}{4} \Rightarrow \theta = \frac{\pi}{2}$$

és

$\alpha_1 = e^{i\phi} \sin \frac{\theta}{2} = -\frac{1}{\sqrt{2}}$. Mivel $\frac{\theta}{2} = \frac{\pi}{4}$, így $\sin \frac{\theta}{2} = \frac{1}{\sqrt{2}}$. Tehát kapjuk hogy $e^{i\phi} = -1$. Ezért $\phi = \pi$.

Figyeljük meg hogy a ϕ és ψ qubiteket a Bloch gömbfelszín áttellenes pontjai reprezentálják.

A Bloch gömb felszínének bármely pontja által kijelölt állapotot felveheti értékéül a qubit. A Bloch gömb felszíne tartalmazza a két bázis állapotot: $|0\rangle$, $|1\rangle$ -t is. Számításink során a qubit kiindulási állapota mindig valamelyik bázis állapot.

5.2. A qubit megmérése

Tegyük fel hogy van egy qubitünk egy ismeretlen $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ állapotban. A qubitet a kvantum rendszer egy fizikai változója valósítja meg. Amikor megmérjük a qubitet akkor ezt a fizikai változót mérjük meg. A fizikai változó megválasztása meghatározza a mérés leírásának a keret rendszerét. A fizikai

változó megválasztása meghatározza a Hilbert tér egy bázisát mint például a $\{ |0\rangle, |1\rangle \}$ bázist. A meghatározott bázis vektorai a megmért fizikai változó sajátvektorai. A mérés egy projekció (leképezés) a qubit állapotából a bázisba.

A rendszer véletlenszerűen változik a $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ vektor által leírt kezdeti állapotból

$|\alpha_0|^2$ valószínűséggel a $|0\rangle$ állapotba megy át vagy
 $|\alpha_1|^2$ valószínűséggel az $|1\rangle$ állapotba megy át.

A mérés hatására egy valós számot kapunk végeredményként. A kapott valós szám a λ_0, λ_1 ($\lambda_0 \neq \lambda_1$) sajátértékek valamelyike. Itt a λ_0 sajátérték a $|0\rangle$ sajátvektorhoz tartozik, és a λ_1 sajátérték az $|1\rangle$ sajátvektorhoz tartozik. Amikor λ_0 -t kapunk végeredményként, akkor a rendszer a $|0\rangle$ állapotba megy át. Amikor λ_1 -t kapunk végeredményként, akkor a rendszer az $|1\rangle$ állapotba megy át.

Tekintsük át a „A fizikai változó megmérése” fejezetet!

Legyen $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ egy qubit. Megmérjük a $|\psi\rangle$ qubitet. A méréshez két projekció operátort rendelünk hozzá. A $\mathbf{M}_0$ projekció operátor a $|0\rangle$ állapotvektorra vetít, és a $\mathbf{M}_1$ projekció operátor az $|1\rangle$ állapotvektorra vetít. $|0\rangle\langle 0| = \mathbf{P}_{|0\rangle} = \mathbf{M}_0$. $|1\rangle\langle 1| = \mathbf{P}_{|1\rangle} = \mathbf{M}_1$.

A megfelelő mátrixok:

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (10) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

és

$$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & \\ & 1 \end{pmatrix} (01) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Annak a valószínűsége hogy a k -adik ($k = 1, 2$) végeredmény lesz a mérés eredménye: $p(k) = \langle \psi | M_k^\dagger M_k | \psi \rangle$. A két lehetséges végeredmény valószínűségének az összege:

$\sum_{k=1}^2 p(k) = \sum_{k=1}^2 \langle \psi | M_k^\dagger M_k | \psi \rangle = 1$. A mérés hatására a qubit megváltoztatja az állapotát. Ha közvetlenül a mérés előtt ψ állapotban volt a qubit akkor a mérés után a $|\phi_k\rangle$ állapotba kerül, ahol

$k = 0$ vagy $k = 1$ és

$$\phi_k = \frac{M_k |\psi\rangle}{\sqrt{\langle \psi | M_k^\dagger M_k | \psi \rangle}}$$

$$M_0^\dagger = M_0,$$

$$M_0^\dagger M_0 = M_0 M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = M_0$$

és

$$M_1^\dagger = M_1,$$

$$M_1^\dagger M_1 = M_0 M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = M_1$$

Annak a valószínűsége hogy a mérés után a $|0\rangle$ -nak megfelelő végeredményt kapjuk:

$$p_0 = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle.$$

Most kiszámítjuk az M_0 operátornak a $|\psi\rangle$ qubitre való alkalmazásának a hatását. $M_0 |\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ 0 \end{pmatrix}$.

A kiindulási ψ vektor duálisa a $\langle\psi| = (\alpha_0^* \ \alpha_1^*)$. Tehát $p_0 = \langle\psi|(M_0|\psi\rangle) = (\alpha_0^* \ \alpha_1^*) = |\alpha_0|^2$.

Mivel $M_0|\psi\rangle = \begin{pmatrix} \alpha_0 \\ 0 \end{pmatrix} = \alpha_0|0\rangle$, kapjuk hogy az M_0 mérési operátor alkalmazás után a qubit állapota:

$$|\phi_0\rangle = \frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} = \frac{\alpha_0|0\rangle}{|\alpha_0|} = \frac{\alpha_0}{|\alpha_0|}|0\rangle.$$

Most kiszámítjuk az M_1 operátornak a $|\psi\rangle$ qubitre való alkalmazásának a hatását. $M_1|\psi\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_1 \end{pmatrix}$.

A kiindulási ψ vektor duálisa a $\langle\psi| = (\alpha_0^* \ \alpha_1^*)$. Tehát $p_1 = \langle\psi|(M_1|\psi\rangle) = (\alpha_0^* \ \alpha_1^*)(M_1|\psi\rangle) = |\alpha_1|^2$.

Annak a valószínűsége hogy a mérés után az $|1\rangle$ -nak megfelelő végeredményt kapjuk:

$p_1 = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle$. Az M_1 mérési operátor alkalmazás után a qubit állapota:

$$|\phi_1\rangle = \frac{M_1|\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} = \frac{\alpha_1|1\rangle}{|\alpha_1|} = \frac{\alpha_1}{|\alpha_1|}|1\rangle.$$

A teljességi feltétel teljesül, mert $p_0 + p_1 = |\alpha_0|^2 + |\alpha_1|^2 = 1$.

5.3. Két qubit 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 $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$ komplex számok. Amikor megmérünk két qubit által alkotott $|\psi\rangle$ párt, akkor a kvantum rendszer $|\psi\rangle$ állapotát

rávetítjük a négy bázis állapot valamelyikére. Eredményül kapjuk a $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ vektorokat, rendre $|\alpha_{00}|^2$, $|\alpha_{01}|^2$, $|\alpha_{10}|^2$, $|\alpha_{11}|^2$ valószínűséggel.

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

Mi történik akkor ha csak egy qubitet mérünk meg? Most mérjük meg csak az első qubitet. Az első qubit $|0\rangle$ lesz

$p'_0 = |\alpha_{00}|^2 + |\alpha_{01}|^2$ valószínűséggel. Az első qubit $|1\rangle$ lesz

$p'_1 = |\alpha_{10}|^2 + |\alpha_{11}|^2$ valószínűséggel. A fentiek alapján: $p'_0 + p'_1 = 1$.

Tekintsük azt az esetet amikor a mérés után az első qubit $|0\rangle$ lesz. ψ'_0 jelöli a mérés utáni állapotot. Tekintsük azt az esetet amikor a mérés után az első qubit $|1\rangle$ lesz. ψ'_1 jelöli a mérés utáni állapotot.

$$|\psi'_0\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

$$|\psi'_1\rangle = \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}.$$

Most mérjük meg csak a második qubitet. A második qubit $|0\rangle$ lesz

$p''_0 = |\alpha_{00}|^2 + |\alpha_{10}|^2$ valószínűséggel. A második qubit $|1\rangle$ lesz

$p''_1 = |\alpha_{01}|^2 + |\alpha_{11}|^2$ valószínűséggel. A fentiek alapján: $p''_0 + p''_1 = 1$.

Tekintsük azt az esetet amikor a mérés után a második qubit $|0\rangle$ lesz. ψ''_0 jelöli a mérés utáni állapotot. Tekintsük azt az esetet amikor a mérés után az első qubit $|1\rangle$ lesz. ψ''_1 jelöli a mérés utáni állapotot.

$$|\psi''_0\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{10}|10\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{10}|^2}}$$

és

$$|\psi_1''\rangle = \frac{\alpha_{01}|01\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}.$$

Tekintük az két qubitből 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 qubit párt pedig EPR párnak hívjuk. Tegyük fel hogy a két qubitből álló rendszer ebben az állapotban van. Amikor megmérjük az első qubitet a két lehetséges eredmény: $|0\rangle$, $\frac{1}{2}$ valószínűséggel és $|1\rangle$, $\frac{1}{2}$ valószínűséggel. A két megfelelő mérés utáni állapot:

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

és

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

Amikor megmérjük a második qubitet, a két lehetséges eredmény: $|0\rangle$, $\frac{1}{2}$ valószínűséggel és $|1\rangle$, $\frac{1}{2}$ 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 qubitet mérjük meg ugyanazt az eredményt kapjuk mint amikor a második qubitet mérjük meg. A két qubit lehet különböző helyen, mégis amikor megmérjük a másodikat tudjuk hogy az első milyen állapotban van.

A Bell állapotok.

Négy speciális állapotot hívunk Bell állapotnak. A Bell állapotok

egy ortonormális bázist alkotnak. A Bell állapotok:

$$1. |\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

$$2. |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},$$

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

$$4. |\beta_{01}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

A Bell állapotokat meg tudjuk különböztetni egymástól. Mind a négy állapotot maximálisan összefonódott állapotnak hívjuk. Az EPR pár az első Bell állapot.

A qubit két kvantum állapotát akkor és csak akkor tudjuk megkülönböztetni mérőeszközeinkkel, ha azok ugyanabban a bázisban vannak reprezentálva. Meg tudjuk különböztetni a $|0\rangle$ -t és $|1\rangle$ kvantum állapotokat. Nem tudjuk megkülönböztetni $|0\rangle$ -t és $\sqrt{\frac{1}{2}}(|0\rangle - |1\rangle)$ kvantum állapotokat.

A kvantum állapot egy ekvivalencia osztályt alkot. $e^{i\gamma}$ -val való szorzás nem változtat meg egység vektort.

A két qubitből álló rendszer lehet szuperpozíció állapotban vagy összefonódott állapotban. A szuperpozíció állapotban mindegyik (mind a kettő) qubitnek jól definiált állapota van. Az összefonódott állapotban a két qubitből álló rendszernek jól definiált állapota van, de egyik qubitnek sincsen jól definiált állapota. Például tekintsük azt az esetet amikor az első qubit az $|1\rangle$ állapotban van, a második qubit pedig a $\sqrt{\frac{1}{2}}(|0\rangle + |1\rangle)$ állapotban van. Ekkor a rendszer állapota előáll a két qubit 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 qubit állapotának a tenzor szorzataként felírni. Általában is igaz, hogy az összefonódott állapotot nem lehet két qubit állapotának a tenzor szorzataként felírni. Ugyanis tegyük fel, hogy

$$(\alpha_1|0\rangle + \alpha_2|1\rangle) \otimes (\beta_1|0\rangle + \beta_2|1\rangle) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{pmatrix} =$$

$$\begin{pmatrix} \sqrt{\frac{1}{2}} \\ 0 \\ 0 \\ \sqrt{\frac{1}{2}} \end{pmatrix} = \sqrt{\frac{1}{2}}(|00\rangle + |11\rangle)$$

Ekkor $\alpha_1\beta_1 = \sqrt{\frac{1}{2}}$, $\alpha_1\beta_2 = 0$, $\alpha_2\beta_1 = 0$, $\alpha_2\beta_2 = \sqrt{\frac{1}{2}}$. Tehát $\alpha_1 \neq 0$, $\beta_1 \neq 0$, $\alpha_2 \neq 0$, $\beta_2 \neq 0$. Viszont ekkor $\alpha_1\beta_2 \neq 0$, ami ellentmondás.

Általában az n qubitből 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.

5.4. A qubit mint részecske fél spinnel

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 mozgás-mennyiséget”. A spin egy szám amely leírja az elektron benső szög mozgásmennyiséget. A kísérletek azt igazolták hogy az elektron spinje $+\frac{1}{2}$ vagy $-\frac{1}{2}$ értéket vesz fel a mérés tengelye mentén, függetlenül attól hogy hogyan választjuk meg a mérés tengelyét.

A $|0\rangle$ és $|1\rangle$ qubit 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:

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

Tekintsük az x, y, z tengelyekkel rendelkező 3 dimenziós koordináta rendszert. Az x, y, z tengelyek mentén rendre megmérjük az elektron spinjét. S_X, S_Y, S_Z jelöli rendre a három mérést leíró mérési operátorokat.

Állítás 5.1 $S_X = \frac{1}{2}\sigma_X = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$

$$S_Y = \frac{1}{2}\sigma_Y = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$S_Z = \frac{1}{2}\sigma_Z = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

1. A S_X spin operátor: sajátérték $-\frac{1}{2}$ a hozzá tartozó sajátvektor $\frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

Sajátérték $+\frac{1}{2}$ a hozzá tartozó sajátvektor $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

2. A S_Y spin operátor: sajátérték $-\frac{1}{2}$ a hozzá tartozó sajátvektor $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$.

Sajátérték $+\frac{1}{2}$ a hozzá tartozó sajátvektor $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$

3. A S_Z spin operátor: sajátérték $-\frac{1}{2}$ a hozzá tartozó sajátvektor $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

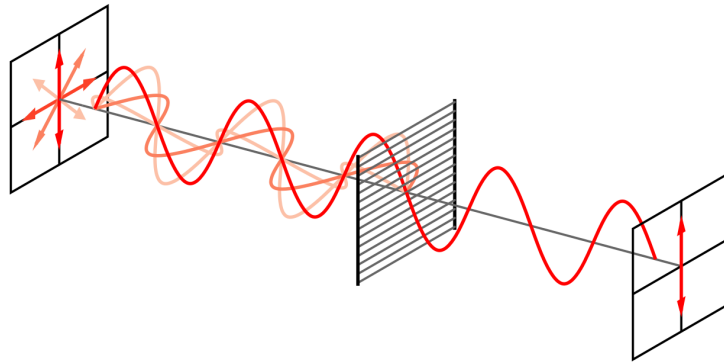
Sajátérték $+\frac{1}{2}$ a hozzá tartozó sajátvektor $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Mind a három operátorra teljesül, hogy a hozzá tartozó a sajátvektor pár egy bázist alkot a $\mathcal{H}_2$ Hilbert tér számára. Az elektron állapot vektora a bázis vektorok lineáris kombinációjaként áll elő. Az együtthatók segítségével megadhatjuk annak a valószínűségét hogy a kísérlet a 'spin fel' (azaz $\frac{1}{2}$) vagy 'spin le' (azaz $-\frac{1}{2}$) sajátértéket ad-e.

5.5. A qubit mint polarizált foton

A foton két állapotú kvantum rendszer amelyet a qubit megvalósítására használnak. A fotonnak két független polarizációja van.

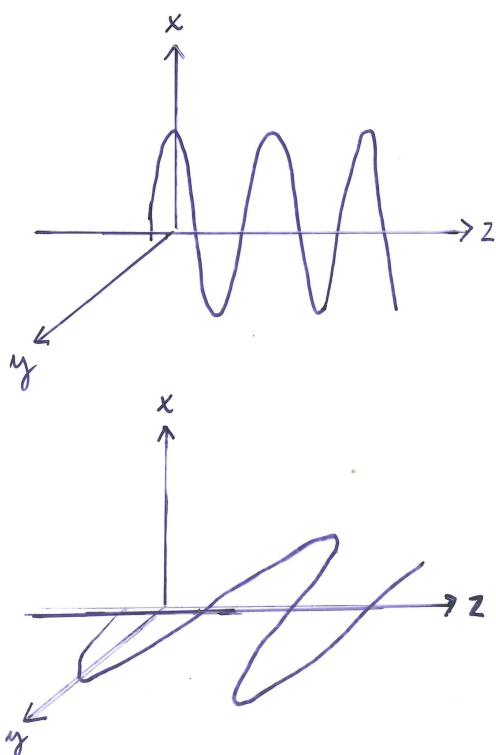
A fotonnak nincsen tömege és 1 spinje van. A fotont a vektor momentuma (mozgásmennyisége) és a polarizációja határozza meg, A fény elektromágneses sugárzás amely elektromos mezője oszcillál. A fény a z tengely mentén halad. Az erre merőleges xy síkban oszcillál az elektromos mező. Amikor az elektromos mező függőlegesen oszcillál a haladásra merőleges síkban, akkor azt mondjuk hogy a fény x polarizált.



17. ábra. Huzalrács polarizátor, hatására az elektromos mező függőlegesen oszcillál. [14]

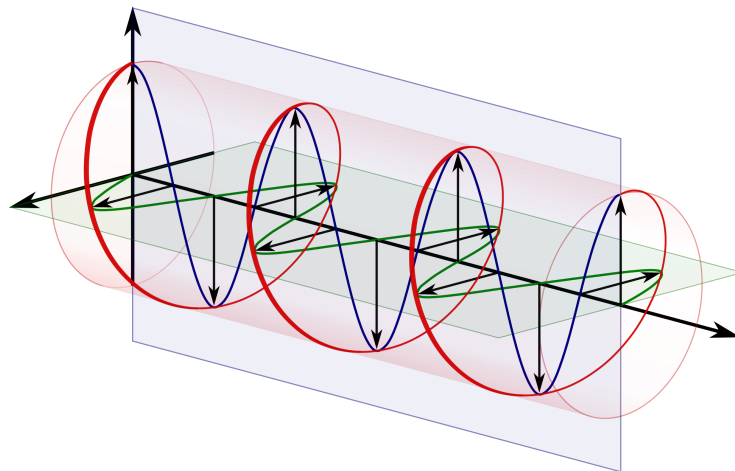
Amikor az elektromos mező vízszintesen oszcillál a haladásra merőleges xy síkban, akkor azt mondjuk hogy a fény y polarizált. Lásd

18 ábrát. Amikor az elektromos mezőnek tetszőleges az iránya az xy síkban, akkor az iránynak van x és y komponense. Ha ezek a komponensek fázisa 90 fokkal tér el egymástól akkor az



18. ábra. Függőlegesen és vízszintesen polarizált fény

elektromos mező forog és a fény elliptikusan polarizált. Amikor az x és y komponensek egyenlőek egymással és a komponensek fázisa 90 fokkal tér el egymástól akkor fény kör alakban polarizált lásd 19. ábra [4].



19. ábra. Kör alakban polarizált fény [4]

Polarizációs szűrőt használunk. A szűrő egy sík lap. A szűrő tengelye meghatározza hogy milyen állapotú fotonokat enged át és milyen állapotú fotonokat nyel el. A fény fotonokat a fenti két polarizációs állapotba kényszeríti majd megszűri a következő módon.

1. Beállíthatjuk a szűrő tengelyét úgy hogy a szűrő az y polarizált fényt engedje át. Ekkor a $|v\rangle$ állapotban lévő fotonokat elnyeli a szűrő, és csak a $|h\rangle$ állapotban lévő fotonokat engedi át.
2. Beállíthatjuk a szűrő tengelyét úgy hogy a szűrő az x polarizált fényt engedje át. Ekkor a $|h\rangle$ állapotban lévő fotonokat elnyeli a szűrő, és csak a $|v\rangle$ állapotban lévő fotonokat engedi át.

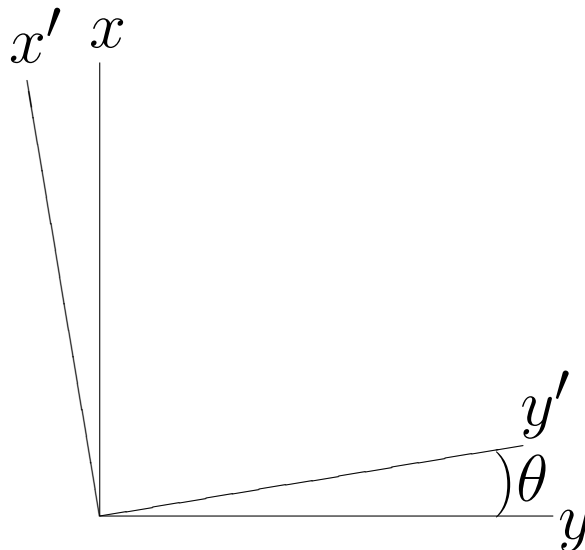
Tekintsük azt az esetet amikor a szűrőt elforgatjuk. Ekkor a fény fotonokat az x' vagy y' polarizációs állapotba kényszeríti

majd megszűri a következő módon.

1'. Beállíthatjuk a szűrő tengelyét úgy hogy a szűrő az y' polarizált fényt engedje át. Ekkor a $|v'\rangle$ állapotban lévő fotonokat elnyeli a szűrő, és csak a $|h'\rangle$ állapotban lévő fotonokat engedi át.

2'. Beállíthatjuk a szűrő tengelyét úgy hogy a szűrő az x' polarizált fényt engedje át. Ekkor a $|h'\rangle$ állapotban lévő fotonokat elnyeli a szűrő, és csak a $|v'\rangle$ állapotban lévő fotonokat engedi át.

Tekintsük az alábbi kísérletet 20. ábra.



20. ábra.

A polarizációs szűrőt θ szöggel elforgatjuk úgy hogy a síkja hogy θ szöget zárjon be a beérkező fény haladási irányára merőleges síkkal, azaz a fény koordináta rendszerének x, y tengelyei által

meghatározott síkkal, lásd 20. ábra. A szűrőből kijövő fénysugár y' irányban polarizált, ahol y és y' θ szöget zárnak be, lásd 21. ábra.

Ekkor a szűrőből kijövő fotonok $|h'\rangle$ állapotban lesznek. Ezt az állapotot a $|h\rangle$ és $|v\rangle$ bázis állapotok lineáris kombinációjaként írhatjuk fel:

$$|h'\rangle = \cos\theta|h\rangle + \sin\theta|v\rangle.$$

A kísérlet második részében ezek a fotonok $|h'\rangle$ állapotban (azaz az y' tengely mentén polarizáltan) mennek keresztül a második polarizációs szűrőn. A második szűrő tengelyét úgy állítjuk be hogy a szűrő az y polarizált fényt engedje át azaz csak a $|h\rangle$ állapotban lévő fotonokat engedi át. Megbecsüljük annak a valószínűségét hogy a $|h'\rangle$ állapotban lévő fotont a szűrő $|h\rangle$ állapotba kényszeríti.

$$\langle h|h'\rangle = \cos\theta\langle h|h\rangle + \sin\theta\langle h|v\rangle$$

itt $|h\rangle$ és $|v\rangle$ ortonormális bázist alkotnak. Tehát $\langle h|h\rangle = 1$ és $\langle h|v\rangle = 0$. Tehát annak a valószínűsége hogy a $|h'\rangle$ állapotban lévő fotont a szűrő $|h\rangle$ állapotba kényszeríti:

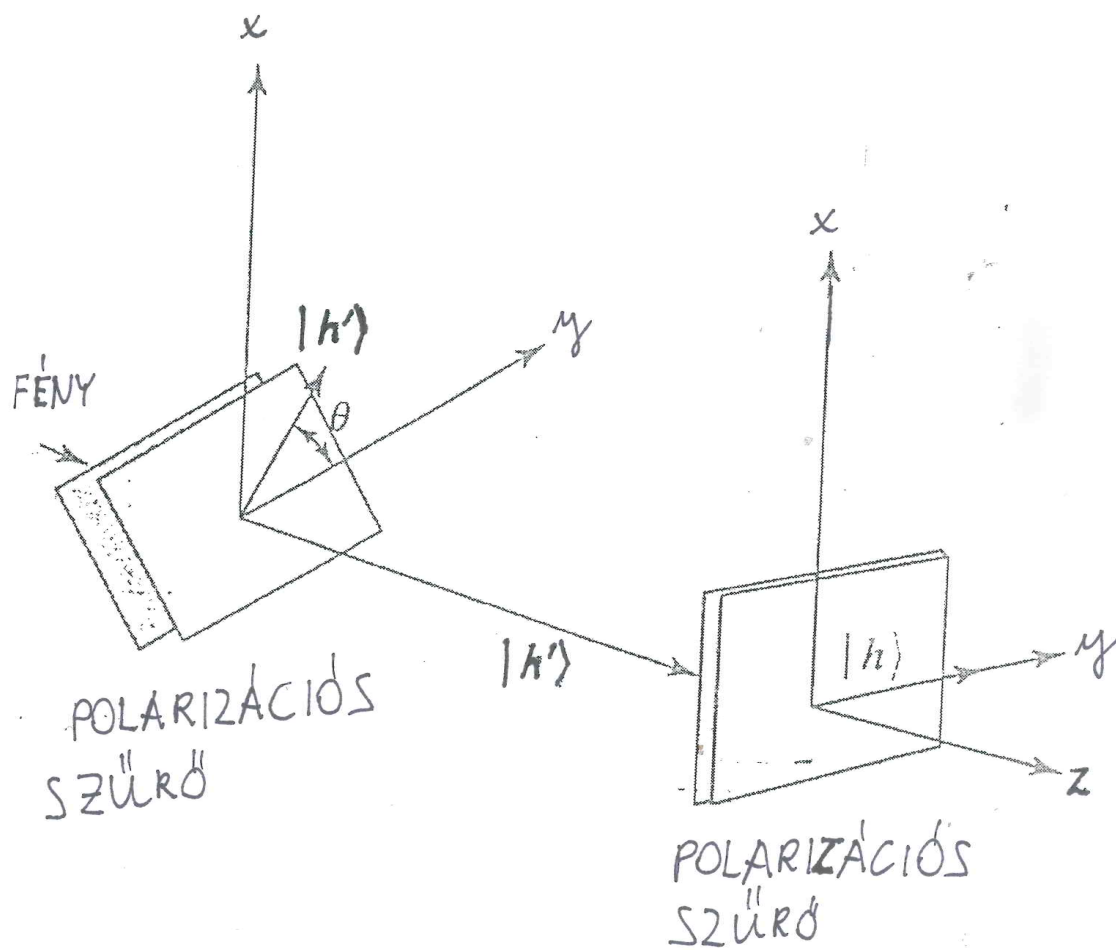
$$|\langle h|h'\rangle|^2 = \cos^2\theta.$$

A polarizációs szűrőt θ szöggel elforgattuk a fény haladási irányának a tengelye körül, ekkor $|h\rangle$ állapotot a $\langle h'\rangle$ állapotba transzformáltuk, és a $|v\rangle$ állapotot a $\langle v'\rangle$ állapotba transzformáltuk.

$$|h\rangle \mapsto |h'\rangle = \cos\theta|h\rangle + \sin\theta|v\rangle.$$

$$|v\rangle \mapsto |v'\rangle = -\sin\theta|h\rangle + \cos\theta|v\rangle.$$

Ennek a transzformációnak a mátrixa: $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$



21. ábra. Függőlegesen és vízszintesen polarizált fény

A mátrix sajátvektorai és sajátértékei:

1. Az $|R\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$ sajátvektorhoz az $e^{i\theta}$ sajátérték tartozik.

Ezt a sajátvektort jobb polarizáció állapotnak hívjuk.

2. Az $|L\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}$ sajátvektorhoz az $e^{-i\theta}$ sajátérték tartozik. Ezt a sajátvektort bal polarizáció állapotnak hívjuk.

Tekintsük a $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ forgatási operátort. $|R\rangle, |L\rangle$ ennek a mátrixnak is a sajátvektorai rendre a 1, -1 sajátértékekkel. Mivel a sajátértékek 1, -1 , ezért azt mondjuk hogy a fotonnak egész spinje van.

5.6. Összefonódás

Tekintsük azt a rendszert amely két elektronból áll amelyek antiszimmetrikusak és amelyek spinje antiparallel. Azaz a fenti két elektron spin vektora párhuzamos de ellentétes irányú.

Az elektronok spinje:

$$\frac{1}{2} \quad -\frac{1}{2}$$

vagy

$$-\frac{1}{2} \quad \frac{1}{2}$$

A két elektron spinjének az összege 0.

A fenti kvantum rendszer a két elektront ellentétes irányban bocsátja ki a kvantum rendszer széthullása után.

A szög momentum megmaradása miatt a fenti két elektron spin vektora párhuzamos de ellentétes irányú. Ezért ha megmérjük

az egyik elektron spinjét valamely irány mellett és azt találjuk hogy az elektron „spin felfelé” állapotba van, akkor ezen irány mentén a másik elektron „spin lefelé” állapotban van. Amikor megmérjük az egyik részecske spinjét, akkor az állapotvektorát a mérés bázisának egy vektorába kényszerítjük. Ugyanekkor a másik részecske állapotvektora automatikusan lesz az eleme ugyanannak a bázisnak.

Tegyük fel hogy a fenti rendszeren az alábbi kísérletet hajtjuk végre. Először megmérjük az első részecske spinjét, az xz tengely valamely vektora mentén és azt találjuk hogy a részecske „spin lefele” állapotban van. Akkor a másik részecske ugyanazon irány mentén „spin felfele” állapotban van. Ezután megmérjük a második részecske spinjét egy olyan vektor mentén amely θ szöget zár be az első irányvektorral. Azt találjuk hogy a második részecske a „spin lefele” és a „spin felfele” állapotok kombinációjában van rendre a $\cos^2(\frac{\theta}{2})$ és $\sin^2(\frac{\theta}{2})$ valószínűségekkel.

Tegyük fel hogy az első részecske mérése után azt találjuk hogy a részecske „spin felfele” állapotban van. Akkor a másik részecske ugyanazon irány mentén „spin lefele” állapotban van. Ezután megmérjük a második részecske spinjét egy olyan vektor mentén amely θ szöget zár be az első irányvektorral. Azt találjuk hogy a második részecske a „spin lefele” és a „spin felfele” állapotok kombinációjában van rendre a $\sin^2(\frac{\theta}{2})$ és $\cos^2(\frac{\theta}{2})$ valószínűségekkel.

Most mérjük meg az első részecskét majd a másodikat. A két mérés két irányvektora zárjon be θ szöget egymással. Most $\sin^2(\frac{\theta}{2})$ annak a valószínűsége hogy a két mérés ugyanazt azt

eredményt adja: „spin felfele” és „spin felfele” vagy „spin lefele” és „spin lefele”. Továbbá $\cos^2(\frac{\theta}{2})$ annak a valószínűsége hogy a két mérés ellenkező eredményt adja: „spin felfele” és „spin lefele” vagy „spin lefele” és „spin felfele”.

Azt mondjuk hogy a fenti két részecske össze van fonódva. Az nem befolyásolja a mérések eredményét hogy milyen messzire kerültek egymástól.

A fenti valószínűségeket többszörös mérés eredményeként kapjuk meg. Nagy számú részecske párt készítünk azonos módon, és ezeken a párokon végezzük el a méréseket. A méréseket függetlenül végezzük el az egyes párokon.

A mérési tengely megválasztása megadja a vektor bázist mind a két elektron számára. Amikor az első részecskét megmérjük valamely irányvektor mentén akkor a második részecske állapota ugyanazon irány mentén „spin lefele” vagy „spin felfele”. Tegyük fel hogy a vízszintes tengely a 0 bináris számot a függőleges tengely az 1 bináris számot reprezentálja. Kiválasztunk egy mérési tengelyt a mérés számára majd mérünk. Ezzel lehetővé válik a 0-k és 1-ek továbbítása nagy távolságokra „azonnal”. Azért írtuk hogy „azonnal”, mert az információ továbbításának a sebessége nem haladja meg a fény sebességét.

5.7. Nagy sűrűségű kódolás (superdense coding)

Alice és Bob rendelkeznek két qubittel, amelyek a

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

összefonódott állapotban vannak. Alice-nál van az első qubit. Bobnál a második. Bob elutazik és magával viszi a második qubitet. Alice 2 hagyományos bitből álló üzenetet küld Bobnak a következő módon. Alice az üzenetnek megfelelő operátort alkalmazza az első qubitre majd Alice qubit csatornán elküldi az első qubitet Bobnak. Ilyen módon két hagyományos bitet tud elküldeni Bobnak. Alice a következő módon jár el.

1. Ha '00'-et akar elküldeni Bobnak, akkor semmit sem csinál a qubitjével. A négy eset egységes tárgyalása végett, azt mondjuk hogy az $\mathbf{I}_{2 \times 2}$ egység mátrixhoz tartozó operátort alkalmazza a qubitjére. Képezzük a két $\mathbf{I}_{2 \times 2}$ egység mátrix tenzor szorzatát. At így kapott mátrixhoz tartozó operátort alkalmazzuk a két qubit által alkotott rendszerre. A két $\mathbf{I}_{2 \times 2}$ egység mátrix tenzor szorzata:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Alkalmazzuk az operátort, azaz balról szorzunk az eredményül kapott $\mathbf{I}_{4 \times 4}$ egység mátrixszal.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Tehát az operátor alkalmazása után a két qubitből álló rendszer marad a kiindulási állapotban. Ezután Alice qubit csatornán elküldi az első qubitet Bobnak.

2. Ha '01'-et akar elküldeni Bobnak, akkor a σ_Z operátort alkalmazza a qubitjére. Azaz Alice a Z mátrixhoz tartozó operátort alkalmazza a qubitjére.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

és a σ_Z operátornak a mátrixa a Z mátrix.

Képezzük a Z és az $\mathbf{I}_{2 \times 2}$ egység mátrix tenzor szorzatát. Az így kapott mátrixhoz tartozó operátort alkalmazzuk a két qubit által alkotott rendszerre. A két mátrix tenzor szorzata:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Alkalmazzuk az operátort!

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

Tehát az operátor alkalmazása után a két qubitből álló rendszer

a

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

állapotba kerül. Ezután Alice qubit csatornán elküldi az első qubitet Bobnak.

3. Ha '10'-át akar elküldeni Bobnak, akkor a NOT kvantum kaput alkalmazza a qubitjére. A *NOT* kapu felcseréli az input qubit komponenseit. Azaz Alice az X mátrixhoz tartozó operátort alkalmazza a qubitjére.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Képezzük az X és a $\mathbf{I}_{2 \times 2}$ egység mátrix tenzor szorzatát. At így kapott mátrixhoz tartozó operátort alkalmazzuk a két qubit által alkotott rendszerre. A két mátrix tenzor szorzata:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Alkalmazzuk az operátort!

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Tehát az operátor alkalmazása után a két qubitből álló rendszer

a

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

állapotba kerül. Ezután Alice qubit csatornán elküldi az első qubitet Bobnak.

4. Ha '11'-et akar elküldeni Bobnak, akkor az iY mátrixhoz tartozó operátort alkalmazza a qubitjére.

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Eképpen

$$iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Képezzük az iY és a $\mathbf{I}_{2 \times 2}$ egység mátrix tenzor szorzatát. At így kapott mátrixhoz tartozó operátort alkalmazzuk a két qubit által alkotott rendszerre. A két mátrix tenzor szorzata:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Alkalmazzuk az operátort!

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}.$$

Tehát az operátor alkalmazása után a két qubitből álló rendszer

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \text{ állapotba kerül. Ezután Alice qubit}$$

csatornán elküldi az első qubitet Bobnak.

A következő 4 állapotot kapjuk Alice által elvégzett transzformáció eredményeképpen:

$$\text{állapot}_{00}: |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\text{állapot}_{01}: |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\text{állapot}_{10}: |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$\text{állapot}_{11}: |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Mint korábban láttuk, ez a négy kapott állapot, a 4 Bell állapot. A Bell állapotok egy ortonormális bázist alkotnak a $\mathcal{H}_4$ Hilbert tér számára. Megfelelő méréssel megkülönböztethetők egymástól. Bob a Bell bázisban méréssel eldönti hogy melyik állapotban van a két qubitből álló rendszer. Ha az állapot₀₀-ban, akkor Alice a 00 biteket küldte. Ha az állapot₀₁-ben, akkor Alice a 01 biteket küldte. Ha az állapot₁₀-ban, akkor Alice a 10 biteket küldte. Ha az állapot₁₁-ben, akkor Alice az 11 biteket küldte.

Kísérlettel megvalósították a nagy sűrűségű kódolás egy változatát. Egymásba fonódott fotonokat használtak fel a kísérlet során.

6. 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 transzformációkat Hermite-féle operátorokkal írjuk le. Az állapot transzformációt leíró mátrixot transzfer (áthelyező) mátrixnak nevezzük.

Az áthelyező (transzfer) mátrix unitér és az általuk indukált transzformációk megfordíthatók. Az unitér transzformáció megfelel egy hossz megőrző és információ megőrző forgatásnak a vektortérben.

A kvantum kapunak a bemenete és a kimenete ugyanannyi véges sok qubitből áll. Tehát a bemenet állhat 1, 2, 3 stb qubitből, a kimenet is ugyanannyi qubitből 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^k ahol k a bemeneti qubitek száma. Azaz a Hilbert tér $\mathcal{H}_2$ amikor a bemenet 1 qubitből áll, $\mathcal{H}_4$ amikor a bemenet 2 qubitből áll, $\mathcal{H}_8$ amikor a bemenet 3 qubitből áll, stb. Az n -qubites kvantum kapu bemeneti állapota az egyes input qubitek $\mathcal{H}_2$ -beli állapotvektorainak a tenzor szorzata. Hasonlóan az n -qubites kvantum kapu kimeneti állapota az egyes output qubitek $\mathcal{H}_2$ -beli állapotvektorainak a tenzor szorzata. Például ha ϕ és ψ a

2-qubites kvantum kapu bemeneti qubitjeinek az állapotvektorai akkor $\phi \otimes \psi$ a kvantum kaput inputjának az állapotvektora. Az n -qubites kvantum kapu elemzésekor használt ortonormális bázis:

1. $|0\rangle$ és $|1\rangle$ $\mathcal{H}_2$ -ben amikor $n = 1$.
 2. $|00\rangle$, $|01\rangle$, $|10\rangle$, 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 $G = [g_{ij}]$ mátrix reprezentálja. Ezen feltételek mellett a kvantum rendszer az eredményül kapott $|W\rangle$ kimeneti állapotára teljesül hogy

$$|W\rangle = G|V\rangle.$$

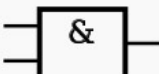
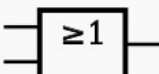
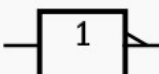
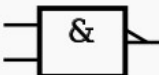
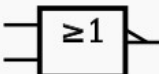
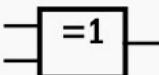
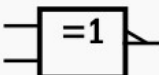
6.1. Klasszikus logikai kapuk és áramkörök

A Boole változók a 0 és 1 értéket veszik fel. *NOT*, *AND*, *NAND*, *OR*, *NOR*, és *XOR* a Boole műveletek.

A logikai kapuk Boole műveleteket valósítanak meg, lásd 22. ábrát.

Itt hét klasszikus logikai kaput látunk. Minden kapura az input Boole függvényeként adjuk meg az outputot. Megadjuk minden egyes Boole függvény igazság tábláját. Az igazság tábla megadja az output értékét a bemeneti változók input értékeinek minden egyes kombinációjára.

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

Kapu	hagyományos jel	szögletes jel	művelet	Igazságtábla																		
AND (és)			$A \cdot B$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A AND B</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	bemenet		kimenet	A	B	A AND B	0	0	0	0	1	0	1	0	0	1	1	1
				bemenet		kimenet																
				A	B	A AND B																
				0	0	0																
				0	1	0																
1	0	0																				
1	1	1																				
OR (megengedő vagy)			$A + B$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A OR B</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	bemenet		kimenet	A	B	A OR B	0	0	0	0	1	1	1	0	1	1	1	1
				bemenet		kimenet																
				A	B	A OR B																
				0	0	0																
				0	1	1																
1	0	1																				
1	1	1																				
NOT (negálás)			$\overline{A}$	<table><tr><th>bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>NOT A</th></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table>	bemenet	kimenet	A	NOT A	0	1	1	0										
				bemenet	kimenet																	
				A	NOT A																	
				0	1																	
				1	0																	
A NOT kaput az elektronikában nevezik még <i>invert</i> eknek is, hiszen gyakorlatilag megfordítja, idegen szóval invertálja a bemenetként kapott igazságértéket.																						
NAND (negált és)			$\overline{A \cdot B}$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A NAND B</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	bemenet		kimenet	A	B	A NAND B	0	0	1	0	1	1	1	0	1	1	1	0
				bemenet		kimenet																
				A	B	A NAND B																
				0	0	1																
				0	1	1																
1	0	1																				
1	1	0																				
NOR (negált vagy)			$\overline{A + B}$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A NOR B</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	bemenet		kimenet	A	B	A NOR B	0	0	1	0	1	0	1	0	0	1	1	0
				bemenet		kimenet																
				A	B	A NOR B																
				0	0	1																
				0	1	0																
1	0	0																				
1	1	0																				
XOR, EXOR vagy MOD2 (kizáró vagy, antivalencia)			$A \oplus B$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A XOR B</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	bemenet		kimenet	A	B	A XOR B	0	0	0	0	1	1	1	0	1	1	1	0
				bemenet		kimenet																
				A	B	A XOR B																
				0	0	0																
				0	1	1																
1	0	1																				
1	1	0																				
XNOR vagy EXNOR (negált kizáró vagy, ekvivalencia)			$\overline{A \oplus B}$	<table><tr><th colspan="2">bemenet</th><th>kimenet</th></tr><tr><th>A</th><th>B</th><th>A XNOR B</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	bemenet		kimenet	A	B	A XNOR B	0	0	1	0	1	0	1	0	0	1	1	1
				bemenet		kimenet																
				A	B	A XNOR B																
				0	0	1																
				0	1	0																
1	0	0																				
1	1	1																				

22. ábra. Logikai kapuk [12]

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

Ismert hogy a *NAND* kapu univerzális. Ez azt jelenti hogy minden logikai függvény kifejezhető *NAND* kapuk felhasználásával. Tehát tetszőleges logikai függvényt kiszámító logikai áramkört fel tudunk építeni *NAND* kapuk felhasználásával. Minden $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$, $n, m \geq 0$ leképezés kiszámítható olyan hagyományos logikai áramkörrel amely *NAND* kapukból épül fel.

A 22. ábrán szereplő összes két Boole változós kapu nem megfordítható. Ez azt jelenti hogy nem teljesül a következő: ha tudjuk az outputot akkor meg tudjuk állapítani 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.

Most egy példát adunk a logikai áramkörre. Az egy-egy bitet összeadó logikai áramkört tekintjük. Az áramkörnek három inputja van: a , b , és *Carryin*, és két outputja: *Sum* és *Carryout*. Az egy-egy bitet összeadó logikai áramkör igazság táblája:

a	b	$Carryin$	Sum	$Carryout$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Az igazság táblából látható hogy

$$Sum = \overline{a}bCarryin \oplus \overline{a}b\overline{Carryin} \oplus a\overline{b}Carryin \oplus ab\overline{Carryin}.$$

$$Carryout = ab \oplus aCarryin \oplus bCarryin$$

A fenti kifejezés alapján kapjuk a

23 ábrán látható klasszikus áramkört.

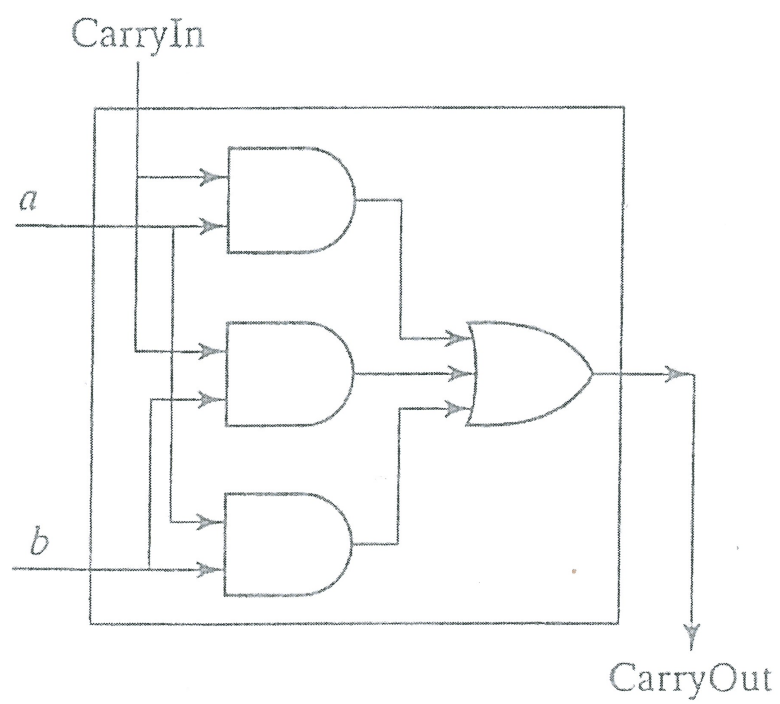
6.2. Egy qubites kvantum kapuk

Egy qubites kvantum kapunak nevezzük azt a fekete dobozt amely a $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ input qubitet átranszformálja a $|\phi\rangle = \alpha'_0|0\rangle + \alpha'_1|1\rangle$ output qubitté. A G egy qubites kvantum kaput megadjuk a 2×2 áthelyező (transzfer) mátrixával.

$$G = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$$

Emlékezzünk vissza hogy a normalizációs feltétel megköveteli hogy

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \text{ és } |\alpha'_0|^2 + |\alpha'_1|^2 = 1. \text{ Ebből következik hogy}$$



23. ábra. A kimenő maradékot kiszámító klasszikus áramkör

G unitér mátrix, azaz $G^\dagger G = GG^\dagger = I_{2 \times 2}$, ahol $I_{2 \times 2}$ a 2×2 -es egység mátrix.

$$G^\dagger = \begin{pmatrix} g_{11}^* & g_{21}^* \\ g_{12}^* & g_{22}^* \end{pmatrix}$$

Tehát

$$G^\dagger G = \begin{pmatrix} g_{11}^* g_{11} + g_{21}^* g_{21} & g_{11}^* g_{12} + g_{21}^* g_{22} \\ g_{12}^* g_{11} + g_{22}^* g_{21} & g_{12}^* g_{12} + g_{22}^* g_{22} \end{pmatrix} = I_{2 \times 2}.$$

Tehát G invertálható, G inverze $G^\dagger$ szintén unitér mátrix. Tehát a kvantum kapuk megfordíthatók. A kvantum kapu által megvalósított transzformáció: $|\phi\rangle = G|\psi\rangle$. Az egy qubites kvantum kapura a fenti egyenlőség az alábbi alakot ölti:

$$\begin{pmatrix} \alpha'_0 \\ \alpha'_1 \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}.$$

Eképpen

$$\alpha'_0 = g_{11}\alpha_0 + g_{12}\alpha_1$$

és

$$\alpha'_1 = g_{21}\alpha_0 + g_{22}\alpha_1.$$

Az alábbiakban megvizsgálunk néhány fontos 1 qubites kaput és megadjuk a hozzá tartozó áthelyező mátrixot.

1. Az I azonosság kapu. Ez a kapu változatlanul hagyja az input qubitet, azaz az output qubit megegyezik az input qubittel.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

2. Az X , vagy másképpen, a NOT kapu. Ez a kapu felcseréli az input qubit komponenseit.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

3. Az Y kapu. Ez a kapu felcseréli az input qubit komponenseit. A csere során az első input komponenst i -vel a második input komponenst $-i$ -vel szorozza meg.

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

4. Az Z kapu. Ez a kapu a második input komponenst -1 -gyel szorozza meg.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. A Hadamard kapu.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

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

Alkalmazzuk a Hadamard kaput a $|0\rangle$ és az $|1\rangle$ állapotokra!

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Tehát ha $x = 0$ vagy $x = 1$, akkor

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle).$$

6.3. A Hadamard kapu, fényosztók, sugárosztók

Felidézzük hogy amikor a foton a fényosztóhoz ér, 50% esélye van arra hogy áthaladjon és 50% esélye van arra hogy visszaverődjön. Más típusú részecskékhez is építettek sugárosztót amely megosztja a részecskék sugárnyalábját.

Tekintsünk egy 50% – 50% sugárnyaláb osztót. Az osztóhoz érkező részecske ugyanannyi valószínűséggel halad át mint amennyi valószínűséggel visszaverődik. Ismert hogy a fénysugár-osztó segítségével megvalósítjuk a Hadamard transzformációt lásd 24. ábra.

A Hadamard kapu a $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ input qubitet átranszformálja a $|\phi\rangle = \alpha'_0|0\rangle + \alpha'_1|1\rangle$ output qubitté. Felidézzük hogy

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

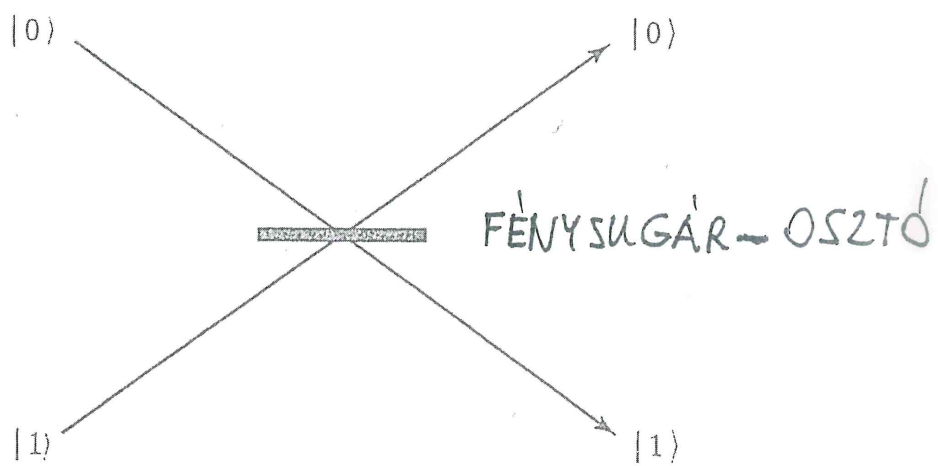
Annak a valószínűségi amplitúdója hogy az osztót elhagyó részecske a $|0\rangle$ bázisállapotban hagyja el az osztót (az ábrán a felfelé haladó sugárnyalábban találjuk):

$$\frac{1}{\sqrt{2}}(\alpha_0 + \alpha_1).$$

Annak a valószínűségi amplitúdója hogy az osztót elhagyó részecske az $|1\rangle$ bázisállapotban hagyja el az osztót (az ábrán a lefelé haladó sugárnyalábban találjuk):

$$\frac{1}{\sqrt{2}}(\alpha_0 - \alpha_1).$$

Hogyan teljesül, hogy az osztóhoz érkező részecske ugyanannyi



24. ábra. Fénysugár-osztó segítségével megvalósítjuk a Hadamard transzformációt

valószínűséggel halad át mint amennyi valószínűséggel visszaverődik? Legyen $\bar{\alpha}_1 = -\alpha_1$. Ekkor

$$\frac{1}{\sqrt{2}}(\alpha_0 + \bar{\alpha}_1) = \frac{1}{\sqrt{2}}(\alpha_0 - \alpha_1) \text{ és}$$

$$\frac{1}{\sqrt{2}}(\alpha_0 - \bar{\alpha}_1) = \frac{1}{\sqrt{2}}(\alpha_0 + \alpha_1).$$

Két fényosztó egymás utáni alkalmazását tekintjük. Most az output:

$$|\phi\rangle = H \times H |\psi\rangle.$$

Az A és B mátrixok szorzatát $A \times B$ jelöli. Igazoljuk hogy $H \times H = I$! Valóban,

$$H \times H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \mathbf{I}_{2 \times 2}.$$

Tehát $|\phi\rangle = |\psi\rangle$.

A fenti eredményt általánosítjuk. Ha a $|\psi\rangle$ állapotban lévő qubitre $n = 2k$ darab fényosztót alkalmazunk egymás után, akkor a végeredmény megegyezik a kiindulási értékkel. $|\phi\rangle = |\psi\rangle$.

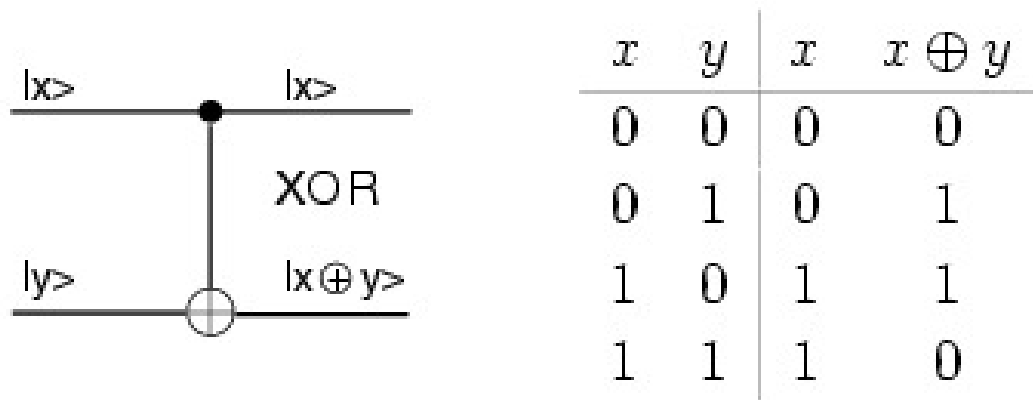
Ha a $|\psi\rangle$ állapotban lévő qubitre $n = 2k + 1$ darab fényosztót alkalmazunk egymás után, akkor a végeredmény megegyezik azazal a végeredménnyel amit egyetlen fényosztó alkalmazásával kapunk:

$$|\phi\rangle = H |\psi\rangle.$$

6.4. Két qubites kvantum kapuk, a CNOT kapu

Most a CNOT kaput írjuk le, lásd a 25. ábrát 26 ábrát.

[22].



25. ábra. A CNOT kvantum kapu [22]

[22]. A CNOT (controlled-not) kapunak két inputja és két outputja van. Az első inputot irányító (más szóval kontrol) inputnak nevezzük, a második inputot cél inputnak nevezzük. A kontrol output megkapja a kontrol input értékét. A cél output értéke megegyezik a cél input értékével ha a kontrol input 0 és a cél output értéke a cél input értékének a negáltja ha a kontrol input 1.

A kvantum CNOT kapunak szintén két inputja van. A kontrol input egy qubit amely a $|\psi\rangle$ állapotban van. A cél input egy qubit amely a $|\phi\rangle$ állapotban van. A kvantum CNOT kapu a kontrol inputot közvetlenül áthelyezi a kontrol outputba. Azaz a kontrol output qubit értékül kapja a kontrol input qubitet. A cél output megegyezik a cél inputtal ha a kontrol input $|0\rangle$. Tegyük fel hogy a kontrol input $|1\rangle$. Ha a cél input $\alpha_0|0\rangle + \alpha_1|1\rangle$, akkor a cél output $\alpha_1|0\rangle + \alpha_0|1\rangle$.

A kvantum CNOT kapu input qubitjeit és output qubitjeit egy-egy vektor reprezentálja a négy dimenziós $\mathcal{H}_4$ Hilbert térben. A kontrol input egy qubit amely a $|\psi\rangle$ állapotban van. A cél input

Before		After	
Control	Target	Control	Target
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

26. ábra. A CNOT kvantum kapu [24]

egy qubit amely a $|\phi\rangle$ állapotban van.

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

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle.$$

A kvantum CNOT kapu input vektora:

$$|V_{CNOT}\rangle = |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

A CNOT kvantum kapu az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |11\rangle \quad |11\rangle \mapsto |10\rangle$$

A CNOT kvantum kapu áthelyezési mátrixa egyenlő az output vektorok és a nekik megfelelő input vektorok külső szorzatainak az összegével.

$$G_{CNOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

Most kiszámoljuk a G_{CNOT} operátor mátrixát. Először kiszámoljuk a $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ bázisvektorokat.

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|00\rangle\langle 00| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} (1000) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$|01\rangle\langle 01| = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} (0100) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$|11\rangle\langle 10| = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} (0010) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|10\rangle\langle 11| = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} (0001) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

A fenti mátrixok összeadásával kapjuk meg a kvantum áramkör G_{CNOT} áthelyező mátrixát.

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

Felidézzük hogy $|V_{CNOT}\rangle$ az input vektor és $|W_{CNOT}\rangle$ az output vektor. Ekkor

$$\begin{aligned}
|W_{CNOT}\rangle &= G_{CNOT}|V_{CNOT}\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \\
&\begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_1 \\ \alpha_1\beta_0 \end{pmatrix} \\
&\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}.
\end{aligned}$$

Tehát $W_{CNOT} = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_1|10\rangle + \alpha_1\beta_0|11\rangle$. Tehát az input vektor első két komponense rendre belemásolódik az output első két komponensébe. Az input vektor harmadik komponense lesz az output vektor negyedik komponense. Az input vektor negyedik komponense lesz az output vektor harmadik komponense.

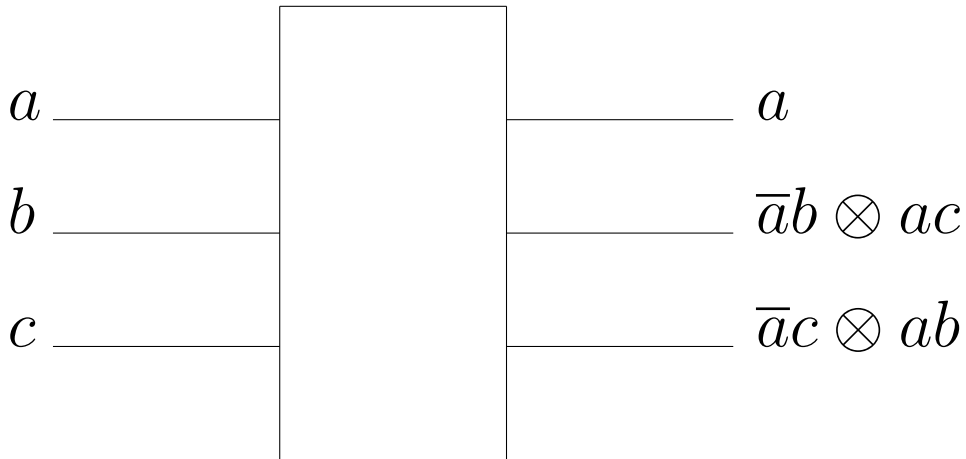
A CNOT kapu megfordítható. Valóban,

$$G_{CNOT}G_{CNOT} = I.$$

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

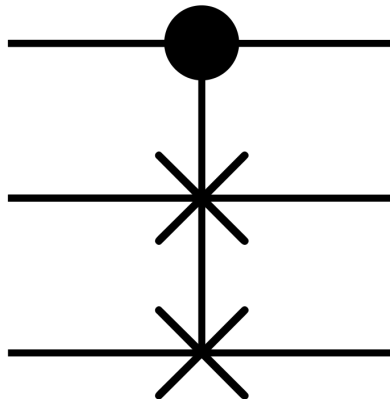
6.5. A Fredkin kapu

A 27. ábrán látható a Fredkin kapu.



27. ábra. A Fredkin kapu

A 28. ábrán látható a Fredkin kapu áramköri jele.



28. ábra. A Fredkin kapu áramköri jele [21]

A klasszikus Fredkin kapu igazság táblája:

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

1. Az a kontrol inputot közvetlenül áthelyezi az outputba: $c' = c$.
2. Amikor $a = 0$, akkor a két cél inputot módosítás nélkül áthelyezi az outputba: $b' = b$, és $c' = c$.
3. Amikor $a = 1$, a két cél input értékét felcseréljük: $b' = c$ és $c' = b$.

Tekintsük a kvantum Fredkin kaput! A három qubitből álló rendszert a nyolc dimenziós $\mathcal{H}_8$ Hilbert térben reprezentáljuk. A bázis nyolc vektorból áll:

$|000\rangle, |001\rangle, |010\rangle, |011\rangle,$
 $|100\rangle, |101\rangle, |110\rangle, |111\rangle,$

Kiszámoljuk a bázisvektorokat.

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|001\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|010\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|011\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|100\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|101\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|110\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

A bázisvektorok rendre megfelelnek az I egységmátrix oszlopainak. Megkonstruáljuk a $\mathbf{G}_{Fredkin}$ operátornak $G_{Fredkin}$ mátrix reprezentációját.

A Fredkin kvantum kapu az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|000\rangle \mapsto |000\rangle \quad |001\rangle \mapsto |001\rangle$$

$$|010\rangle \mapsto |010\rangle \quad |011\rangle \mapsto |011\rangle$$

$$|100\rangle \mapsto |100\rangle \quad |101\rangle \mapsto |110\rangle$$

$$|110\rangle \mapsto |101\rangle \quad |111\rangle \mapsto |111\rangle$$

Eképpen

$$G_{Fredkin} = |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |001\rangle\langle 011| + |100\rangle\langle 100| + |101\rangle\langle 110| + |110\rangle\langle 101| + |111\rangle\langle 111|.$$

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

A $\mathcal{H}_8$ térben a Fredkin kapu $|V_{Fredkin}\rangle$ input vektora a bázisvektorok lineáris kombinációja az α_{000} , α_{001} , α_{010} , α_{011} , α_{100} , α_{101} , α_{110} , α_{111} komplex szám együtthatókkal.

$$|V_{Fredkin}\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle.$$

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

Állítás 6.1 A klaszikus Fredkin kapu megfordítható.

Bizonyítás. A klaszikus Fredkin kapu igazságtáblájának közvetlen vizsgálatával.

□

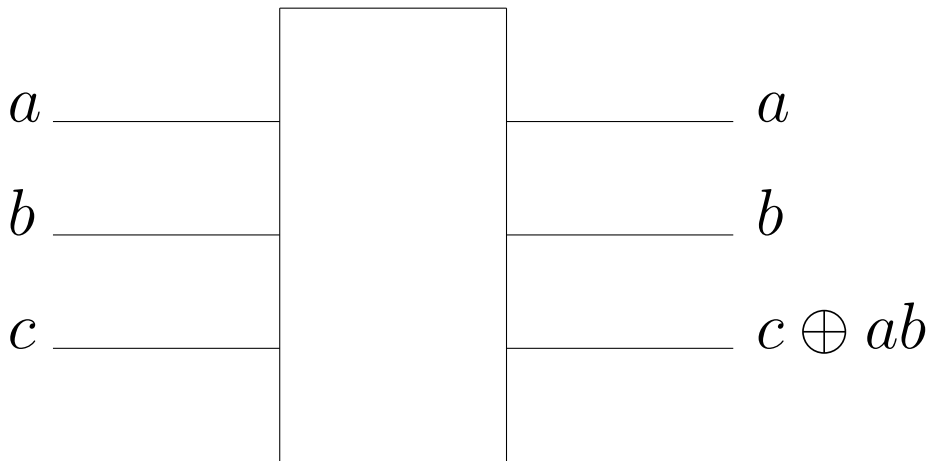
Állítás 6.2 Ha a klasszikus Fredkin kapu outputjára ismét alkalmazzuk a klasszikus Fredkin kaput, akkor visszakapjuk az első kapu inputját.

Bizonyítás. A klaszikus Fredkin kapu igazságtáblájának közvetlen vizsgálatával.



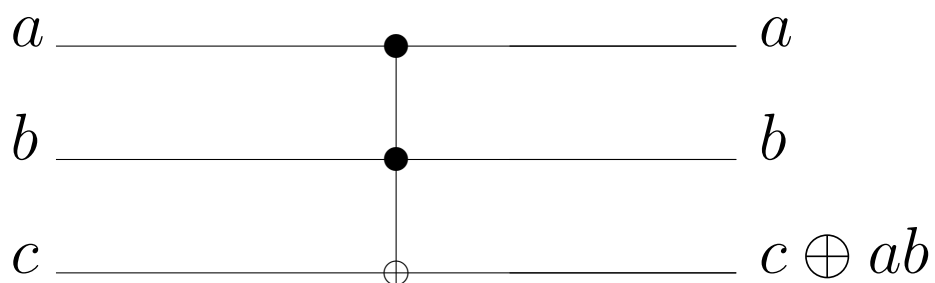
6.6. A Toffoli kapu

A Toffoli kapunak két kontrol inputja van, a és b , és egy cél inputja van, c . A kimenetek $a' = a$, $b' = b$ és c' , lásd 29. ábra.

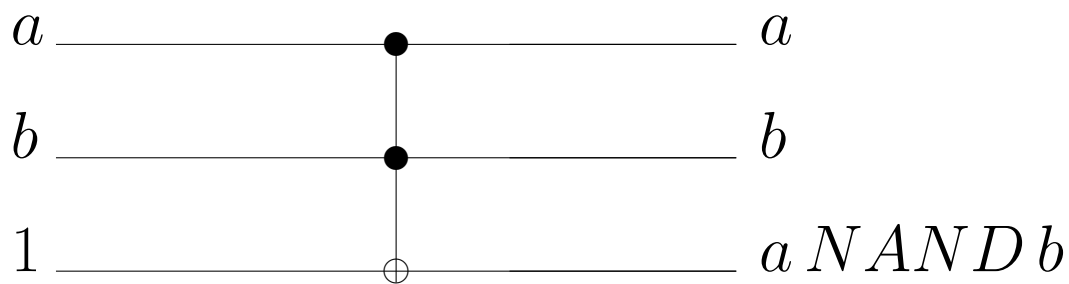


29. ábra. A Toffoli kapu.

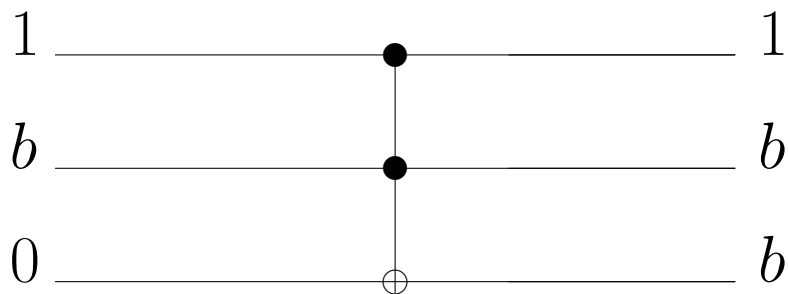
Ha mind a kettő kontrol bit 1, akkor c értéke megváltozik, különben c értéke nem változik. A Toffoli kapu univerzális és megfordítható. A klasszikus Toffoli kapu és a kvantum Toffoli kapu igazság táblája megegyezik. Hasonlóan, a klasszikus Toffoli kapu és a kvantum Toffoli kapu áthelyező függvénye megegyezik.



30. ábra. A Toffoli kapu áramköri jelölése.



31. ábra. A Toffoli kapu segítségével megvalósítjuk a NAND kaput.



32. ábra. A Toffoli kapu megvalósítja a FANOUT függvényt

A klasszikus Toffoli kapu igazság táblája:

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Az igazságtábla közvetlen vizsgálatával kapjuk hogy $c' = c \oplus (a \text{ AND } b)$. Ha $c = 1$ akkor $c' = a \text{ NAND } b$. Ha $c = 0$ akkor $c' = a \text{ AND } b$.

A Toffoli kapu megvalósítja a NAND függvényt, lásd a 31 ábrát.

A FANOUT függvényt a $FANOUT(x) = (x, x)$ egyenlőséggel definiáljuk. A 32. ábra mutatja megvalósítjuk a FANOUT függvényt: amikor $a = 1$ és $c = 0$, akkor $c' = 0 \oplus (1ANDb) = 0 \oplus b = b$. Azaz a második input bitet másoljuk c' -be.

A Toffoli kapu univerzális. Ezt azt jelenti, hogy bármely $f(x_1, \dots, x_m)$ Boole függvényhez létezik olyan Toffoli kapukból álló áramkör amelynek

az inputja $x_1, x_2, \dots, x_m$ és valamennyi segédbit

az outputja $x_1, x_2, \dots, x_m, f(x_1, \dots, x_m)$ és további bitek (szemét).

Ez azt jelenti, hogy Toffoli kapukból fel tudunk építeni egy tetszőleges Boole függvényt kiszámoló áramkört.

A következőkben a kvantum Toffoli kaput vizsgáljuk. Az a, b, c inputnak megfelelő qubiteket rendre $|\psi\rangle, |\phi\rangle$ és $|\zeta\rangle$ jelöli.

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

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$|\zeta\rangle = \gamma_0|0\rangle + \gamma_1|1\rangle$$

Az input állapot a fenti három qubit tenzor szorzata.

$$|V_{Toffoli}\rangle = |\psi\rangle \otimes |\phi\rangle \otimes |\zeta\rangle =$$

$$\alpha_0\beta_0\gamma_0|000\rangle + \alpha_0\beta_0\gamma_1|001\rangle + \alpha_0\beta_1\gamma_0|010\rangle + \alpha_0\beta_1\gamma_1|011\rangle +$$

$$\alpha_1\beta_0\gamma_0|100\rangle + \alpha_1\beta_0\gamma_1|101\rangle + \alpha_1\beta_1\gamma_0|110\rangle + \alpha_1\beta_1\gamma_1|111\rangle$$

Az input állapotot leíró vektor:

$$|V_{Toffoli}\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \gamma_0 \\ \gamma_1 \end{pmatrix} =$$

$$\begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \otimes \begin{pmatrix} \gamma_0 \\ \gamma_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0\gamma_0 \\ \alpha_0\beta_0\gamma_1 \\ \alpha_0\beta_1\gamma_0 \\ \alpha_0\beta_1\gamma_1 \\ \alpha_1\beta_0\gamma_0 \\ \alpha_1\beta_0\gamma_1 \\ \alpha_1\beta_1\gamma_0 \\ \alpha_1\beta_1\gamma_1 \end{pmatrix}$$

Most megkonstruáljuk a $\mathbf{G}_{Toffoli}$ operátor $G_{Toffoli}$ mátrixát. A Toffoli kvantum kapu igazságtáblája alapján a a Toffoli kvantum kapu az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|000\rangle \mapsto |000\rangle \quad |001\rangle \mapsto |001\rangle$$

$$|010\rangle \mapsto |010\rangle \quad |011\rangle \mapsto |011\rangle$$

$$|100\rangle \mapsto |100\rangle \quad |101\rangle \mapsto |101\rangle$$

$$|110\rangle \mapsto |111\rangle \quad |111\rangle \mapsto |110\rangle$$

Eképpen

$$G_{Toffoli} = |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 111| + |111\rangle\langle 110|.$$

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

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

6.7. Kvantum áramkörök

Definíció 6.3 Kvantum számítógépnek nevezzük az n qubitből álló rendszert amelyre az alábbi műveletek hajthatók végre:

1. Minden qubitnek a kezdőértékét beállíthatjuk a $|0\rangle$ értékre.
2. Minden qubitet megmérhetünk a $\{|0\rangle, |1\rangle\}$ bázisban.
3. Véges sokszor, tetszés szerint alkalmazhatunk kvantum kaput a qubitek tetszőleges, rögzített nagyságú részhalmazára.
4. A qubitek kizárólag a fenti transzformációk szerint fejlődnek.

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

1. Az áramkörök nem tartalmazznak kört. Nincsen visszacsatolás.
2. Nem tudunk ismeretlen qubitet értékének megőrzésével másolni.

6.8. Nem tudunk ismeretlen qubitet értékének megőrzésével másolni (klónozni)

Állítás 6.4 Nem tudunk ismeretlen qubitet értékének megőrzésével másolni (klónozni).

Bizonyítás. Tegyük fel hogy van egy olyan két qubites kapu amely képes valamelyik inputját értékének megőrzésével másolni. A kapu lineáris transzformációt hajt végre. 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 egymásra merőleges qubit állapot. Az első input előbb a $|\psi\rangle$ és azután a $|\phi\rangle$ állapot lesz, mindkét esetben a második input a $|0\rangle$ qubit 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. $|\xi\rangle$ legyen a másoló kapu első inputja és $|0\rangle$ qubit a második inputja. Mivel $\mathbf{G}$ lineáris transzformáció,

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

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

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

$$\begin{aligned} \mathbf{G}(|\xi 0\rangle) &= |\xi\xi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) \otimes \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) = \\ &= \frac{1}{2}(|\psi\psi\rangle + |\psi\phi\rangle + |\phi\psi\rangle + |\phi\phi\rangle) \neq \frac{1}{\sqrt{2}}(|\psi\psi\rangle + |\phi\phi\rangle). \end{aligned}$$

Ellentmondás.

A fenti bizonyítást természetes módon általánosíthatjuk tetszőleges kvantum számítógépre.

□

Szemléletesen: a kvantum rendszer állapotának két példánya szigorúan több információt tartalmaz mint egy példány. Ezért nem lehet másolni az ismeretlen kvantum állapotot.

6.9. A qubit felcserélése és az összeadás áramkörök

A 33. ábrán két bit összeadására szolgáló áramkört látunk. Az áramkört megfordítható kapukból építettük fel. Az áramkör egy Toffoli kapuból és egy CNOT kapuból áll. A CNOT kapu követi a Toffoli kaput. A Toffoli kapu két kontrol inputja a és b . A Toffoli kapu cél inputja $c = 0$. A Toffoli kapu cél outputja $c' = a \text{ AND } b$. Ez az állapot jelenik meg az áramkör outputján. $c'' = c' = a \text{ AND } b$.

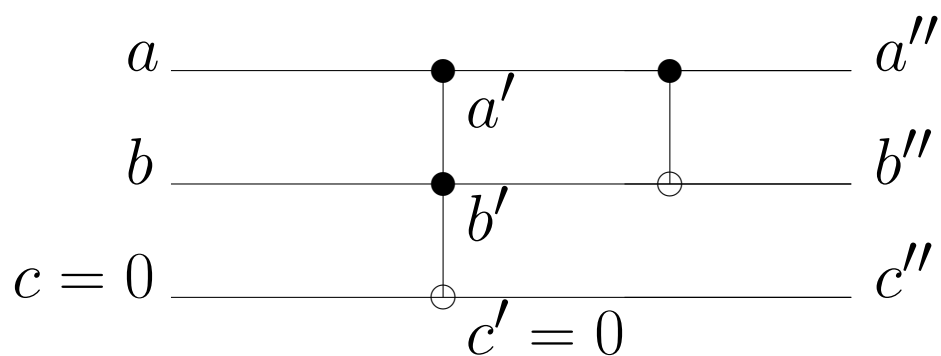
A CNOT kapu $a' = a$ kontrol inputja változatlanul kerül ki az outputra: $a'' = a' = a$. A CNOT kapu cél inputja $b' = b$. A CNOT kapu cél outputja:

$$b'' = (a' \text{ XOR } b') = (a \text{ XOR } b).$$

$$a'' = a$$

$$b'' = Sum = aXORb$$

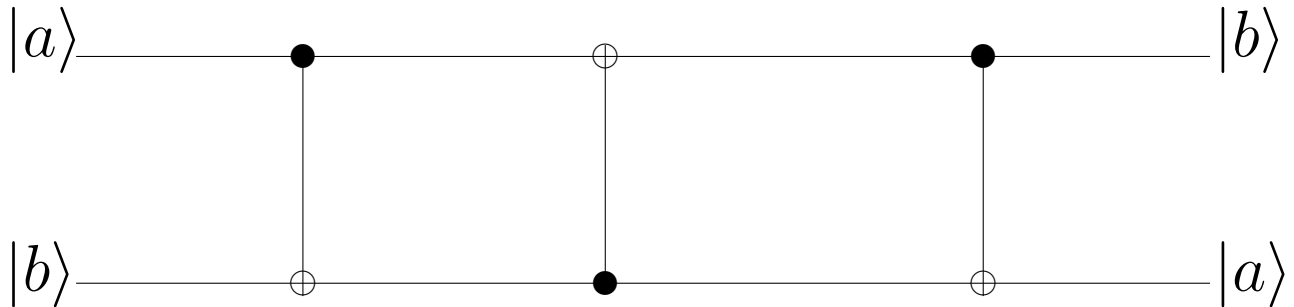
$$c'' = CarryOut = aANDB \oplus ab$$



33. ábra. Két bitet összeadó áramkör.

Tehát az áramkör két outputja az a , b inputok összege és az összeadás kimenő maradéka.

A 34. ábrán látható áramkör felcseréli a két input qubitet.



34. ábra. Két qubitet felcserélő kvantum áramkör

Az áramkör három CNOT kapuból áll.

Az első qubit értéke rendre: $|a\rangle$, $|a\rangle$, $|a \oplus (a \oplus b)\rangle$, $|b\rangle$.

A második qubit értéke rendre: $|b\rangle$, $|a \oplus b\rangle$, $|a \oplus b\rangle$, $|a\rangle$.

Felhasználjuk hogy

$$a \oplus (a \oplus b) = (a \oplus a) \oplus b = b$$

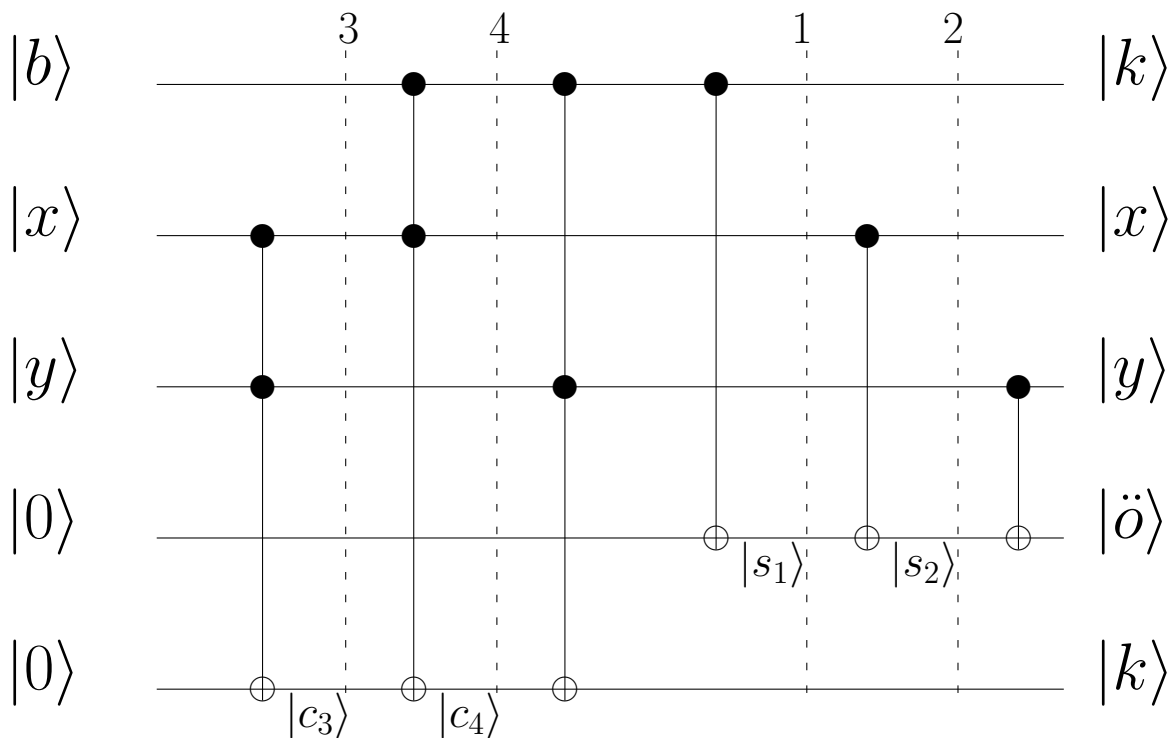
$$b \oplus (b \oplus a) = (b \oplus b) \oplus a = a$$

$$a \oplus a = 0$$

és

$$0 \oplus b = b.$$

A 35 ábrán két qubit összeadására szolgáló kvantum áramkört látunk. A két qubit összeadásakor bejövő maradékot figyelembe vesszük és a kimenő maradékot kiszámoljuk. Az áramkör Toffoli és CNOT kapukból áll. b a bejövő maradék, x és y az összeadandó bitek, k a kimenő maradék. A felső három qubit: $|b\rangle$, $|x\rangle$, és $|y\rangle$ a kontrol qubitek az áramkör minden kapuján. Így változtatás nélkül az outputra mennek. Az 1 pontban a CNOT



35. ábra. Két qubit összeadására szolgáló kvantum áramkör

transzformáció eredményét $|s_1\rangle$ jelöli. A 2 pontban a CNOT transzformáció eredményét $|s_2\rangle$ jelöli.

$$|s_1\rangle = |c \oplus 0\rangle = |c\rangle,$$

$$|s_2\rangle = |s_1 \oplus x\rangle = |c \oplus x\rangle,$$

$$|\ddot{o}\rangle = |s_2 \oplus y\rangle = |(c \oplus x) \oplus y\rangle.$$

Állítás 6.5 $|(c \oplus x) \oplus y\rangle = |xyc + x\bar{y}\bar{c} + y\bar{x}\bar{c} + c\bar{x}\bar{y}\rangle$.

Bizonyítás. Ehhez elegendő belátni hogy

$$(c \oplus x) \oplus y = xyc + x\bar{y}\bar{c} + y\bar{x}\bar{c} + c\bar{x}\bar{y}.$$

1. A bizonyítás történhet mindkét oldal igazság táblájának a megkonstruálásával majd a két igazság tábla összehasonlításával.

2. A bizonyítás történhet úgy hogy a bizonyítás során felhasználjuk hogy

$$x \oplus y = x\bar{y} + \bar{x}y$$

és

$$\overline{x + y} = \overline{xy}$$

$$\text{és } \overline{xy} = \overline{x} + \overline{y}.$$

□

A 6.1 alfejezetben igazoltuk hogy a A 6.5 állításban szereplő egyenlőség jobb oldala a két bit összege.

Az első Toffoli kapu cél qubitje a $|c_3\rangle$ output értéket veszi fel a 3 pontban.

Az második Toffoli kapu cél qubitje a $|c_4\rangle$ output értéket veszi fel a 4 pontban.

$$|c_3\rangle = |0 \oplus (xy)\rangle = |xy\rangle$$

$$|c_4\rangle = |c_3 \oplus (bx)\rangle = |(xy) \oplus (bx)\rangle$$

$$|Carryout\rangle = |c_4 \oplus (by)\rangle = |(xy) \oplus (bx) \oplus (by)\rangle$$

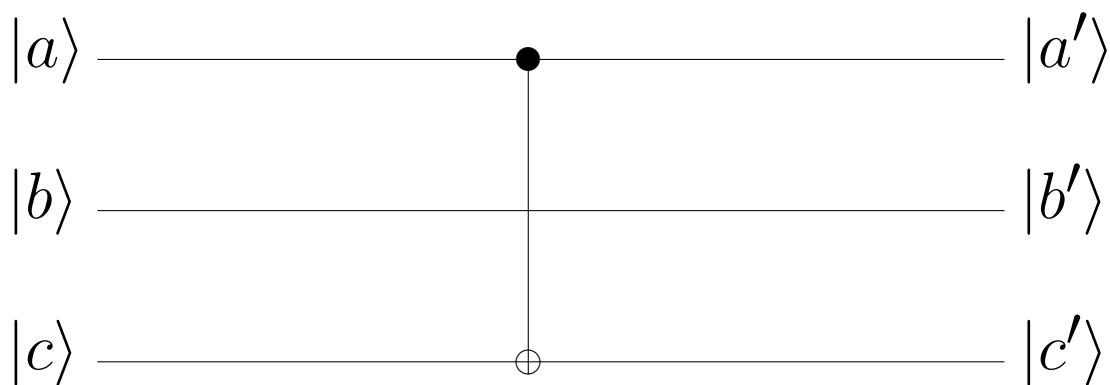
Könnyen látható hogy $(xy) \oplus (bx) \oplus (by) = xyb + \overline{x}yb + x\overline{y}b + xy\overline{b}$.

$$\text{Tehát } |k\rangle = |xyb + \overline{x}yb + x\overline{y}b + xy\overline{b}\rangle.$$

A 6.1 alfejezetben igazoltuk hogy ha eltekintünk a vektor reprezentációtól, akkor a fenti egyenlőség jobb oldala a kimenő maradék.

Tekintsük a 36. ábrán látható kvantum áramkört és konstruáljuk meg a transzfer mátrixát!

A legfelső $|a\rangle$ qubit a CNOT kapu kontrol qubitje. Eképpen változatlanul kerül ki az outputra: $|a'\rangle = |a\rangle$. A második qubit nem módosul: $|b'\rangle = |b\rangle$. A harmadik qubit ellenkező értékre változik ha $|a\rangle = |1\rangle$, különben nem változik. Az áramkör igazság táblája:



36. ábra. 3-qubites CNOT kapu

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	1	0

A kvantum áramkör az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|000\rangle \mapsto |000\rangle \quad |001\rangle \mapsto |001\rangle$$

$$|010\rangle \mapsto |010\rangle \quad |011\rangle \mapsto |011\rangle$$

$$|100\rangle \mapsto |101\rangle \quad |101\rangle \mapsto |100\rangle$$

$$|110\rangle \mapsto |111\rangle \quad |111\rangle \mapsto |110\rangle$$

Eképpen $\mathbf{G}_{3,CNOT} = |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| +$

$$|100\rangle\langle 101| + |101\rangle\langle 100| + |110\rangle\langle 111| + |111\rangle\langle 110|.$$

Miután kiszámítjuk a külső szorzatokat és összeadjuk a mátrixokat kapjuk hogy

$$G_Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

6.10. Unitér transzformációk és forgatási mátrixok

Tekintsük az alábbi operátorokat!

1. A Hadamard (H) operátor.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

2. A fázis (S) operátor.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

3. A $\frac{\pi}{8}$ (T) operátor.

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

4. A θ szöggel való fázis eltolás (P_θ)

$$P_\theta = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

$$5. R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$6. \text{ Minden } k \geq 0 \text{ számra, } R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

Emlékeztető:

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

A qubit a Bloch gömb felszínének bármely pontja által kijelölt állapotot felveheti értékéül. Azaz a qubit állapotát egy egységvektor írja le amely a Bloch gömb felszínének valamely pontjára mutat. Amikor egy transzformációt alkalmazunk a qubit állapotára akkor a neki megfelelő vektort szintén transzformáljuk. Különösen érdekel minket a vektornak az x , y , z tengelyek körüli θ szöggel való elforgatása. A fenti három elforgatást $\mathcal{R}_x(\theta)$ $\mathcal{R}_y(\theta)$ $\mathcal{R}_z(\theta)$ jelöli. A fenti három elforgatást a σ_X , σ_Y és σ_Z Pauli mátrixok segítségével valósítjuk meg.

$$\mathcal{R}_X(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\sigma_X = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

$$\mathcal{R}_y(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\sigma_Y = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

$$\mathcal{R}_z(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\sigma_Z = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix},$$

A rotációs mátrixok kielégítik az alábbi feltételeket:

$$\mathcal{R}_y(\theta_1)\mathcal{R}_y(\theta_2) = \mathcal{R}_y(\theta_1 + \theta_2),$$

$$\mathcal{R}_z(\theta_1)\mathcal{R}_z(\theta_2) = \mathcal{R}_z(\theta_1 + \theta_2),$$

$$\sigma_X\mathcal{R}_y(\theta)\sigma_X = \mathcal{R}_y(-\theta),$$

$$\sigma_X\mathcal{R}_z(\theta)\sigma_X = \mathcal{R}_z(-\theta),$$

Állítás 6.6 Minden U unitér 2×2 -es mátrix az alábbi alakban írható fel:

$$U = e^{i\alpha}\mathcal{R}_z(\beta)\mathcal{R}_y(\gamma)\mathcal{R}_z(\delta),$$

valamely $\alpha, \beta, \gamma, \delta$ valós számokra.

Szemléletesen, itt $e^{i\alpha}$ komplex szám átfogó fázis faktor, és $e^{i\alpha}$ értéke nem mutatható ki kísérleti eszközzel és ezért $e^{i\alpha}$ -t a továbbiakban figyelmen kívül hagyjuk.

Állítás 6.7 Minden U unitér 2×2 -es mátrix esetén, meg tudunk adni olyan A, B, C unitér 2×2 -es mátrixokat hogy

$$1. \ ABC = I \text{ és}$$

$$2. \ U = A\sigma_X B\sigma_X C.$$

Itt σ_X a korábban definiált Pauli mátrix.

Bizonyítás. A megelőző állítás szerint:

$$U = \mathcal{R}_z(\beta)\mathcal{R}_y(\gamma)\mathcal{R}_z(\delta)$$

valamely β, γ, δ valós számokra.

Legyen

$$A = \mathcal{R}_z(\beta)\mathcal{R}_y\left(\frac{\gamma}{2}\right)$$

$$B = \mathcal{R}_y(-\frac{\gamma}{2})\mathcal{R}_z(-\frac{\delta+\beta}{2})$$

$$C = \mathcal{R}_z(\frac{\delta-\beta}{2}).$$

Lássuk be hogy $ABC = I$. Valóban,

$$ABC = \mathcal{R}_z(\beta)\mathcal{R}_y(\frac{\gamma}{2})\mathcal{R}_y(-\frac{\gamma}{2})\mathcal{R}_z(-\frac{\delta+\beta}{2})\mathcal{R}_z(\frac{\delta-\beta}{2})$$

A forgatási mátrixok tulajdonságainak a felhasználásával:

$$\mathcal{R}_y(\frac{\gamma}{2})\mathcal{R}_y(-\frac{\gamma}{2}) = \mathcal{R}_y(\frac{\gamma}{2} - \frac{\gamma}{2}) = \mathcal{R}_y(0) = I.$$

Továbbá

$$\mathcal{R}_z(\beta)\mathcal{R}_z(-\frac{\delta+\beta}{2})\mathcal{R}_z(\frac{\delta-\beta}{2}) = \mathcal{R}_z(\beta - \frac{\delta+\beta}{2} + \frac{\delta-\beta}{2}) = \mathcal{R}_z(0) = I.$$

Számoljuk ki $A\sigma_X B\sigma_X C$ -t! Mivel $\sigma_X\sigma_X = I$, beszúrjuk $\sigma_X\sigma_X$ -et $A\sigma_X B\sigma_X C$ kifejtésébe.

$$A\sigma_X B\sigma_X C = A(\sigma_X \mathcal{R}_y(-\frac{\gamma}{2})\sigma_X)(\sigma_X \mathcal{R}_z(-\frac{\delta+\beta}{2})\sigma_X)C$$

Mivel

$$\sigma_X \mathcal{R}_y(-\frac{\gamma}{2})\sigma_X = \mathcal{R}_y(\frac{\gamma}{2}),$$

$$\sigma_X \mathcal{R}_z(-\frac{\delta+\beta}{2})\sigma_X = \mathcal{R}_z(\frac{\delta+\beta}{2}),$$

így

$$A\sigma_X B\sigma_X C = \mathcal{R}_z(\beta)\mathcal{R}_y(\gamma)\mathcal{R}_z(\delta) = U.$$

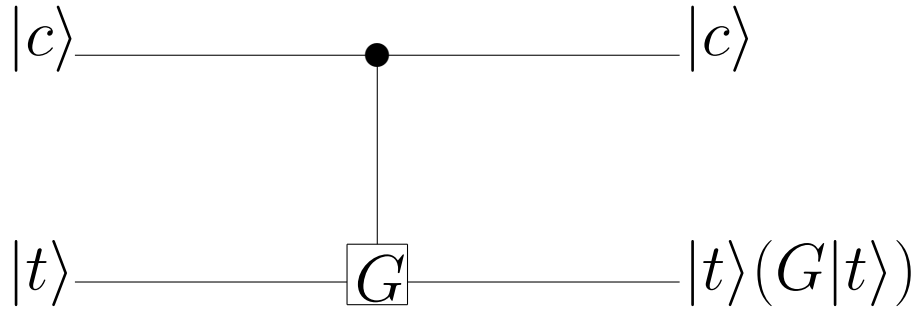
□

6.11. Egyetlen qubit által irányított műveletek

A 37. ábrán látható általános kvantum áramkör az alábbi módon számol.

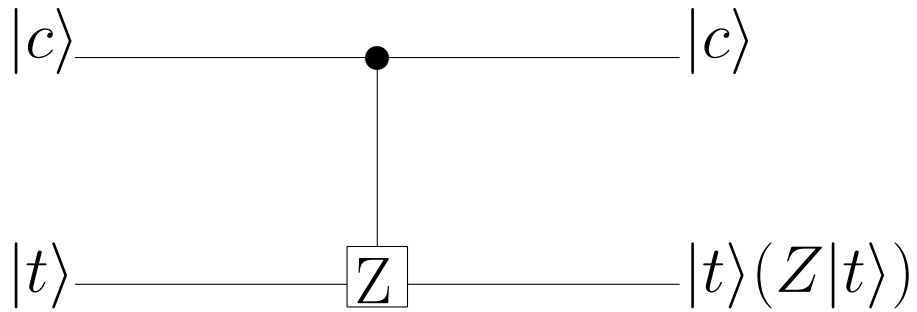
1. ha a $|c\rangle$ kontrol qubit értéke $|0\rangle$, akkor a $|t\rangle$ cél qubit közvetlenül az outputra kerül.

2. ha a $|c\rangle$ kontrol qubit értéke $|1\rangle$, akkor a G által megvalósított transzformációt alkalmazzuk a $|t\rangle$ cél qubitre.



37. ábra. irányított G művelet

Az irányított-Z művelet.



38. ábra. irányított Z művelet

A 38. ábrán láthatjuk az irányított-Z művelet kvantum áramkörét. Emlékezzünk hogy a Z kapu a második input komponenst -1 -gyel szorozza meg. A kapu által megvalósított transzformáció mátrixa:

$$Z = \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Eképpen

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle.$$

A fentiek alapján az irányított-Z kapu az alábbi transzformációt

hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |01\rangle$$

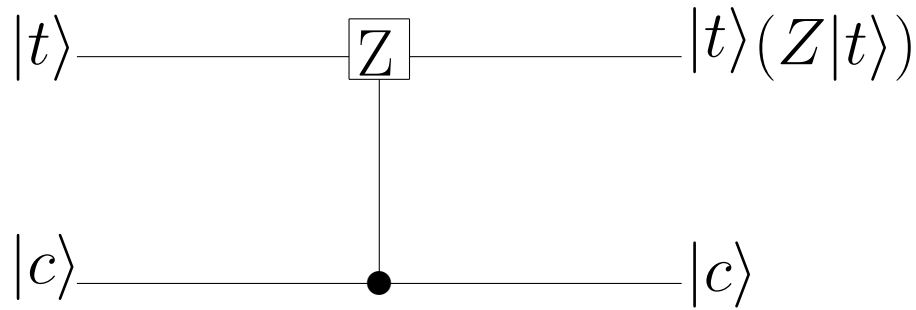
$$|10\rangle \mapsto |10\rangle \quad |11\rangle \mapsto -|11\rangle.$$

Számítsuk ki az irányított-Z kapu áthelyező mátrixát!

$$G_{irányít-Z} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$G_{irányít-Z} = \begin{pmatrix} I_2 & \mathbf{0} \\ \mathbf{0} & \sigma_z \end{pmatrix}.$$

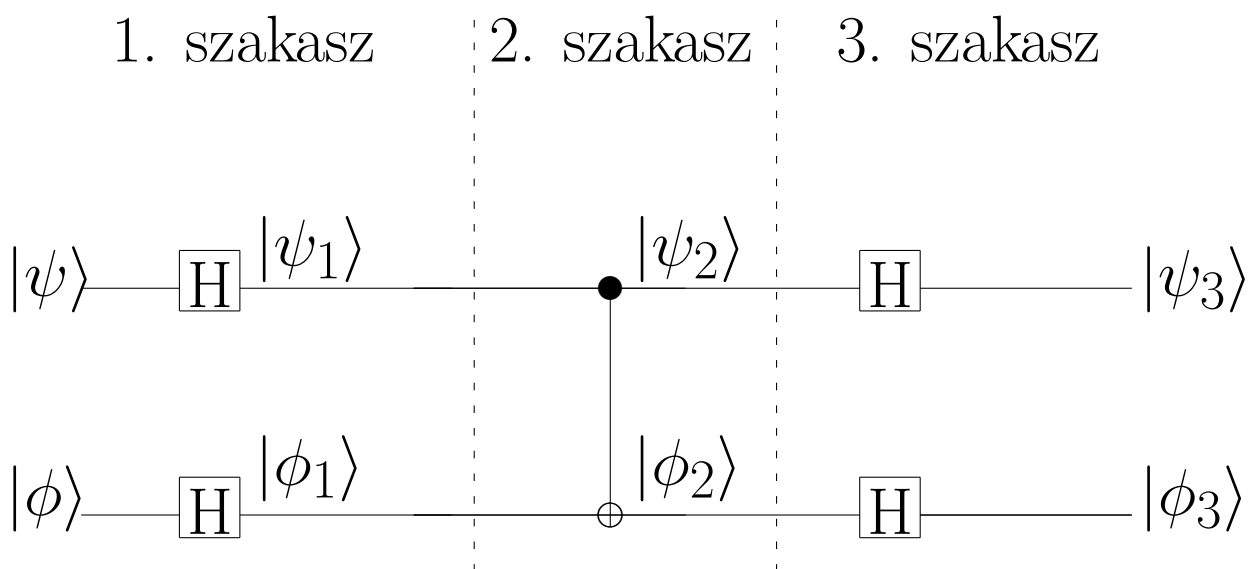


39. ábra. Felcseréltük az irányító qubit és a cél qubit szerepét az irányított Z műveletben

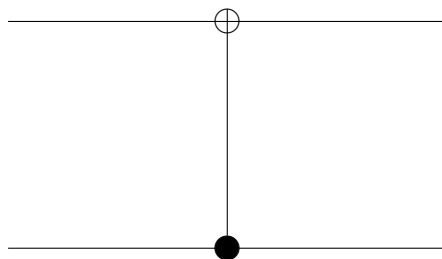
Nyilvánvaló hogy a 39. ábrán látható áramkör ekvivalens a 38. ábrán látható áramkörrel.

Tekintsük az ekvivalens quantum áramköröket tartalmazó 40. és 41. ábrákat.

G_a jelöli a 40. ábrán látható áramkör áthelyezési mátrixát.



40. ábra. Az irányító és a cél qubit szerepének felcserélése, első ábra



41. ábra. Az irányító és a cél qubit szerepének felcserélése, második ábra

$$|\xi\rangle = |\psi\rangle \otimes |\phi\rangle, |\xi_1\rangle = |\psi_1\rangle \otimes |\phi_1\rangle = H \otimes H |\xi\rangle, |\xi_2\rangle = |\psi_2\rangle \otimes |\phi_2\rangle = G_{CNOT} |\xi_1\rangle, |\xi_3\rangle = |\psi_3\rangle \otimes |\phi_3\rangle = H \otimes H |\xi_2\rangle = G_a |\xi\rangle.$$

Az irányító qubit és a cél qubit szerepét meg tudjuk cserélni a bázis megfelelő megváltoztatásával a 40. ábrán látható módon. Az ábrán három fejlődési szakaszt jelöltünk be.

Két módszert ismertetünk. Az első módszer nem elég általános.

1. módszer: megfigyeljük az egyes qubitek értékének alakulását az egyes szakaszokban.

Először $|\psi\rangle$ -nek, az első qubitnek, az értékének az alakulását tekintjük. Az első fejlődési szakaszban a

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

qubitre alkalmazzuk a Hadamard kaput.

$$|\psi_1\rangle = H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 + \alpha_1 \\ \alpha_0 - \alpha_1 \end{pmatrix}$$

A második szakasz nem változtatja meg az első qubit állapotát, mivel az első qubit a CNOT kapu irányító qubitje. Tehát $|\psi_2\rangle = |\psi_1\rangle$. A harmadik szakasz az alábbi módon változtatja meg az első qubit állapotát:

$$|\psi_3\rangle = H|\psi_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 + \alpha_1 \\ \alpha_0 - \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}.$$

Tehát $|\psi_3\rangle = |\psi\rangle$.

Most $|\phi\rangle$ -nek, a második qubit értékének, a fejlődését követjük nyomon.

$$|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$$

Az első fejlődési szakaszban $|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$ qubitre alkalmazzuk a Hadamard kaput.

$$|\phi_1\rangle = H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \beta_0 + \beta_1 \\ \beta_0 - \beta_1 \end{pmatrix}$$

A második szakaszban $|\phi_2\rangle$ értéke az irányító qubittól függ. Az 1. módszer most nem működik.

A következőkben egy általánosabb módszert követünk.

2. módszer: megkonstruáljuk minden egyes fejlődési szakasz áthelyezési mátrixát, a G_1 , G_2 és G_3 mátrixokat, majd összeszorozzuk őket. Így megkapjuk az egész áramkör áthelyezési mátrixát. Tekintsük az első fejlődési szakaszt.

$$G_1 = H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

A második szakasz áthelyezési mátrixa:

$$G_2 = G_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Az első két szakasz áthelyezési mátrixa:

$$G_2 G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} =$$

$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

A harmadik fejlődési szakasz áthelyezési mátrixa

$$G_3 = H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Az egész áramkör áthelyezési mátrixa

$$G_a = G_3 G_2 G_1 = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} =$$

$$\frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix}$$

Tehát $G_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Az input állapot $|\xi\rangle = |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$.

A rendszer állapota a harmadik fejlődési szakasz után:

$$|\xi_3\rangle = G_a|\xi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_1\beta_1 \\ \alpha_1\beta_0 \\ \alpha_0\beta_1 \end{pmatrix}.$$

Tekintsük a 41. ábrát. Az itt látható kvantum áramkör az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |11\rangle$$

$$|10\rangle \mapsto |10\rangle \quad |11\rangle \mapsto |01\rangle.$$

Az áramkör áthelyezési mátrixa: $G_b = |00\rangle\langle 00| + |11\rangle\langle 01| + |10\rangle\langle 10| + |01\rangle\langle 11|$. Így $G_b =$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

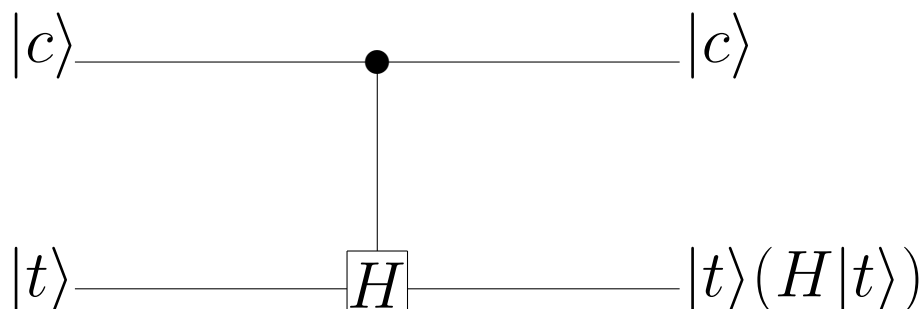
Tehát

$$G_b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Azt kapjuk hogy $G_a = G_b$.

Ezzel beláttuk hogy a 40. ábrán és a 41. ábrán szereplő kvantum áramkörök ugyanazt a leképezést valósítják meg. Azaz ekvivalensek.

6.12. Az irányított H művelet



42. ábra. Az irányított H művelet

Tekintsük a 42. ábrát! Itt az irányított H műveletet megvalósító kvantum áramkört látjuk. Az itt látható kvantum áramkör az

alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$\begin{aligned} |00\rangle &\mapsto |00\rangle, & |01\rangle &\mapsto |01\rangle, \\ |10\rangle &\mapsto |1\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & |11\rangle &\mapsto |1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Az áramkör áthelyezési mátrixa:

$$\begin{aligned} \mathbf{G}_b &= |00\rangle\langle 00| + \\ &|01\rangle\langle 01| + \\ &|1\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 10| + \\ &|1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 11| \end{aligned}$$

Így $\mathbf{G}_{iranyit-H} =$

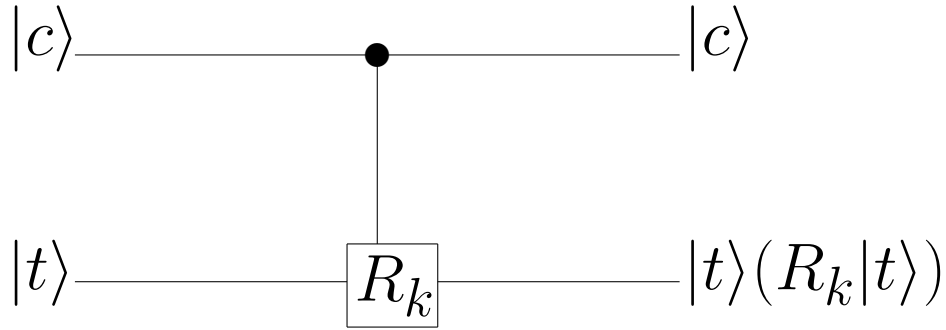
$$\begin{aligned} &\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} = \\ &\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \end{aligned}$$

Tehát

$$\mathbf{G}_{iranyit-H} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} I_2 & \mathbf{0} \\ \mathbf{0} & H \end{pmatrix}.$$

6.13. Az irányított R_k művelet

Minden $k \geq 0$ számra, $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$



43. ábra. irányított R_k művelet

A 43. ábra mutatja az irányított R_k műveletet megvalósító kvantum áramkört. Az itt látható kvantum áramkör az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |10\rangle \quad |11\rangle \mapsto e^{\frac{2\pi i}{2^k}} |11\rangle$$

Az áramkör áthelyezési mátrixa: $\mathbf{G}_{iranyit-R_k} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{\frac{2\pi i}{2^k}} |11\rangle\langle 11|$.

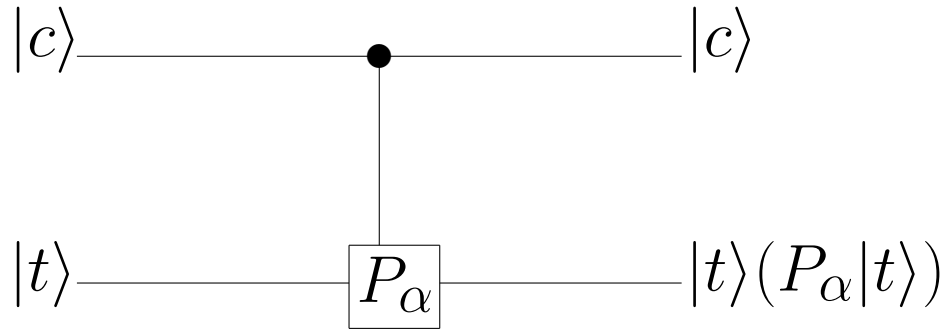
Így

$$\mathbf{G}_{iranyit-R_k} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix} \\
= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

6.14. Az irányított P_α művelet

A 44. ábrán láthatjuk az irányított P_α művelet kvantum áramkörét.



44. ábra. Az irányított P_α művelet

A 45 ábrán láthatjuk a fázis eltolás kvantum áramkörét.

Legyen α tetszőleges valós szám. P_α a fázis eltolás transzformáció. Az áthelyezési mátrixa: $P_\alpha = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$.

T_α a fázis transzformáció. Az áthelyezési mátrixa:

$$|c\rangle \text{-----} \boxed{T_\alpha} \text{-----} T_\alpha |c\rangle$$

$$|t\rangle \text{-----} |t\rangle$$

45. ábra. A T_α művelet

$$T_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

A 44. ábrán láthatjuk az irányított-P áramkört. Az itt látható kvantum áramkör az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

$$\begin{aligned} |00\rangle &\mapsto |00\rangle & |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto e^{i\alpha}|10\rangle, & |11\rangle &\mapsto e^{i\alpha}|11\rangle. \end{aligned}$$

Az áramkör áthelyezési mátrixa: $\mathbf{G}_b = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\alpha}|10\rangle\langle 10| + e^{i\alpha}|11\rangle\langle 11|$

Így

$$\mathbf{G}_{iranyit-P} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

Tehát

$$\mathbf{G}_{iranyit-P} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}.$$

Tekintsük a 45. ábrát! Itt α tetszőleges valós szám. T_α a fázis transzformáció. Az áthelyezési mátrixa:

$$T_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

A 45. ábrán látható kvantum áramkör áthelyezési mátrixa:

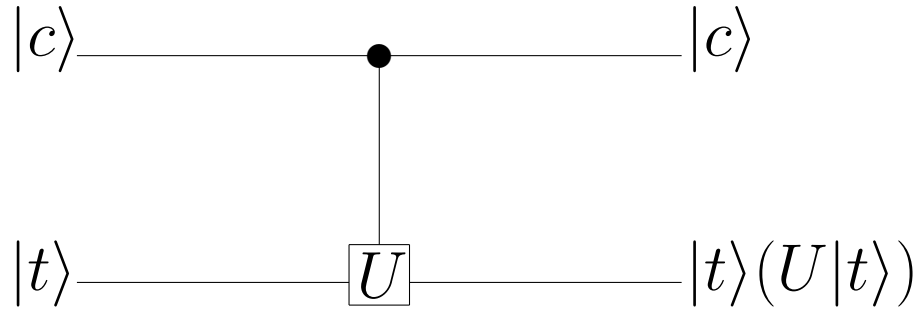
$$G_{T_\alpha} = T_\alpha \otimes I = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}.$$

Tehát $\mathbf{G}_{iranyit-P} = G_{T_\alpha}$. A két kvantum áramkör ekvivalens.

Legyen U egy tetszőleges egy qubit irányított kvantum kapu. Az A , B és C forgatási mátrixokat a 6.10 fejezetben adtuk meg U -hoz. Felidézzük hogy

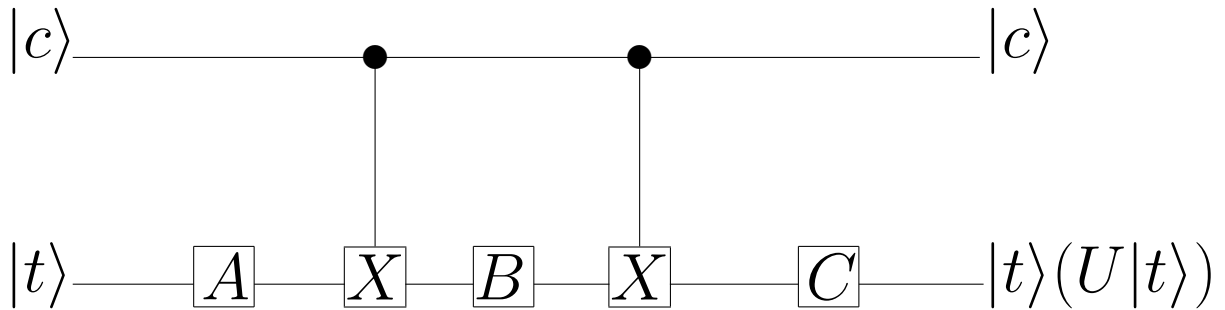
1. $ABC = I$ és
2. $U = A\sigma_X B\sigma_X C$.

Itt σ_X a korábban definiált Pauli mátrix.



46. ábra. Az irányított U művelet

Tekintsük a 46. és 47. ábrákat!



47. ábra. Az irányított U művelet utánzása

A 47. ábrán látható áramkör utánozza az 46. ábrán látható áramkört. Az első kapu a C kapu, második kapu a B kapu és a harmadik kapu az A kapu. Az X mátrixszal balról való szorzás a $|0\rangle$ qubithez a $|1\rangle$ qubitet rendeli és az $|1\rangle$ qubithez a $|0\rangle$ qubitet rendeli. Az X mátrixhoz rendeltük a σ_X transzformációt.

Ha az irányító qubit $|c\rangle = |0\rangle$, akkor a cél qubit

$$|t\rangle \mapsto ABC|t\rangle = I|t\rangle = |t\rangle.$$

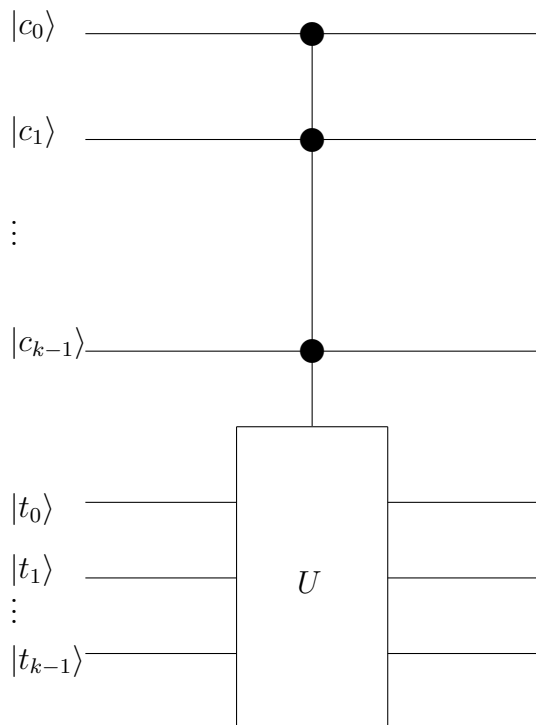
Ha az irányító qubit $|c\rangle = |1\rangle$, akkor a cél qubit

$$|t\rangle \mapsto A\sigma_X B\sigma_X C|t\rangle = U|t\rangle.$$

Tehát a 46. és 47. ábrákon látható két áramkör ugyanazt a transzformációt számolja ki.

6.15. Több qubit által irányított műveletek

Tekintsük a 48. ábrát!



48. ábra. n darab irányító qubit, k darab cél qubit, az U unitér transzformációt alkalmazzuk a k darab cél qubitre

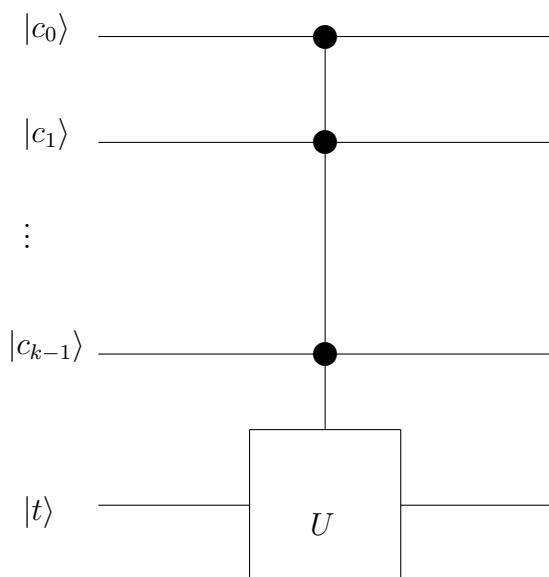
Itt azt a kvantum áramkört látjuk amely az $\mathbf{U}$ unitér transzformációt hajtja végre a

$$|c_0\rangle, |c_1\rangle, \dots, |c_{n-1}\rangle$$

input irányító qubittel és

$$|t_0\rangle, |t_1\rangle, \dots, |t_{k-1}\rangle$$

input cél qubittel. A 49. ábrán a $k = 1$ eset látható. Tekintsük a 49. ábrát! Az $\mathbf{U}$ unitér operátor U mátrixát az alábbi módon adjuk meg:



49. ábra. n darab irányító qubit, 1 darab cél qubit, az U unitér transzformációt alkalmazzuk a cél qubitre

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}.$$

Az itt látható kvantum áramkör az alábbi transzformációt hajtja végre. Tegyük fel hogy minden egyes irányító input qubit a $|0\rangle$ és $|1\rangle$ bázisvektorok valamelyike. Ha az összes irányító input qubit értéke $|1\rangle$ akkor az $\mathbf{U}$ operátort alkalmazzuk a $t = \alpha_0|0\rangle + \alpha_1|1\rangle$ cél qubitre. Továbbá az irányító qubitek közvetlenül az outputra kerülnek.

Ha $c_0 \text{ AND } c_1 \text{ AND } \dots \text{ AND } c_{n-1} = 0$ akkor az input qubitek közvetlenül az outputra kerülnek.

Állítás 6.8 A kvantum áramkör áthelyező mátrixa az alábbi $2^{n+1} \times 2^{n+1}$ méretű mátrix.

$$V = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & u_{00} & u_{01} \\ 0 & 0 & \dots & 0 & u_{10} & u_{11} \end{pmatrix}$$

Bizonyítás vázlat 1. Tegyük fel hogy az összes irányító input qubit értéke $|1\rangle$. Ekkor az irányító input qubitek tenzor szorzata:

$$|11\dots 1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Ezért a $t = \alpha_0|0\rangle + \alpha_1|1\rangle$ cél qubittel való tenzorszorzás elvégzése után kapjuk hogy az input

$$|11\dots 1t\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \alpha_0 \\ \alpha_1 \end{pmatrix}$$

Most a V mátrixszal balról megszorozzuk az input vektort. A V mátrisszal való szorzás tényleg 49. ábrán látható $\mathbf{U}$ transzformációt hajtja végre a cél qubiten. Az irányító qubitek értéke nem változik.

2. Tegyük fel hogy az utolsó irányító input qubit értéke $|0\rangle$, és a többi irányító input qubit értéke $|1\rangle$. Ekkor az irányító input qubitek tenzor szorzata:

$$|11\dots 10\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$$

Ezért a $t = \alpha_0|0\rangle + \alpha_1|1\rangle$ cél qubittel való tenzorszorzás elvégzése után kapjuk hogy az input

$$|11...10t\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \alpha_0 \\ \alpha_1 \\ 0 \\ 0 \end{pmatrix}$$

Most a V mátrixszal balról megszorozzuk a fenti vektort, azaz a $|c_0\rangle|c_1\rangle \dots |c_{n-1}\rangle|t\rangle$ tenzor szorzatot leíró input vektort. Eredményül megkapjuk a fenti input vektort. Tehát a V mátrisszal való szorzás tényleg 49. ábrán látható áramkörhöz tartozó transzformációt hajtja végre.

3. Általános eset: tegyük fel hogy az irányító input qubitek között van $|0\rangle$ qubit. Tekintsük az irányító input qubitek

$$|c_0\rangle|c_1\rangle \dots |c_{n-1}\rangle$$

tenzor szorzatát leíró vektort. Annak az utolsó komponense 0. Ezért a $|c_0\rangle|c_1\rangle \dots |c_{n-1}\rangle|t\rangle$ tenzor szorzatot leíró

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{2^{n+1}-4} \\ \beta_{2^{n+1}-3} \\ 0 \\ 0 \end{pmatrix}$$

vektor utolsó két komponense 0. Most a V mátrixszal balról megszorozzuk a fenti vektort, azaz a $|c_0\rangle|c_1\rangle\ldots|c_{n-1}\rangle|t\rangle$ tenzor szorzatot leíró input vektort. Eredményül megkapjuk a fenti input vektort. Tehát a V mátrisszal való szorzás tényleg 49. ábrán látható áramkörhöz tartozó transzformációt hajtja végre.

□

Tekintsük a 48. ábrát! Az itt látható kvantum áramkör az alábbi transzformációt hajtja végre amikor az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok. Ha az összes irányító qubit értéke $|1\rangle$ akkor az $\mathbf{U}$ operátort alkalmazzuk a $|t_0\rangle, |t_1\rangle, \ldots, |t_{k-1}\rangle$ cél qubitekre. Továbbá az irányító qubitek közvetlenül az outputra kerülnek.

Ha $c_0 \text{ AND } c_1 \text{ AND } \ldots \text{ AND } c_{n-1} = 0$ akkor az input qubitek közvetlenül az outputra kerülnek.

Tekintsük a 50. ábrát! Az ábrán látható kvantum áramkör Toffoli kapukból áll, $n = 6$ irányító qubitből áll:

$|c_1\rangle, |c_2\rangle, |c_3\rangle, |c_4\rangle, |c_5\rangle, |c_6\rangle$ és egy cél qubitből: $|t\rangle$. Az áramkört általánosíthatjuk tetszőleges n számú irányító qubitre. Az áramkörnek van még $n-1 (= 5)$ munka qubitje: $|w_1\rangle, |w_2\rangle, |w_3\rangle, |w_4\rangle, |w_5\rangle$, mindegyik a $|0\rangle$ kezdő állapotban. Az áramkör számításának a végén mindegyik munka qubit értékét visszaállítjuk a $|0\rangle$ kezdő állapotba.

Az áramkör elemzésével megmutatjuk hogy az áramkör ugyanazt a transzformációt valósítja meg mint a 49. ábrán látható kvantum áramkör. Azaz a két kvantum áramkör ekvivalens. Mind a két kvantum áramkör lineáris transzformációt valósít meg. Ezért elegendő belátni hogy a 50. ábra áramköre ugyanazt a tran-

szformációt valósítja meg mint a 49. ábrán látható kvantum áramkör amikor az input irányító qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok. Ezért feltesszük hogy az input qubitek a $|0\rangle$ és $|1\rangle$ bázisvektorok.

A 50. ábrán látható kvantum áramkört három fejlődési szakaszra osztjuk. Az első fejlődési szakasz kiszámítja a $|c_1\rangle, |c_2\rangle, |c_3\rangle, |c_4\rangle, |c_5\rangle, |c_6\rangle$ irányító qubitek logikai szorzatát: $|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \text{ AND } |c_6\rangle$ és betölti az eredményt a w_5 munka qubitbe. A második szakasz végrehajtja az egyetlen qubit irányított U transzformációt a t cél qubiten. A harmadik szakasz visszaállítja a $|w_1\rangle, |w_2\rangle, |w_3\rangle, |w_4\rangle, |w_5\rangle$ munka qubitek értékét az eredeti értékeikre, $|0\rangle$ -re.

Most igazoljuk hogy az első szakasz kiszámítja a $|c_1\rangle, |c_2\rangle, |c_3\rangle, |c_4\rangle, |c_5\rangle, |c_6\rangle$ irányító qubitek logikai szorzatát. Az első Toffoli kapu kiszámítja $|c_1\rangle \text{ AND } |c_2\rangle$ -t és w_1 értékét $|0\rangle$ -ről $|c_1\rangle \text{ AND } |c_2\rangle$ -re változtatja. A következő Toffoli kapu w_2 értékét $|0\rangle$ -ről $|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle$ -re változtatja. És így tovább. Az ötödik Toffoli kapu $|w_5\rangle$ értékét $|0\rangle$ -ről $|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \text{ AND } |c_6\rangle$ -re változtatja.

A harmadik szakaszban visszaállítjuk a munka qubitek értékét $|0\rangle$ -ra. A harmadik szakasz első Toffoli kapuja $|w_5\rangle$ értékét

$$|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \text{ AND } |c_6\rangle$$

-ről

$$|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \text{ AND } |c_6\rangle \oplus$$

$|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \text{ AND } |c_6\rangle = |0\rangle$
-re változtatja. A harmadik szakasz második Toffoli kapuja $|w_4\rangle$ értékét

$$|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle$$

-ről

$$|c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle \oplus \\ |c_1\rangle \text{ AND } |c_2\rangle \text{ AND } |c_3\rangle \text{ AND } |c_4\rangle \text{ AND } |c_5\rangle = |0\rangle$$

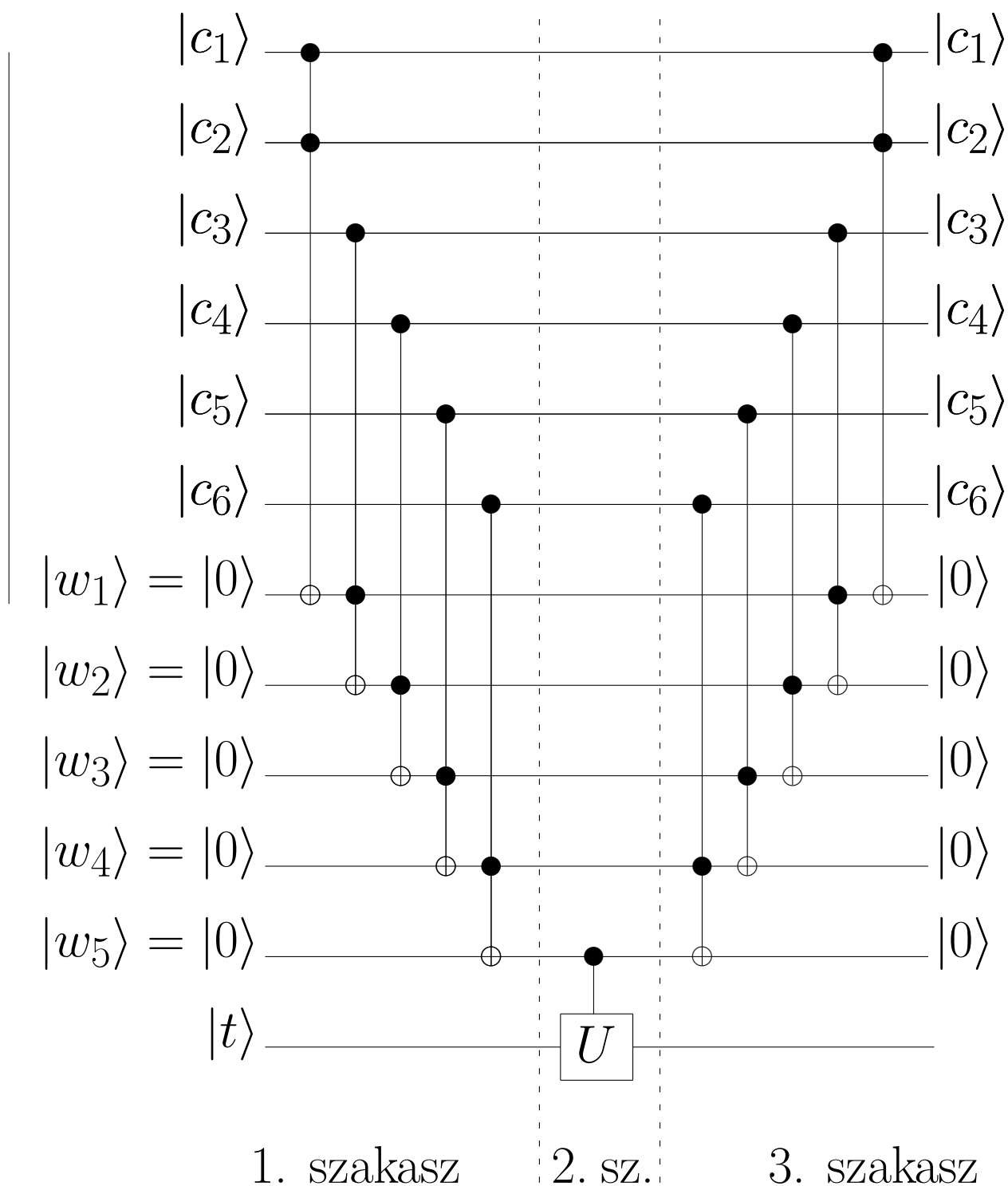
-re változtatja. És így tovább.

6.16. Univerzális kvantum kapuk

Megmutatjuk hogy a Toffoli kaput meg tudjuk valósítani az irányított nem (CNOT) és a H, S, T, $T^\dagger$ egy qubit kapukkal.

Figyeljük meg hogy a 50. ábra kvantum áramkörben Toffoli kapuk vannak. A 50. ábrát tetszőleges n -re tudjuk általánosítani. Így azt kapjuk hogy tetszőleges n qubit irányított 1 cél qubites kvantum áramkörhöz meg tudunk építeni egy vele ekvivalens n qubit irányított kvantum áramkört amely csupán irányított nem (CNOT), Hadamard (H), fázis (S), T és $T^\dagger$ kvantum kapukat használ. További általánosítással kapjuk hogy tetszőleges n qubit irányított k cél qubites kvantum áramkörhöz meg tudunk építeni egy vele ekvivalens n qubit irányított k cél qubites kvantum áramkört amely csupán irányított nem (CNOT), Hadamard (H), fázis (S), T és $T^\dagger$ kvantum kapukat használ. Emlékeztető:

1. A Hadamard (H) operátor.



50. ábra. Az U unitér transzformáció – 1 cél qubiten, 6 irányító és 5 munka qubittel – megvalósítása Toffoli kapukkal

kapu. Más szavakkal: a Toffoli kvantum kaput megvalósítjuk a 51. ábrán látható módon csupán Hadamard (H), fázis (S) és T kvantum kapuk felhasználásával.

Bizonyítás. Emlékezzünk hogy

$$G_{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X \end{pmatrix}$$

ahol

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

A 51. ábrán lévő kvantum áramkört 13 fejlődési szakaszra osztottuk fel. Például a 3. fejlődési szakasz a 2-vel címkézett és a 3-mal címkézett egyenes vonal között van. $G^{(i)}$ jelöli az i -edik fejlődési szakasz áthelyezési mátrixát.

$$G^{(1)} = I \otimes I \otimes H = \begin{pmatrix} H & 0 & 0 & 0 \\ 0 & H & 0 & 0 \\ 0 & 0 & H & 0 \\ 0 & 0 & 0 & H \end{pmatrix}$$

$$G^{(5)} = I \otimes I \otimes T = \begin{pmatrix} T & 0 & 0 & 0 \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{pmatrix}$$

$$G^{(9)} = I \otimes T^\dagger \otimes T = \begin{pmatrix} T & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}}T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & e^{-i\frac{\pi}{4}}T \end{pmatrix}$$

$$G^{(11)} = I \otimes T^\dagger \otimes H = \begin{pmatrix} H & 0 & 0 & 0 \\ 0 & e^{-i\frac{\pi}{4}}H & 0 & 0 \\ 0 & 0 & H & 0 \\ 0 & 0 & 0 & e^{-i\frac{\pi}{4}}H \end{pmatrix}$$

$$G^{(13)} = T \otimes S \otimes I = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & iI & 0 & 0 \\ 0 & 0 & e^{i\frac{\pi}{4}}I & 0 \\ 0 & 0 & 0 & ie^{i\frac{\pi}{4}}I \end{pmatrix}$$

Több fejlődési szakasznak megegyezik az áthelyezési mátrixa.

$$G^{(2)} = G^{(6)} = I \otimes G_{CNOT} = I \otimes \begin{pmatrix} I & 0 \\ 0 & \sigma_X \end{pmatrix} =$$

$$\begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sigma_X & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X \end{pmatrix}$$

$$G^{(3)} = G^{(7)} = I \otimes I \otimes T^\dagger = \begin{pmatrix} T^\dagger & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & T^\dagger & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & T^\dagger & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & T^\dagger \end{pmatrix}$$

$$G^{(4)} = G^{(8)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X \end{pmatrix}$$

$$G^{(10)} = G^{(12)} = G_{CNOT} \otimes I = \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & \sigma_X \end{pmatrix} \otimes I = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \end{pmatrix}$$

A következőkben kiszámítjuk $G^{(13)} \dots G^{(1)}$ több rész szorzatát.

$$G^{(4)} G^{(3)} G^{(2)} G^{(1)} = \begin{pmatrix} T^\dagger H & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & T^\dagger \sigma_X H & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X T^\dagger H & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X T^\dagger \sigma_X H \end{pmatrix}$$

$$G^{(8)}G^{(7)}G^{(6)}G^{(5)} = \begin{pmatrix} IT^\dagger IT & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & IT^\dagger \sigma_X T & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X T^\dagger IT & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X T^\dagger \sigma_X T \end{pmatrix} =$$

$$\begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & T^\dagger \sigma_X T & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \sigma_X & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X T^\dagger \sigma_X T \end{pmatrix}$$

$$G^{(12)}G^{(11)}G^{(10)}G^{(9)} = \begin{pmatrix} IHIT & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & e^{-i\frac{\pi}{2}} IHIT & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & e^{-i\frac{\pi}{4}} IHIT & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & e^{-i\frac{\pi}{2}} IHIT \end{pmatrix} =$$

$$\begin{pmatrix} HT & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & e^{-i\frac{\pi}{2}} HT & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & e^{-i\frac{\pi}{4}} HT & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & e^{-i\frac{\pi}{4}} HT \end{pmatrix}$$

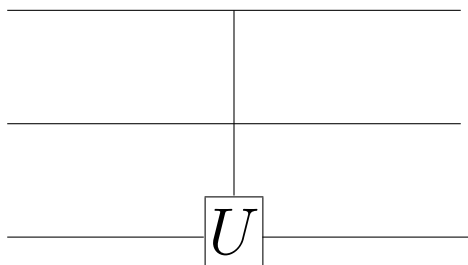
$$G_{teljes} = G^{(13)} \dots G^{(1)} = G^{(13)}(G^{(12)}G^{(11)}G^{(10)}G^{(9)})(G^{(8)}G^{(7)}G^{(6)}G^{(5)})(G^{(4)}G^{(3)}G^{(2)}G^{(1)}) =$$

$$\begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sigma_X \end{pmatrix}$$

Tehát $G_{teljes} = G_{Toffoli}$. Azaz a 51. ábrán látható kvantum áramkör áthelyező mátrixa megegyezik a Toffoli kapu áthelyező mátrixával. Ezért a 51. ábrán látható kvantum áramkör ekvivalens a Toffoli kapuval. Azaz ugyanazt a transzformációt valósítja meg mint a Toffoli kapu.

□

Tekintsük a 52. ábrát és a 53. ábrát!



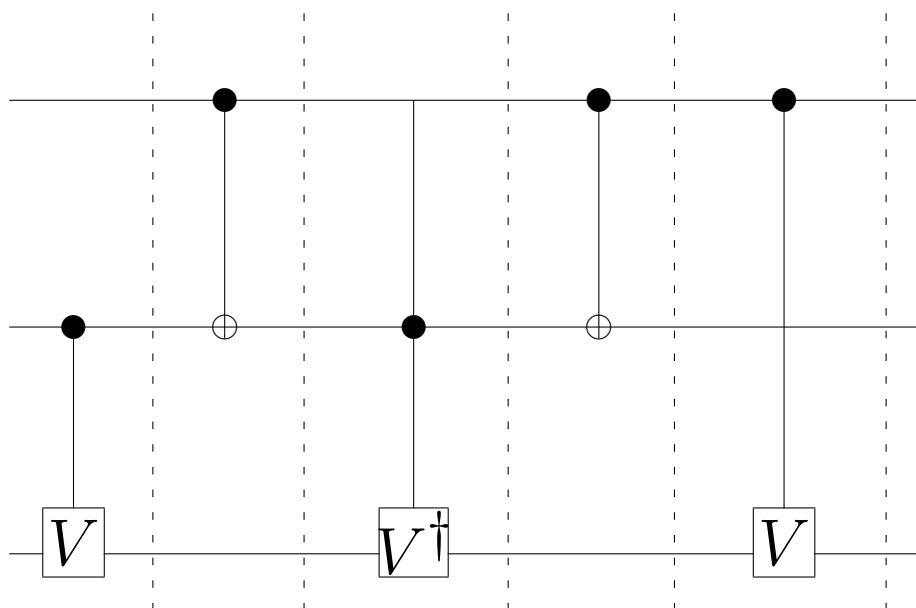
52. ábra. 2 qubit irányítja az U transzformációt

Igazoljuk hogy a 52. ábrán látható kettő qubit irányított kaput megvalósítjuk a 53. ábrán látható módon egy qubit irányított kapuk kombinációjaként!

Állítás 6.10 A 52. ábrán látható kettő qubit irányított kapu ugyanazt a transzformációt valósítja meg mint a 53. ábrán látható egy qubit irányított kapukból felépített kvantum áramkör.

Bizonyítás. Megkonstruáljuk az adott U operátor U áthelyezési mátrixát a szokásos módon: tekintjük a Hilbert térben rendre minden egyes bázisvektort és rendre kiszámoljuk a hozzá rendelt vektort. Képezzük a megfelelő külső szorzatokat és a kapott mátrixokat összeadjuk. Így megkonstruáljuk az U áthelyezési mátrixot.

1. sz. 2. sz. 3. sz. 4. sz. 5. sz.



53. ábra. Az egy qubit által irányított kapukból felépített kvantum áramkör megvalósítja a 52. ábrán látható kettő qubit által irányított kaput

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}.$$

Az U segítségével megkonstruáljuk a $G_{ketqubitirany}$ mátrixot:

$$G_{ketqubitirany} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & U \end{pmatrix}$$

ahol I 2×2 méretű egység mátrix.

Tekintsük a 53. ábrát. A kvantum áramkörben kettő CNOT kaput és három egy qubit irányított kaput látunk. Mindegyik kapunál a cél qubitre a V vagy $V^\dagger$ operációt hajtjuk végre ha az irányító qubit $|1\rangle$. Az 52. és 53. ábrákon látható U és V kvantum kapuk U és V áthelyező mátrixai közötti kapcsolat: $V^2 = U$.

A 53. ábra egyes fejlődési szakaszainak az áthelyezési mátrixai rendre $G_{tC}^{(1)}$, $G_{tC}^{(2)}$, $G_{tC}^{(3)}$, $G_{tC}^{(4)}$ és $G_{tC}^{(5)}$.

$$G_{tC}^{(1)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & V & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V \end{pmatrix}$$

$$G_{tC}^{(2)} = G_{tC}^{(4)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \end{pmatrix}$$

$$G_{tC}^{(3)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & V^\dagger & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V^\dagger \end{pmatrix}$$

$$G_{tC}^{(5)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & V & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V \end{pmatrix}$$

Szorozzuk össze a fenti mátrixokat!

$$G_{tC}^{(2)} G_{tC}^{(1)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & V & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \end{pmatrix}$$

$$G_{tC}^{(3)} G_{tC}^{(2)} G_{tC}^{(1)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V \\ \mathbf{0} & \mathbf{0} & V^\dagger & \mathbf{0} \end{pmatrix}$$

$$G_{tC}^{(4)} G_{tC}^{(3)} G_{tC}^{(2)} G_{tC}^{(1)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & V^\dagger & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V \end{pmatrix}$$

$$G_{tC}^{(5)} G_{tC}^{(4)} G_{tC}^{(3)} G_{tC}^{(2)} G_{tC}^{(1)} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & V^2 \end{pmatrix}$$

Mivel $V^2 = U$, a 52. ábra áramkörének az áthelyezési mátrixa egyenlő a 53. ábra áramkörének az áthelyezési mátrixával.

□

6.17. A Walsh-Hadamard transzformáció kvantum áramkörrel való megvalósítása

Emlékeztető. A Hadamard (H) operátor:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

A H operátort a Hadamard kapuval valósítja meg. A Hadamard kapu a $|0\rangle$ állapotban lévő input qubitet a

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

állapotba transzformálja át. A Hadamard kapu az $|1\rangle$ állapotban lévő input qubitet a

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

állapotba transzformálja át. Azaz $H(|i\rangle) = \frac{(|0\rangle + (-1)^i |1\rangle)}{\sqrt{2}} \quad i = 0, 1$.

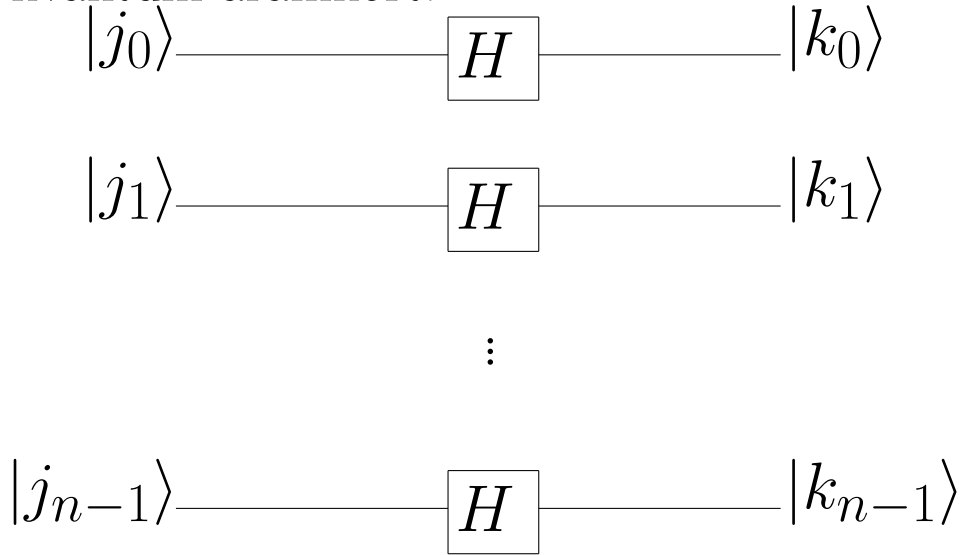
A H operátor önmaga inverze. Ha a H operátort kétszer alkalmazzuk a $|0\rangle$ qubitre, önmagát kapjuk vissza. Ha a H operátort kétszer alkalmazzuk az $|1\rangle$ qubitre, önmagát kapjuk vissza.

Definíció 6.11 A Walsh-Hadamard transzformációt rekurzívan definiáljuk.

$$W_1 = H,$$

$$W_{j+1} = H \otimes W_j, \quad j = 1, 2, \dots$$

A 54. ábrán látjuk a Walsh-Hadamard transzformációt megvalósító kvantum áramkört.



54. ábra. A Walsh-Hadamard transzformációt megvalósító kvantum áramkör

Alkalmazzuk a Walsh-Hadamard transzformációt n darab $|0\rangle$ állapotban lévő qubitre.

$$\begin{aligned} & (H \otimes H \otimes H \otimes \dots \otimes H)(|0\rangle|0\rangle|0\rangle \dots |0\rangle) = \\ & = \frac{1}{2^{\frac{n}{2}}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle)] \end{aligned}$$

Állítás 6.12 A Walsh-Hadamard transzformáció áthelyezési mátrixa a G_{H^n} $2^n \times 2^n$ -es mátrix. A G_{H^n} mátrix elemei:

$$g_{jm} = \left(\frac{1}{\sqrt{2}}\right)^n (-1)^{j \cdot m} = \frac{1}{2^{\frac{n}{2}}} (-1)^{j \cdot m}, \quad 0 \leq j, m \leq 2^n - 1.$$

Itt a $j \cdot m$ rövidítést az alábbi módon értelmezzük. A j és m számok bináris alakját tekintjük

$$\begin{aligned} j &= j_0 2^{n-1} + j_1 2^{n-2} + \dots + j_{n-2} 2 + j_{n-1} 2^0. \\ m &= m_0 2^{n-1} + m_1 2^{n-2} + \dots + m_{n-2} 2 + m_{n-1} 2^0. \end{aligned}$$

Most

$$j \cdot m = j_0 m_0 + j_1 m_1 + \cdots + j_{n-2} m_{n-2} + j_{n-1} m_{n-1}.$$

Bizonyítás. n szerinti teljes indukcióval.

$n = 1$: A H transzformáció mátrixa a G_{H^1} mátrix. A G_{H^1} 2×2 -es mátrix közvetlen vizsgálatával.

Indukciós lépés:

$$W_{n+1} = H \otimes W_n.$$

A $(\frac{1}{\sqrt{2}})^{n+1}$ szorzótényező nyilvánvaló. W_{n+1} -nek $G_{H^{n+1}}$ mátrixa négy példányban tartalmazza W_n -nek G_{H^n} mátrixát.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának bal felső negyedében megmaradnak a G_{H^n} mátrixbeli előjelek.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának jobb felső negyedében megmaradnak a G_{H^n} mátrixbeli előjelek.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának bal alsó negyedében megmaradnak az előjelek.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának jobb alsó negyedében átfordulnak a G_{H^n} mátrixbeli előjelek.

Vessük össze a fenti megfigyeléseket az állításban szereplő képlettel! Vajon ugyanazt kapjuk? Igen.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának bal felső negyedében megmaradnak a G_{H^n} mátrixbeli előjelek. Mert a sor koordináta bináris alakjának az értéke változatlan marad és az oszlop koordináta bináris alakjának az értéke változatlan marad. A sor koordináta bináris alakja a 2^n helyiértékkel bővül, és a 2^n helyiértékre 0-t írunk. Hasonlóan az oszlop koordináta bináris alakja a 2^n helyiértékkel bővül, és a 2^n helyiértékre 0-t írunk. A 2^n helyiértéken álló bitek szorzata $0 \cdot 0 = 0$, így $j \cdot m$ nem változik.

- W_{n+1} -nek mátrixának jobb felső negyedében megmaradnak a G_{H^n} mátrixbeli előjelek. Mert a sor koordináta bináris alakjának az értéke változatlan marad. A sor koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 0-t írunk. Hasonlóan az oszlop koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 1-t írunk. A 2^n helyiértéken álló bitek szorzata $0 \cdot 1 = 0$, így $j \cdot m$ nem változik.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának bal alsó negyedében megmaradnak az előjelek. Mert az oszlop koordináta bináris alakjának az értéke változatlan marad. A sor koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 1-t írunk. Hasonlóan az oszlop koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 0-t írunk. A 2^n helyiértéken álló bitek szorzata $1 \cdot 0 = 0$, így $j \cdot m$ nem változik.

- W_{n+1} -nek $G_{H^{n+1}}$ mátrixának jobb alsó negyedében átfordulnak a G_{H^n} mátrixbeli előjelek. A sor koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 1-t írunk. Hasonlóan az oszlop koordináta bináris alakja a 2^n helyiértékkal bővül, és a 2^n helyiértékre 1-t írunk. A 2^n helyiértéken álló bitek szorzata $1 \cdot 1 = 1$, így $j \cdot m$ 1-gyel nő.

□

Legyen $|j\rangle$ az input állapot vektora és $|k\rangle$ az output állapot vektora a 54. ábrán látható kvantum áramkörnek. $|j\rangle$ az alábbi alakot ölti:

$$|j\rangle = |j_0\rangle \otimes |j_1\rangle \otimes |j_2\rangle \otimes \dots \otimes |j_{n-2}\rangle \otimes |j_{n-1}\rangle = |j_0 j_1 j_2 \dots j_{n-2} j_{n-1}\rangle.$$

$$|k\rangle = G_{H^n} |j\rangle = (H \otimes H \otimes H \otimes \dots \otimes H) (|j_0\rangle \otimes |j_1\rangle \otimes |j_2\rangle \otimes \dots \otimes |j_{n-1}\rangle)$$

$$\cdots \otimes |j_{n-2}\rangle \otimes |j_{n-1}\rangle) = \\ H(|j_0\rangle) \otimes H(|j_1\rangle) \otimes H(|j_2\rangle) \otimes \cdots \otimes H(|j_{n-1}\rangle) =$$

$$\frac{1}{2^{\frac{n}{2}}} [|0\rangle + (-1)^{j_0}|1\rangle] \otimes [|0\rangle + (-1)^{j_1}|1\rangle] \otimes \cdots \otimes [|0\rangle + (-1)^{j_{n-1}}|1\rangle] = \quad (5)$$

$$\frac{1}{2^{\frac{n}{2}}} \sum_{m=0}^{2^n-1} (-1)^{j_0 m_0} |m_0\rangle \otimes (-1)^{j_1 m_1} |m_1\rangle \otimes \cdots \otimes (-1)^{j_{n-1} m_{n-1}} |m_{n-1}\rangle$$

A fenti összegben az egyes kitevőkben az m szám bináris alakjának a bitjei állnak, azaz

$$m = m_0 2^{n-1} + m_1 2^{n-2} + \cdots + m_{n-2} 2 + m_{n-1} 2^0.$$

Indoklás: A tenzor szorzat összeadásra való disztributivitása alapján az (5)-ben szereplő tenzor szorzat egy összeg. Minden egyes tagja megfelel egy tenzor szorzatnak. Minden egyes ilyen tenzor szorzat megfelel egy bináris számot leíró 0-k és 1-k n hosszú

$$m_0, m_1, \dots, m_{n-1}$$

sorozatának, amit a fenti m szám bináris alakjának tekintünk. Minden $0 \leq \ell \leq n-1$ szám esetén egyik tagot kiválasztjuk a $[|0\rangle + (-1)^{j_\ell}|1\rangle]$ tényezőből. $m_\ell = 0$ jelenti hogy a $|0\rangle$ tagot választjuk ki és tenzor szorozzuk; és $m_\ell = 1$ jelenti hogy a $(-1)^{j_\ell}|1\rangle$ ($0 \leq \ell \leq n-1$) tagot választjuk ki és tenzor szorozzuk. Ezért összegezzük az $m = 0, 1, \dots, 2^n - 1$ számok szerint felhasználva azok bináris alakját. Amikor $m_\ell = 0$ és az ℓ -edik tényezőből azaz a $[|0\rangle + (-1)^{j_\ell}|1\rangle]$ tényezőből a $|0\rangle$ tagot

választjuk ki, akkor

$$(-1)^{j_\ell m_\ell} = (-1)^{j_\ell 0} = (-1)^0 = 1$$

-el szorozzuk a $|0\rangle$ qubitet. Amikor $m_\ell = 1$ és az ℓ -edik tényezőből azaz a $[|0\rangle + (-1)^{j_\ell} |1\rangle]$ tényezőből az $|1\rangle$ tagot választjuk ki, akkor

$$(-1)^{j_\ell} = (-1)^{j_\ell m_\ell}$$

-el szorozzuk az $|1\rangle$ qubitet.

Tehát akár a $|0\rangle$ tagot akár a $|1\rangle$ tagot választjuk ki az ℓ -edik tényezőből azt $(-1)^{j_\ell m_\ell}$ -el szorozzuk meg.

Kapjuk hogy

$$\begin{aligned} & \frac{1}{2^{\frac{n}{2}}} \sum_{m=0}^{2^n-1} (-1)^{j_0 m_0} (-1)^{j_1 m_1} \dots (-1)^{j_{n-1} m_{n-1}} |m_0\rangle \otimes |m_1\rangle \otimes \dots \otimes \\ & |m_{n-1}\rangle = \\ & \frac{1}{2^{\frac{n}{2}}} \sum_{m=0}^{2^n-1} (-1)^{j \cdot m} |m\rangle . \end{aligned}$$

Itt az $|m_0\rangle \otimes |m_1\rangle \otimes \dots \otimes |m_{n-1}\rangle$ tenzor szorzatot röviden $|m\rangle$ jelöli.

$$\begin{aligned} |k\rangle &= G_{H^n} |j\rangle = (H \otimes H \otimes H \otimes \dots \otimes H) (|j_0\rangle \otimes |j_1\rangle \otimes |j_2\rangle \otimes \\ & \dots \otimes |j_{n-2}\rangle \otimes |j_{n-1}\rangle) = \frac{1}{2^{\frac{n}{2}}} \sum_{m=0}^{2^n-1} (-1)^{j \cdot m} |m\rangle . \end{aligned}$$

7. A kvantum számítógép matematikai modellje.

A kvantum számítógép bemeneti és kimeneti kvantum vezetékekből és kvantum áramkörökből áll. A kvantum áramkörök kvantum kapukból épülnek fel. A kvantum kapu q darab input qubitet képez q darab output kvantum bitbe. Ez a megfordíthatóság szükséges és elegendő feltétele. A kvantum kapu áthelyező mátrixa

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

Minden qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ alakú, ahol $|0\rangle$ és $|1\rangle$ ortonormális bázisvektorok $\mathcal{H}_2$ -ben. A kvantum kapu input vektora a $\mathcal{H}_{2^q}$ Hilbert tér állapota. Hasonlóan kvantum kapu output vektora a $\mathcal{H}_{2^q}$ Hilbert tér állapota. Mind az input vektor mind az output vektor q darab qubit tenzor szorzata.

Tekintsünk egy n -qubites kvantum számítógépet amely a $\mathcal{H}_{2^n}$ Hilbert tér felett működik. $\mathcal{H}_{2^n}$ a tenzor szorzata az n darab qubitekhez tartozó $\mathcal{H}_2$ Hilbert tereknek.

Legyen $b = b_0b_1b_2\cdots b_{n-1}$ egy bináris sztring (szó). A $|V_{b_0}\rangle, |V_{b_1}\rangle, \dots, |V_{b_{n-1}}\rangle$ $\mathcal{H}_2$ -beli vektorok rendre megfelelnek a $b_0, b_1, b_2, \dots, b_{n-1}$ klasszikus biteknek. (Ha $b_0 = 0$, akkor $|V_{b_0}\rangle = |0\rangle$, ha $b_0 = 1$, akkor $|V_{b_0}\rangle = |1\rangle$.) A tenzor szorzata a fenti vektoroknak:

$$|V_b\rangle = |b_0b_1b_2\cdots b_{n-1}\rangle = |V_{b_0}\rangle \otimes |V_{b_1}\rangle \otimes \cdots \otimes |V_{b_{n-1}}\rangle.$$

Definíció 7.1 Minden $0 \leq j \leq 2^n - 1$ esetén, ha a j szám bináris alakja

$$j = j_02^{n-1} + j_12^{n-2} + \cdots + j_{n-2}2 + j_{n-1}2^0, \text{ akkor legyen}$$

$$u_j = |j_0\rangle \otimes |j_1\rangle \otimes \cdots \otimes |j_{n-1}\rangle.$$

azaz

$$|u_0\rangle = |000\cdots 000\rangle, |u_1\rangle = |000\cdots 001\rangle, u_2 = |000\cdots 010\rangle, \\ u_3 = |000\cdots 011\rangle, \dots, u_{2^n-2} = |111\cdots 110\rangle, u_{2^n-1} = |111\cdots 111\rangle.$$

Állítás 7.2 Az $|u_0\rangle = |000\cdots 000\rangle, |u_1\rangle = |000\cdots 001\rangle, u_2 = |000\cdots 010\rangle, u_3 = |000\cdots 011\rangle, \dots, u_{2^n-2} = |111\cdots 110\rangle, u_{2^n-1} = |111\cdots 111\rangle$ vektorok a $\mathcal{H}_{2^n}$ Hilbert tér bázis vektorai.

A kvantum számítógép áthelyező mátrixa egy G unitér márix amely 2^n darab sorból és 2^n darab oszlopból áll. A kvantum számítógép inputja k hagyományos bitből álló bináris sztring, ahol $k \leq n$. Ezt az inputot kiegészítjük n hosszú hagyományos bináris sztringre, az első $n - k$ bitet 0-ra állítjuk. Legyen $b' = 00 \dots 0b_0b_1 \dots b_{k-1}$. Tekintsük a fenti sztringnek megfelelő $|V_{b'}\rangle$ $\mathcal{H}_{2^n}$ Hilbert térbeli vektort. A kvantum számítógép outputja

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

Az α_j komplex számot, $1 \leq j \leq 2^n - 1$ 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 az $|u_j\rangle$ eredményt kapjuk $|\alpha_j|^2$ valószínűséggel, $1 \leq j \leq 2^n - 1$. Az $|u_j\rangle$ eredménynek megfeleltetjük a j szám 2-es számrendszerbeli alakját, $1 \leq j \leq 2^n - 1$. Lásd a 7.1 definíciót.

A kvantum számítógép minden kapuja amelyet $q \leq n$ qubitre alkalmazunk egy transzformációt valósít meg a $\mathcal{H}_{2^n}$ Hilbert tér felett. Például tekintsünk egy két qubites kaput amelynek 4×4 nagyságú áthelyezési mátrixa van. Ennek a kapunak a tevékenységét leíró áthelyezési mátrix egyenlő a G és $n - 2$ darab

egységmátrix tenzorszorzatával, ahol minden egység mátrix egy kimaradó qubitet transzformál.

Állítás 7.3 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.

A megfordítható kvantum áramkörnek szüksége van munka qubitekre. Ezek a munka qubitek tartalmazzák a számítás során kapott részeredményeket. Például a 50. ábrán látható kvantum áramkör öt qubitet használ fel hogy tárolja az irányító qubitek szorzatának részszorzatait. Végül betöltjük az összes irányító qubit szorzatát az egyik munka qubitbe. Így ez a munka qubit irányítja azt a kaput amely átranszformálja a cél qubitet. A munka qubitek kezdőértéke $|0\rangle$ -ra van állítva. A visszafordítható áramkör a kezdő állapotba állítja őket vissza mielőtt befejezi a számolást.

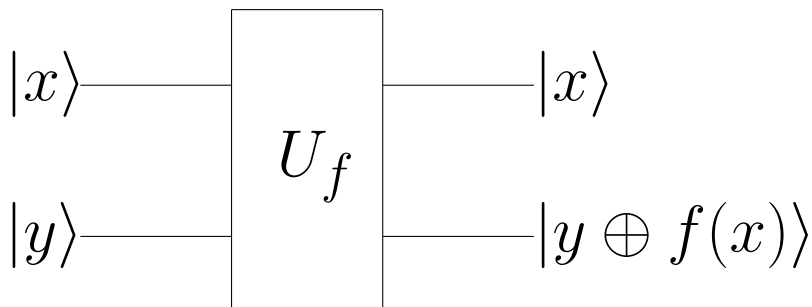
A Toffoli hagyományos kapu univerzális. Ezt azt jelenti, hogy bármely $f(x_1, \dots, x_m)$ Boole függvényhez létezik olyan Toffoli kapukból álló áramkör amelynek

az inputja $x_1, x_2, \dots, x_m$ és valamennyi segédbit

az outputja $x_1, x_2, \dots, x_m, f(x_1, \dots, x_m)$ és további bitek (szemét).

Tekintsük az 55. ábrát! Az ábrán látható két qubites kvantum áramkör egy adott $f(x)$ függvényre az $U_f : |xy\rangle \rightarrow |x(y \oplus f(x))\rangle$ leképezést valósítja meg. Tehát az $|x\rangle, |y\rangle$ qubiteket rendre az $|x\rangle, |y \oplus f(x)\rangle$ qubitekbe transzformálja át. Amikor $|y\rangle = |0\rangle$,

akkor a transzformáció: $|x0\rangle \mapsto |xf(x)\rangle$.



55. ábra. Az ábrán látható 2 qubites kvantum kapu az $U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ leképezést valósítja meg.

Tetszőleges $f(x)$ függvényre meg tudjuk konstruálni a 55. ábrán látható kvantum áramkört úgy hogy csupán kvantum Toffoli kapukat tartalmaz. Hangsúlyozzuk hogy az $f(x)$ függvény be van huzalozva a kvantum áramkörbe.

Az általános esetben több irányító qubitünk ($|x\rangle$) és több munka qubitünk ($|y\rangle$) lehet. A kvantum áramkör által megvalósított transzformáció:

$$|xy\rangle \mapsto |f(x)g(x)\rangle$$

alakú. Itt $f(x)$ az eredmény, a munka qubitekben kapott $g(x)$ melléktermék outputra nincsen szükségünk, az $|y\rangle$ munkaqubitek értékét vissza kell állítanunk. Itt $|xy\rangle$ jelöli $|x\rangle$ és $|y\rangle$ tenzor szorzatát. Legyen m darab irányító qubitünk:

$|x\rangle = |x_0x_1 \dots x_j \dots x_{m-1}\rangle$ ahol $x_j \in \{0, 1\}$, $j = 0, 1, \dots, m - 1$.

Legyen k darab munka qubitünk:

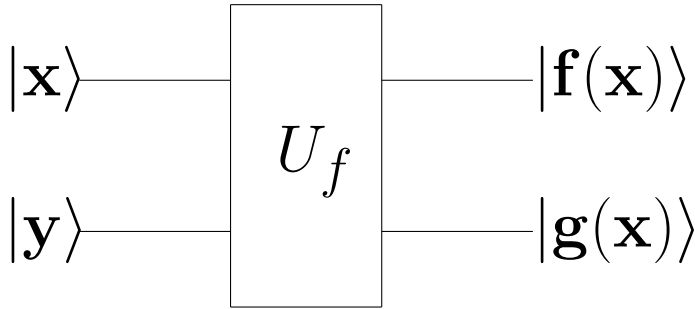
$|y\rangle = |y_0y_1 \dots y_j \dots y_{k-1}\rangle$ ahol $y_j \in \{0, 1\}$, $j = 0, 1, \dots, k-1$. Minden munka qubit kezdőértéke $|0\rangle$. Ebben az esetben a kvantum áramkör által kiszámított függvény

$$|x_0x_1 \dots x_j \dots x_{m-1}00 \dots 0\rangle \mapsto |f(x)g(x)\rangle.$$

Ezt tömören az alábbi rövid alakban is írhatjuk

$$|x_0x_1 \dots x_j \dots x_{m-1}\mathbf{0}\rangle \mapsto |f(x)g(x)\rangle.$$

Fokozatosan bővítjük a kvantum áramkörünket hogy visszafordítható számítást hajtsen végre lásd az 56., 57., 58., 59. ábrákat.

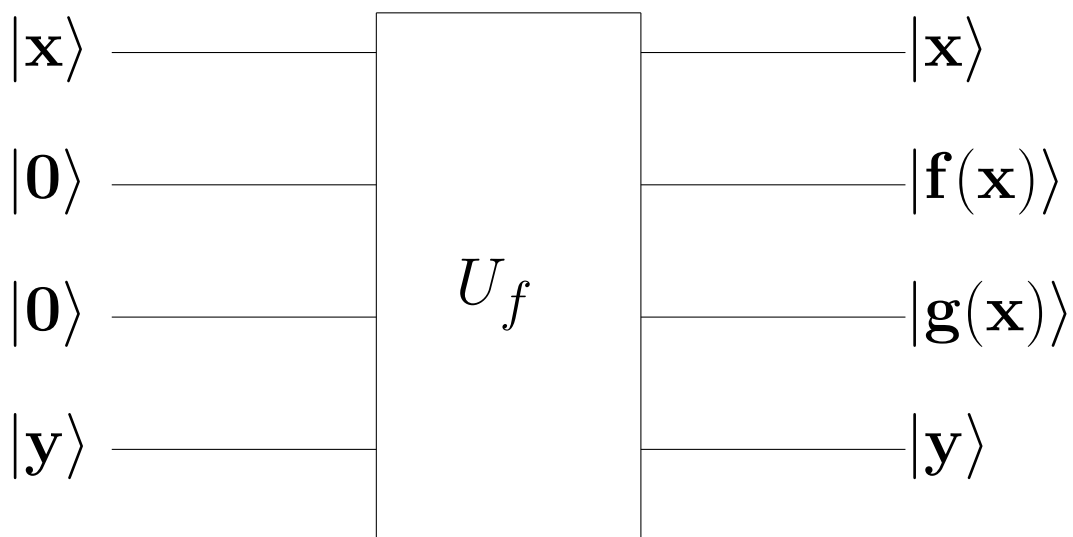


56. ábra. A kiinduló kvantum áramkör

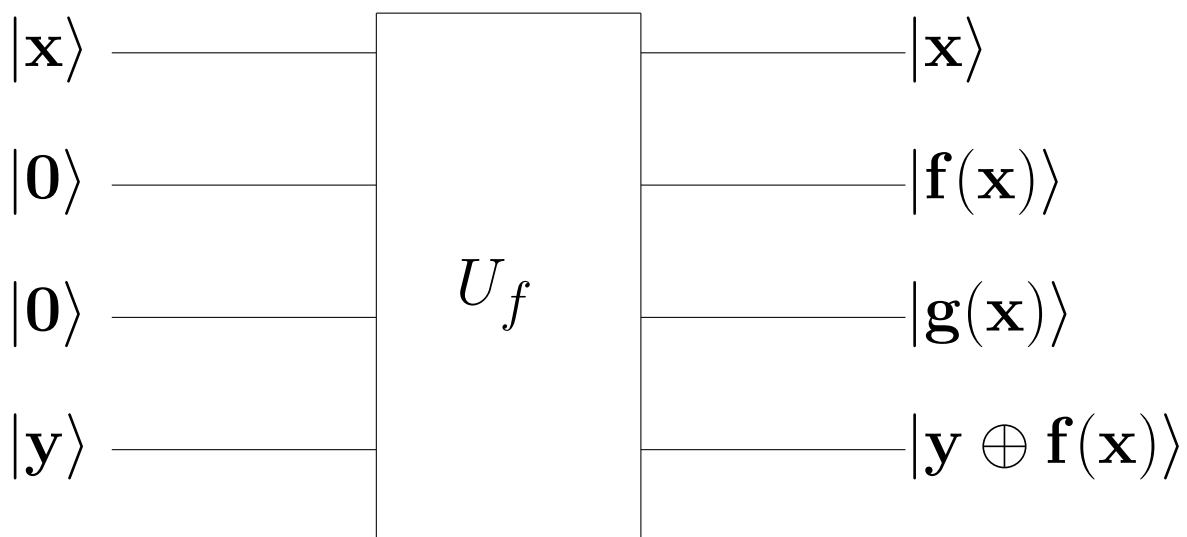
Először az $|x\rangle$ inputnak elkészítjük a másolatát egy CNOT kapu segítségével. Ez a másolati példányt nem fogjuk megváltoztatni a számolás során. Most az áramkör által megvalósított transzformáció:

$$|x\mathbf{00}\rangle \mapsto |xf(x)g(x)\rangle.$$

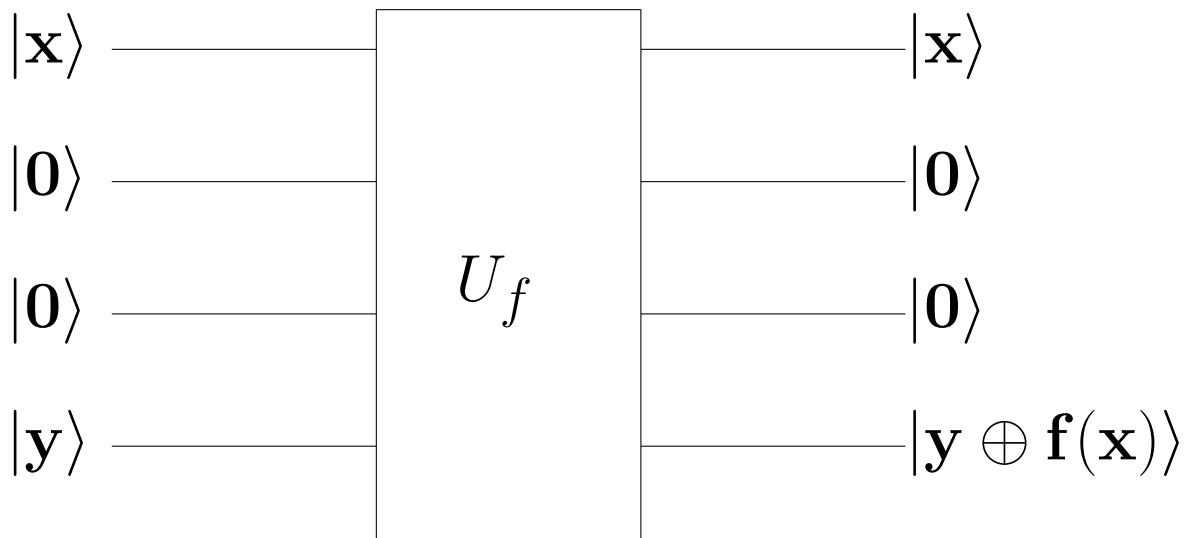
Megkonstruálunk egy kvantum áramkört amelynek négy input regisztere van. Az első tartalmazza az $|x\rangle$ inputot. A második eredetileg $|\mathbf{0}\rangle$ -t tartalmaz és $f(x)$ kiszámításának a végén az $f(x)$



57. ábra. Az első lépés eredményeként kapott kvantum áramkör



58. ábra. A második lépés eredményeként kapott kvantum áramkör



59. ábra. A végeredményül kapott kapott kvantum áramkör

végeredményt tartalmazza. A harmadik munka qubiteket tartalmaz $|0\rangle$ kezdőértékkel, a számítás során egy ponton a $|g(x)\rangle$ melléktermékként keletkezett eredményt tartalmazza. A negyedik az $|y\rangle$ kezdőértéket tartalmazza először. Ezzel a négy regiszterrel az áramkör az alábbi transzformációt hajtja végre:

$$|x00y\rangle \mapsto |xf(x)g(x)y\rangle.$$

A következő lépésben CNOT kapukat adunk a kvantum áramkörhöz hogy qubitenként hozzáadjuk a második regiszterben előállott $|f(x)\rangle$ -t a negyedik regiszterben lévő $|y\rangle$ -hoz. Így módon kapjuk hogy

$$|x00y\rangle \mapsto |xf(x)g(x)y\rangle \mapsto |xf(x)g(x)y \oplus f(x)\rangle.$$

Emlékezzünk hogy az $|f(x)\rangle$ kiszámítása visszafordítható. Ezért a második és a harmadik regiszter tartalmát visszaírhatjuk $|0\rangle$

kvantum bitekre. Így végül kapjuk hogy

$$|x\mathbf{00}y\rangle \mapsto |xf(x)g(x)y\rangle \mapsto |xf(x)g(x)y \oplus f(x)\rangle \mapsto |x\mathbf{00}(y \oplus f(x))\rangle.$$

A fenti eredmény így rövidíthetjük:

$$|xy\rangle \mapsto |x(y \oplus f(x))\rangle.$$

Tehát elméletben, tetszőleges hagyományos áramkörrel kiszámítható $f(x)$ függvényre meg tudunk konstruálni egy megfordítható kvantum áramkört amely az $|x\rangle$ inputon kiszámítja az $|f(x)\rangle$ függvényt.

8. Kvantum párhuzamosság

Tekintsük a 60., 61. és 62. ábrákat! Korábban láttuk hogy adott $f(x)$ egy változós függvényhez meg tudunk konstruálni egy olyan kvantum áramkört amely Toffoli kapukból áll és az $|x\rangle$ és $|y\rangle$ (két darab) input qubitet az $|x(y \otimes f(x))\rangle$ állapotba transzformálja át, lásd az 60. ábrát.

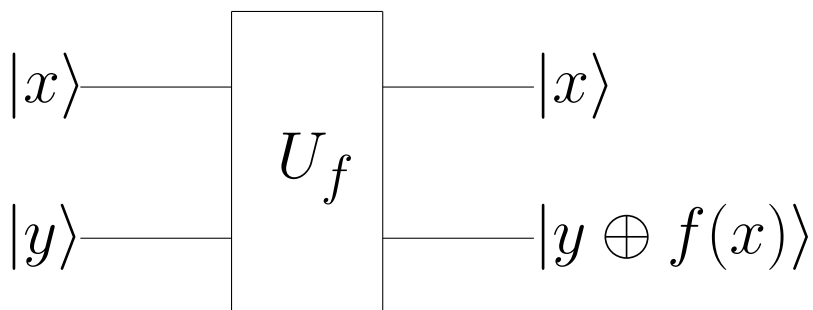
Az $f(x)$ függvény bele van huzalozva az áramkörbe. Amikor a második input qubit $|0\rangle$, akkor az áramkör által kiszámolt transzformáció:

$$|x0\rangle \mapsto |xf(x)\rangle$$

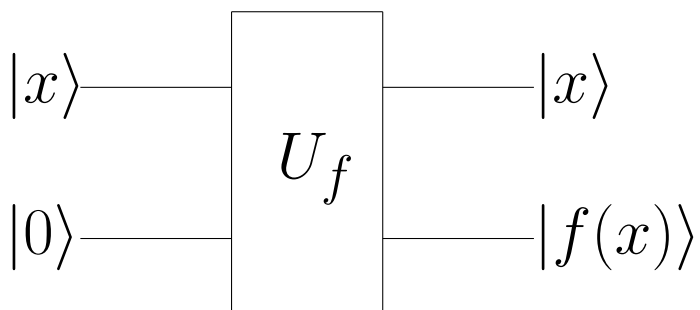
lásd a 61. ábrát.

Most tekintsük a 62. ábrát!

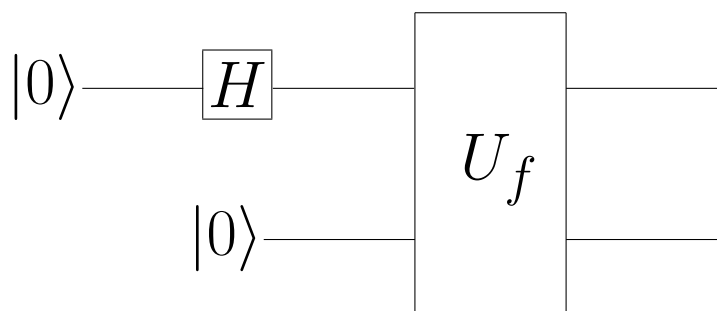
A $|0\rangle$ qubit állapotra először alkalmazzuk a Hadamard kaput. Az outputra $(\frac{|0\rangle+|1\rangle}{\sqrt{2}})$ alkalmazzuk a 62. ábra áramkörét. A két output qubit a



60. ábra. Az ábrán látható 2 qubites kvantum kapu az $U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ leképezést valósítja meg.



61. ábra. Az ábrán látható 2 qubites kvantum kapu az $U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ leképezést valósítja meg.



62. ábra. Az első qubit a $(|0\rangle + |1\rangle)/\sqrt{2}$ állapotba kerül, a második input qubit $|0\rangle$. Az output: $\frac{|0f(0)\rangle + |0f(1)\rangle + |1f(0)\rangle + |1f(1)\rangle}{2}$

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

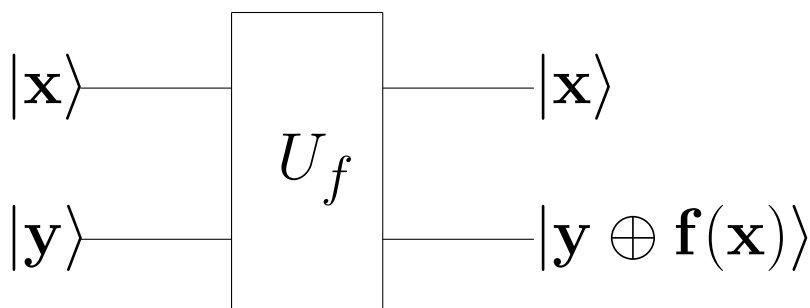
és a

$$f\left(\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}\right) = \frac{(|f(0)\rangle + |f(1)\rangle)}{\sqrt{2}}.$$

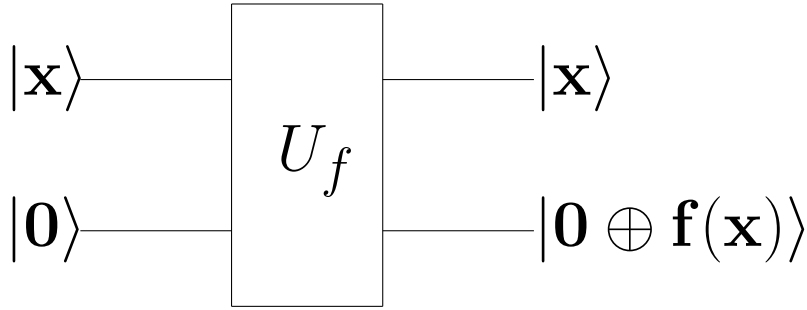
A kvantum rendszer outputja ennek a két vektornak a tenzor szorzata:

$$\frac{(|0f(0)\rangle + |0f(1)\rangle + |1f(0)\rangle + |1f(1)\rangle)}{2}.$$

Az output állapot információt tartalmaz $f(0)$ -ról is és $f(1)$ -ről is. Ezt a jelenséget kvantum párhuzamosságnak hívjuk.



63. ábra. Az ábrán látható 2 regiszteres kvantum kapu az $U_f : |\mathbf{x}\rangle|\mathbf{y}\rangle \rightarrow |\mathbf{x}\rangle|\mathbf{y} \oplus \mathbf{f}(\mathbf{x})\rangle$ leképezést valósítja meg.



64. ábra. Az ábrán látható 2 regiszteres kvantum kapu az $U_f : |\mathbf{x}\rangle|\mathbf{0}\rangle \rightarrow |\mathbf{x}\rangle|\mathbf{0} \oplus \mathbf{f}(\mathbf{x})\rangle$ leképezést valósítja meg.

A kvantum párhuzamosságot kiterjesztjük m input qubitre. Mindegyik a $|0\rangle$ állapotban van. Mindegyiket áttanszformáljuk a Hadamard kapuval.

$$\begin{aligned} & (H \otimes H \otimes H \otimes \dots H)(|0\rangle|0\rangle|0\rangle \dots |0\rangle) = \\ & \frac{1}{2^{\frac{n}{2}}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) = \\ & \frac{1}{2^{\frac{n}{2}}}(\sum_{m=0}^{2^n-1} |m\rangle) . \end{aligned}$$

Adjunk k qubites regisztert (azaz k qubitet) a kvantum áramkörhöz. Mindegyik hozzáadott qubit a $|0\rangle$ állapotban van. Lásd 64. ábra.

Tegyük fel hogy az U_f áramkör számítja ki az f függvényt, és az eredményt a második regiszterben kapjuk meg. Az első m input qubit értéke közvetlenül az outputra kerül (azaz az első m output qubitbe).

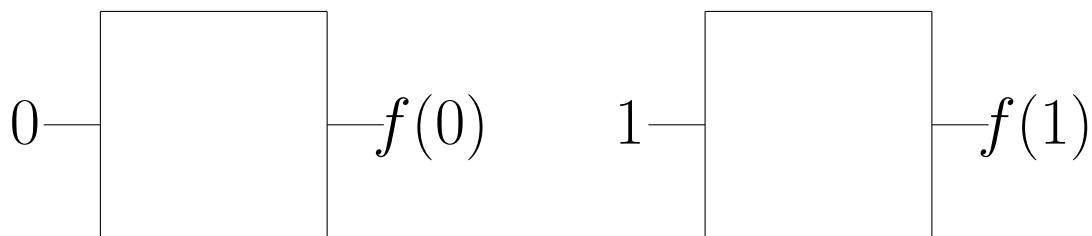
$$\begin{aligned} & U_f\left(\frac{1}{2^{\frac{m}{2}}} \sum_{x=0}^{2^m-1} |x\mathbf{0}\rangle\right) = \\ & \frac{1}{2^{\frac{m}{2}}} \sum_{x=0}^{2^m-1} U_f(|x\mathbf{0}\rangle) = \\ & \frac{1}{2^{\frac{m}{2}}} \sum_{x=0}^{2^m-1} |xf(x)\rangle . \end{aligned}$$

9. Deutsch problémája

Tekintsünk egy fekete dobozt amelyhez tartozó $f : \{0, 1\} \rightarrow \{0, 1\}$ függvény egy input bitet képez egy input bitbe. Feltesszük hogy

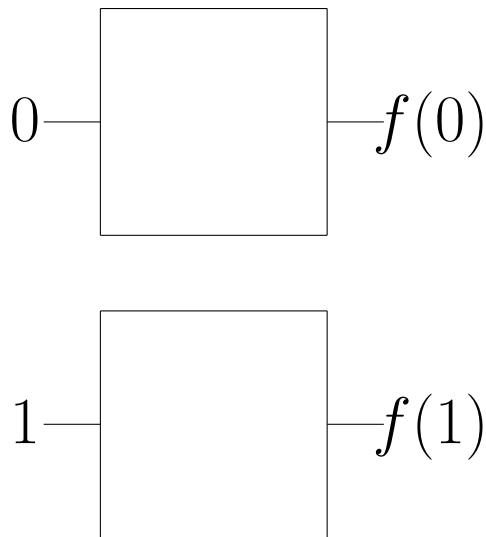
- T ideig tart kiszámítani $f(0)$ értékét és ugyanennyi ideig tart kiszámítani $f(1)$ értékét.
- A két eredmény összehasonlítása 0 időt igényel.

Döntsük el hogy $f(0) = f(1)$ vagy $f(0) \neq f(1)$! Hagyományos számítógép felhasználásával kiszámítjuk $f(0)$ -t és $f(1)$ -et. Majd a két eredmény összehasonlítjuk. Ez $2T$ időt igényel, lásd az 65. ábrát.



65. ábra. Hagyományos számolás

A klasszikus párhuzamos megoldás látható az 66 ábrán, ahol két példányunk van a hagyományos áramkörből. Az első áramkör bemenetére 0-t, a második áramkör bemenetére 1-t teszünk. Az eredményeket összehasonlítjuk. Ebben az esetben T idő alatt kapjuk meg a választ, de a hagyományos áramkör két példányát használjuk fel.



66. ábra. Klasszikus párhuzamos számolás

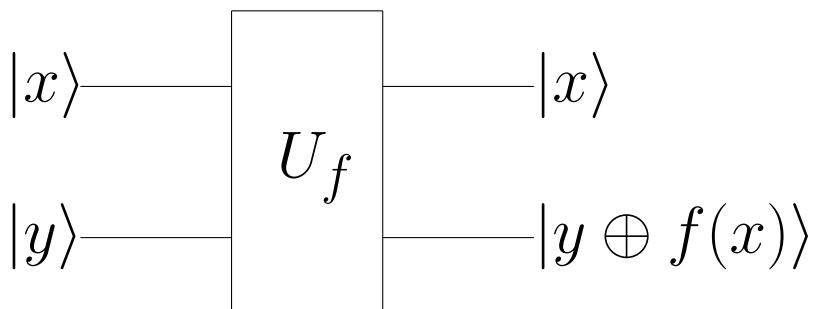
A konstrukciónk szemléletes alapötlete: Tekintsünk most egy kvantum számítógépet U_f áthelyező függvénnnyel. A kvantum számítógép két input qubitet kap: az $|x\rangle$ és $|y\rangle$ qubiteket. A kvantum számítógép két output qubitet ad ki: $|x\rangle$ és $y \oplus f(x)\rangle$, lásd a 67. ábrát.

Legyen $|x\rangle = \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ és $|y\rangle = \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$.

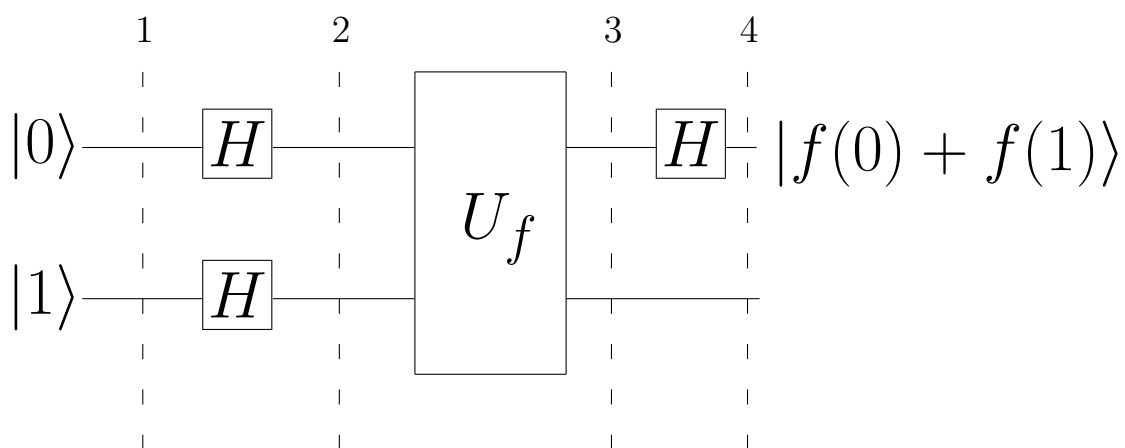
Most megmutatjuk hogy az első output qubit értéke $|f(0) \oplus f(1)\rangle$. Így ha $f(0) = f(1)$ akkor az első output qubit $|0\rangle$; ha $f(0) \neq f(1)$ akkor az első output qubit $|1\rangle$.

Pontos bizonyítás: A 68. ábrán láthatjuk a Deutsch problémáját megoldó kvantum áramkört.

Az áramkört négy fejlődési szakaszra osztjuk fel. A 0, 1, 2, 3 pontokban a rendszer rendre a ξ_0 , ξ_1 , ξ_2 és ξ_3 , állapotokban van. Az input vektor:



67. ábra. Az ábrán látható 2 qubites kvantum kapu az $U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ leképezést valósítja meg.



68. ábra. Deutsch problémáját megoldó kvantum áramkör. Az első output qubit $|f(0) + f(1)\rangle$. Ha $|f(0) + f(1)\rangle = |0\rangle$, akkor $f(0) = f(1)$. Ha $|f(0) + f(1)\rangle = |1\rangle$, akkor $f(0) \neq f(1)$.

$$\xi_0 = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ Az első szakasz áthelyezési}$$

mátrixa:

$$G_1 = H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Most

$$|\xi_1\rangle = G_1|\xi_0\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

$$\text{Azaz } |\xi_1\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)].$$

Alkalmazzuk U_f -et a $|\xi_1\rangle$ állapotvektorra!

$$\xi_2 = U_f\left(\frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]\right) = \frac{1}{2}[|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)]$$

Tekintsük a

$$|0'\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1'\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

bázis vektorokat! Itt $|0'\rangle, |1'\rangle$ a duális bázis. A

$$\xi_2 = \frac{1}{2}[|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)]$$

egyenlőségből kapjuk az alábbiakat: Ha $f(0) = f(1) = 0$, akkor

$$\xi_2 = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |0'\rangle|1'\rangle.$$

Ha $f(0) = f(1) = 1$, akkor

$$\xi_2 = \frac{1}{2}(|0\rangle + |1\rangle)(|1\rangle - |0\rangle) = -|0'\rangle|1'\rangle.$$

Ha $f(0) = 0$ és $f(1) = 1$, akkor

$$\xi_2 = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) = |1'\rangle|1'\rangle.$$

Ha $f(0) = 1$ és $f(1) = 0$, akkor

$$\xi_2 = \frac{1}{2}(|0\rangle - |1\rangle)(|1\rangle - |0\rangle) = -|1'\rangle|1'\rangle.$$

Figyeljük meg: Ha az első output qubit $|0'\rangle$ akkor $f(0) = f(1)$.

Ha az első output qubit $|1'\rangle$ akkor $f(0) \neq f(1)$.

A 68. ábrán látható utolsó Hadamard kaput az első output qubitre alkalmazzuk, ez a Hadamard kapu átforgatja a duális bázisvektorokat az eredeti bázis vektoraiba: $|0'\rangle$ -t $|0\rangle$ -ba $|1'\rangle$ -t $|1\rangle$ -be.

Megmérjük az első output qubitet. Ha az első output qubit $|0\rangle$ akkor $f(0) = f(1)$. Ha az első output qubit $|1\rangle$ akkor $f(0) \neq f(1)$. Tehát megkapjuk $f(0) \oplus f(1)$ értékét első output qubit megmérésével.

Egyszer számítjuk ki $f(x)$ függvény értékét. Tehát T idő alatt döntöttük el Deutsch problémáját.

10. A kvantum Fourier transzformáció

A kvantum Fourier transzformáció (QFT) egy operátor amely a $\mathcal{H}_N$ Hilbert tér felett a

$$\{ |0\rangle, |1\rangle, \dots, |j\rangle, \dots, |k\rangle, \dots, |N-1\rangle \}$$

ortonormális bázist áttanszformálja az alábbi módon.

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{i2\pi jk}{N}} |k\rangle.$$

A kvantum Fourier transzformáció (QFT) áthelyezési mátrixa:

$$G_{QFT} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}$$

ahol $\omega = e^{\frac{2\pi i}{N}}$ az 1 szám N -edik gyöke. A G_{QFT} mátrixnak N sora és N oszlopa van.

Állítás 10.1 A QFT a $|0\rangle$ $\mathcal{H}_N$ -beli állapotvektorhoz a

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

állapotvektort rendeli hozzá. Amikor $N = 2^n$, akkor ugyanazt az állapotvektort rendeli hozzá mint a Walsh-Hadamard transzformáció.

Bizonyítás. $G_{QFT}|0\rangle = G_{QFT} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} =$

a G_{QFT} mátrix első oszlopa =

$$= \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

Tekintsük az $N = 2^n$ esetet. Most $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$

$N = 2^n$ komponensű vektor (ami megfelel n darab qubitnek.)

$$G_{QFT}|0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle =$$

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{N}} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \dots + \frac{1}{\sqrt{N}} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}.$$

Legyenek most $|0\rangle$ és $|1\rangle$ $\mathcal{H}_2$ -beli állapotok $\mathcal{H}_N$ -beli állapotok helyett, és hajtsuk végre a Walsh-Hadamard transzformációt a

$$|0\rangle \otimes \dots \otimes |0\rangle$$

$\mathcal{H}_N$ -beli állapoton! Eredményül kapjuk:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =$$

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}$$

□

$$F_{2^3} = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} \end{bmatrix} = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}.$$

69. ábra. A QFT mátrixa $N = 8$ esetén [20]

Tekintsük egy $|v\rangle$ állapotát a kvantum rendszernek! A QFT átranzformálja a $|v\rangle$ állapotot a $|w\rangle$ állapotba az alábbi módon:

$$|v\rangle \mapsto |w\rangle \text{ ahol}$$

$$|v\rangle = \sum_{j=0}^{N-1} v_j |j\rangle,$$

$$|w\rangle = \sum_{k=0}^{N-1} w_k |k\rangle.$$

Minden $k = 0, 1, \dots, N - 1$ esetén,

$$w_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} v_j e^{\frac{i2\pi jk}{N}}.$$

Azt mondjuk hogy a w_k amplitúdók a v_j amplitúdók diszkrét Fourier transzformáltjai.

Tekintsük az $N = 2^n$ esetet. Most a $\mathcal{H}_N$ Hilbert tér felett a $\{ |0\rangle, |1\rangle, \dots, |j\rangle, \dots, |k\rangle, \dots, |N - 1\rangle \}$

ortonormális bázist n darab qubittel a

$$\{ |0 \dots 0\rangle, |0 \dots 1\rangle, \dots, |1 \dots 1\rangle \}$$

alakban írhatjuk fel, ahol

$$|0\rangle = |0 \dots 0\rangle = |0\rangle \dots |0\rangle,$$

$$|1\rangle = |0\rangle \dots |0\rangle |1\rangle = |0\rangle \dots |0\rangle |1\rangle,$$

$$|2\rangle = |0 \dots 10\rangle = |0\rangle \dots |1\rangle |0\rangle,$$

...

$$|N-1\rangle = |1 \dots 1\rangle = |1\rangle \dots |1\rangle.$$

Tekintsük a j és k egész számok kettes számrendszerbeli alakját.

$$j = j_0 2^{n-1} + j_1 2^{n-2} + \dots + j_{n-2} 2^1 + j_{n-1} 2^0.$$

$$k = k_0 2^{n-1} + k_1 2^{n-2} + \dots + k_{n-2} 2^1 + k_{n-1} 2^0.$$

Figyeljük meg hogy

$$|j\rangle = |j_0 2^{n-1} + j_1 2^{n-2} + \dots + j_{n-2} 2^1 + j_{n-1} 2^0\rangle = |j_0 j_1 \dots j_{n-2} j_{n-1}\rangle$$

és

$$|k\rangle = |k_0 2^{n-1} + k_1 2^{n-2} + \dots + k_{n-2} 2^1 + k_{n-1} 2^0\rangle =$$

$$|k_0 k_1 \dots k_{n-2} k_{n-1}\rangle$$

és

$$k_0 2^{n-1} + k_1 2^{n-2} + \dots + k_{n-2} 2^1 + k_{n-1} 2^0 = \sum_{m=0}^{n-1} k_m 2^{n-(m+1)}.$$

A fenti képletek felhasználásával a QFT definícióját az alábbi módon írhatjuk fel:

$$|j\rangle = |j_0 j_1 \dots j_{n-2} j_{n-1}\rangle \mapsto$$

$$\frac{1}{2^{\frac{n}{2}}} \sum_{k_0=0,1} \sum_{k_1=0,1} \dots \sum_{k_{n-1}=0,1} e^{i2\pi j \sum_{m=0}^{n-1} k_m 2^{-(m+1)}} |k_0 k_1 \dots k_{n-2} k_{n-1}\rangle.$$

$$|j\rangle = |j_0 j_1 \dots j_{n-2} j_{n-1}\rangle \mapsto$$

$$\frac{1}{2^{\frac{n}{2}}} \sum_{k_0=0,1} \sum_{k_1=0,1} \dots \sum_{k_{n-1}=0,1} \bigotimes_{m=0}^{n-1} e^{i2\pi j k_m 2^{-(m+1)}} |k_m\rangle.$$

A fenti átalakításban a hatványozás $e^{n+\ell} = e^n \cdot e^\ell$ azonosságát használtuk fel, a kitevőben lévő összeget szorzattá alakítottuk. A kapott szorzat tényezőit egy tenzor szorzat tényezőibe tettük át tényezőként.

$$|j_0 j_1 \cdots j_{n-2} j_{n-1}\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \bigotimes_{m=0}^{n-1} \{ \sum_{k_m=0,1} e^{i2\pi j k_m 2^{-(m+1)}} |k_m\rangle \}.$$

A k_m bit a 0 vagy 1 értéket veszi fel a fenti összegek mindegyikében. Tekintsük azt az esetet amikor $k_m = 0$. Ebben az esetben $e^{i2\pi j k_m 2^{-(m+1)}} = e^0 = 1$. Eképpen $e^{i2\pi j k_m 2^{-(m+1)}} |k_m\rangle = |0\rangle$. Tekintsük azt az esetet amikor $k_m = 1$. Ebben az esetben $e^{i2\pi j k_m 2^{-(m+1)}} |k_m\rangle = e^{i2\pi j 2^{-(m+1)}} |1\rangle$. A fentiek alapján:

$$|j\rangle = |j_0 j_1 \cdots j_{n-2} j_{n-1}\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \bigotimes_{m=0}^{n-1} (|0\rangle + e^{i2\pi j 2^{-(m+1)}} |1\rangle).$$

Vegyük észre hogy

$$|0\rangle + e^{i2\pi j 2^{-(m+1)}} |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ e^{i2\pi j 2^{-(m+1)}} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i2\pi j 2^{-(m+1)}} \end{pmatrix}.$$

Tehát a QFT a $|j\rangle$ inputon az alábbi alakú:

$$|j\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \begin{pmatrix} 1 \\ e^{\frac{i2\pi j}{2^1}} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ e^{\frac{i2\pi j}{2^2}} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ e^{\frac{i2\pi j}{2^3}} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ e^{\frac{i2\pi j}{2^n}} \end{pmatrix}$$

Bevezetjük az alábbi jelölést:

$$0.j_m j_{m+1} \cdots j_{n-1} = j_m 2^{-1} + j_{m+1} 2^{-2} + \cdots + j_{n-1} 2^{m-n}.$$

Szemléletesen, a bal oldalon egy kettes számrendszerbeli tört szám áll. A tört 0-val kezdődik majd a kettes pont következik majd a felek, negyedek, nyolcadok, stb. A jobb oldalon látjuk a

bal oldal értékét törtek összegeként. Például: $0.101 = \frac{1}{2} + \frac{1}{8}$.

Ismert hogy minden x valós szám esetén $e^{ix} = \cos x + i \sin x$.

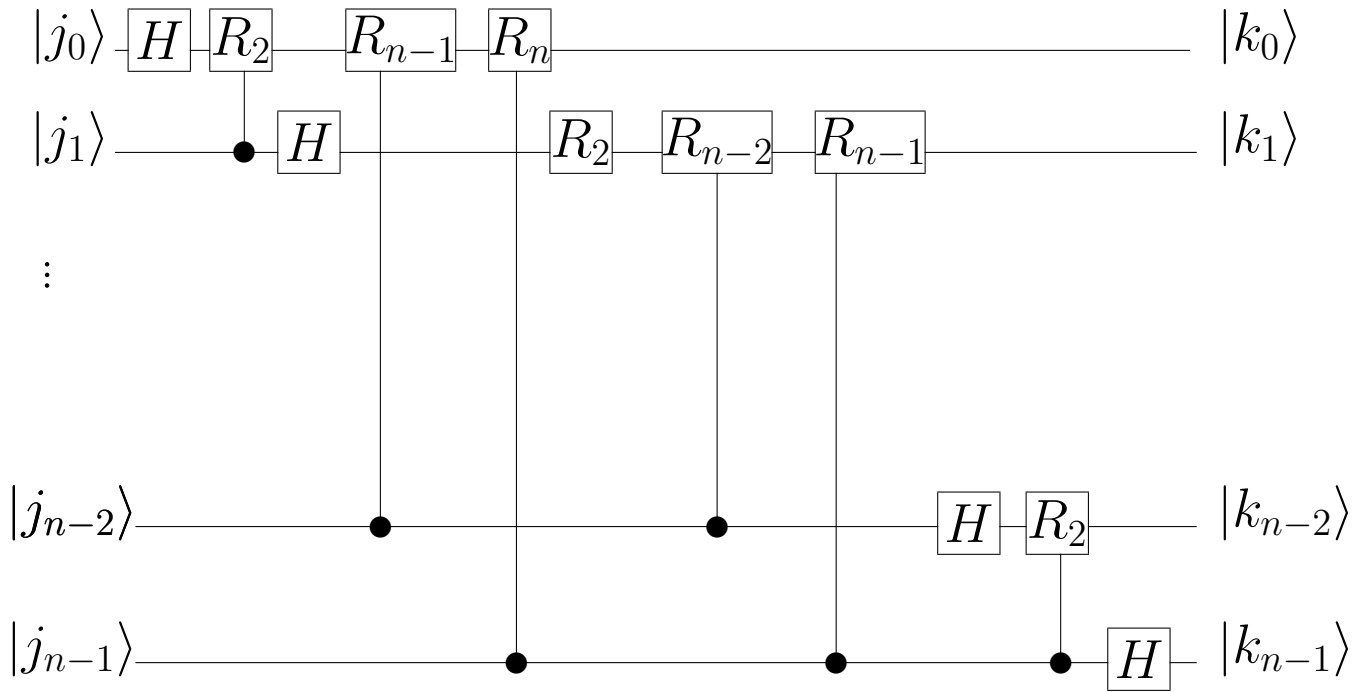
Így $e^{i2k\pi} = 1$, $k = 0, 1, 2, \dots$

A fenti jelölés és egyenlőség alkalmazásával felírjuk a transzformációt:

$$|j\rangle = |j_0 j_1 \cdots j_{n-2} j_{n-1}\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \{ |0\rangle + e^{i2\pi 0 \cdot j_{n-1}} |1\rangle \} \otimes \{ |0\rangle + e^{i2\pi 0 \cdot j_{n-2} j_{n-1}} |1\rangle \} \otimes \cdots \otimes \{ |0\rangle + e^{i2\pi 0 \cdot j_0 j_1 \cdots j_{n-1}} |1\rangle \}.$$

Indoklás: Tekintsük az első tényezőt a tenzor szorzatban: $\{ |0\rangle + e^{i2\pi 0 \cdot j_{n-1}} |1\rangle \}$. A benne szereplő e hatvány kitevőjét úgy kaptuk, hogy levágtuk a $j_0, j_1, \dots, j_{n-2}$ biteket. Azaz csak a $0 \cdot j_{n-1}$ tört részt hagytuk meg. Azért tehettük ezt meg, mert az elhagyott egész részt $i2\pi$ -vel szorozzuk, és mert $e^{i2k\pi} = 1$, $k = 0, 1, 2, \dots$. A második tényezőben az e hatvány kitevőjét úgy kaptuk, hogy levágtuk a $j_0, j_1, \dots, j_{n-3}$ biteket. Azaz csak a $0 \cdot j_{n-1} j_{n-2}$ tört részt hagytuk meg. Azért tehettük ezt meg, mert az egész részt $i2\pi$ -vel szorozzuk, és mert $e^{i2k\pi} = 1$, $k = 0, 1, 2, \dots$.

A 70. ábrán láthatjuk a QFT-t megvalósító kvantum áramkört. Az áramkört a fenti kifejezés alapján építettük fel. Előbb-utóbb minden egyes bázis vektort egy-egy Hadamard kapu segítségével átranszformáljuk. Az így kapott állapot áthalad egy vagy több irányított R_k ($k \geq 1$) kapun keresztül. Emlékezzünk hogy az R_k kapu mátrixa:



70. ábra. A QFT transzformációt megvalósító kvantum áramkör

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix} \text{ minden } k \geq 1 \text{ számra.}$$

Tehát az R_k kapu úgy transzformál át egy qubitet hogy az $|1\rangle$ bázis vektorra vetett vetületét megszorozza a $e^{\frac{2\pi i}{2^k}}$ számmal.

Az első qubitre alkalmazott Hadamard kapu az alábbi állapotváltozást eredményezi:

$$|j_0 j_1 j_2 \dots j_{n-1}\rangle \mapsto \frac{1}{2^{\frac{1}{2}}} (|0\rangle + e^{i2\pi 0 \cdot j_0} |1\rangle) |j_1 j_2 \dots j_{n-1}\rangle$$

itt $e^{i2\pi 0 \cdot j_0} = e^{\frac{i2\pi j_0}{2}} = 1$ ha $j_0 = 0$ és $e^{i2\pi 0 \cdot j_0} = e^{\frac{i2\pi j_0}{2}} = -1$ ha $j_0 = 1$.

Az első qubitre alkalmazott minden egyes irányított R_k kapu hozzáírja az irányító qubitnek megfelelő bitet az e hatványkitevő-

jének a végére. Más szóval, az első qubitnek az $|1\rangle$ bázis vektorra vetett vetületének a fázisához (azaz az $|1\rangle$ bázis vektor együtthatóját e hatványnak tekintve a hatványkitevő végére) írja az irányító qubitnek megfelelő bitet. Ha az irányító qubit $|0\rangle$, akkor a 0 bitet írja hozzá, és ekkor az e szám kitevőjének az értéke nem változik meg. Először a $|j_1\rangle$ irányító qubithez tartozó j_1 bitet. Másodszor a $|j_2\rangle$ irányító qubithez tartozó j_2 bitet. És így tovább. Eredményként az alábbi állapotváltozás sorozatot kapjuk:

$$\begin{aligned}
|j_0 j_1 j_2 \dots j_{n-1}\rangle &\mapsto \frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0 \cdot j_0} |1\rangle) |j_2 \dots j_{n-1}\rangle \\
&\mapsto \text{első irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0 \cdot j_0 j_1} |1\rangle) |j_2 \dots j_{n-1}\rangle \\
&\mapsto \text{második irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0 \cdot j_0 j_1 j_2} |1\rangle) |j_2 \dots j_{n-1}\rangle \\
&\mapsto \text{harmadik irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0 \cdot j_0 j_1 j_2 j_3} |1\rangle) |j_2 \dots j_{n-1}\rangle \mapsto \\
&\dots \\
&\mapsto (n-1)\text{-edik (utolsó) } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0 \cdot j_0 j_1 j_2 \dots j_{n-1}} |1\rangle) |j_2 \dots j_{n-1}\rangle
\end{aligned}$$

A második qubitre alkalmazott minden egyes irányított R_k kapu hozzáírja az irányító qubitnek megfelelő bitet az e hatványkitevőjének a végére. Más szóval, a második qubitnek az $|1\rangle$ bázis vektorra vetett vetületének a fázisához (azaz az $|1\rangle$ bázis vektor együtthatóját e hatványnak tekintve a hatványkitevő végére) írja az irányító qubitnek megfelelő bitet. Ha 0 bitet ír hozzá, akkor

az e szám kitevőjének az értéke nem változik meg. Eredményként az alábbi állapotváltozás sorozatot kapjuk:

$$\begin{aligned}
&\mapsto \text{első irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0.j_0j_1j_2\dots j_{n-1}}|1\rangle)(|0\rangle + e^{i2\pi 0.j_2}|1\rangle) |j_3 \dots j_{n-1}\rangle \\
&\mapsto \text{második irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0.j_0j_1j_2\dots j_{n-1}}|1\rangle)(|0\rangle + e^{i2\pi 0.j_2j_3}|1\rangle) |j_3 \dots j_{n-1}\rangle \\
&\mapsto \text{harmadik irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0.j_0j_1j_2\dots j_{n-1}}|1\rangle)(|0\rangle + e^{i2\pi 0.j_2j_3j_4}|1\rangle) |j_3 \dots j_{n-1}\rangle \\
&\mapsto \text{negyedik irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0.j_0j_1j_2\dots j_{n-1}}|1\rangle)(|0\rangle + e^{i2\pi 0.j_2j_3j_4j_5}|1\rangle) |j_3 \dots j_{n-1}\rangle \\
&\dots \\
&\mapsto \text{utolsó irányított } R_k \text{ kapu} \mapsto \\
&\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{i2\pi 0.j_0j_1j_2\dots j_{n-1}}|1\rangle)(|0\rangle + e^{i2\pi 0.j_2j_3j_4\dots j_{n-1}}|1\rangle) |j_3 \dots j_{n-1}\rangle.
\end{aligned}$$

A fentiek szerint folytatjuk minden egyes qubitre.

Az $n - 1$ -edik qubitre alkalmazott irányított R_k kapu hozzáír egy bitet az $n - 1$ -edik qubitnek az $|1\rangle$ bázis vektorra vetett vetület fázisához (azaz az e szám kitevőjének a végére ír egy bitet).

Megkapjuk a végső állapotot:

$$\frac{1}{2^{\frac{n}{2}}} \{ |0\rangle + e^{i2\pi 0.j_0j_1\dots j_{n-1}}|1\rangle \} \otimes \{ |0\rangle + e^{i2\pi 0.j_1\dots j_{n-1}}|1\rangle \} \otimes \dots \otimes \{ |0\rangle + e^{i2\pi 0.j_{n-2}j_{n-1}}|1\rangle \} \{ |0\rangle + e^{i2\pi 0.j_{n-1}}|1\rangle \}.$$

Az átláthatóság kedvéért az 70. ábrán nem mutatjuk az output qubitek sorrendjét felcserélő kapukat. Ezek segítségével megfordítjuk az output qubitek sorrendjét. Kapjuk:

$$\frac{1}{2^{\frac{n}{2}}} \{ |0\rangle + e^{i2\pi 0 \cdot j_{n-1}} |1\rangle \} \otimes \{ |0\rangle + e^{i2\pi 0 \cdot j_{n-2} j_{n-1}} |1\rangle \} \otimes \cdots \otimes \{ |0\rangle + e^{i2\pi 0 \cdot j_0 j_1 \cdots j_{n-1}} |1\rangle \}.$$

Az 70. ábrán látható kvantum kapuk száma: $1+2+\cdots+n = \frac{n}{n+1}$. Az első és utolsó output qubitet cseréljük fel. A második és utolsó előtti output qubitet cseréljük fel. És így tovább. Tehát legfeljebb $\frac{n}{2}$ darab csere van. Minden egyes cserét 3 darab CNOT kapuval valósítunk meg, lásd 34. ábra.

A fenti áramkör $N = 2^n$ esetén számítja ki a kvantum Fourier transzformációt. Különbözik csupán a kvantum Fourier transzformáció közelítését adja (azaz közelítő eredményt ad).

11. A Fourier transzformáció a véges Ábel csoport felett

Legyen $(G, +)$ egy tetszőleges véges Ábel csoport! A csoport műveletet $+$ jelöli. $|G|$ jelöli G elemeinek a számát. Legyen C^* a nullától különböző komplex számok halmaza! Tekintsük a

$$\chi : G \rightarrow C^*$$

függvényt! Azt mondjuk hogy χ egy irreducibilis reprezentációja G -nek ha teljesül hogy

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2). \quad (6)$$

Azaz, χ egy csoport homomorfizmus a $(G, +)$ additív csoportból a $(C^*, \cdot)$ multiplikatív csoportba. Itt $\cdot$ a komplex számok jól ismert szorzás műveletét jelöli.

Jelölje S^1 az 1 abszolút értékű komplex számok halmazát! Figyeljük meg, hogy χ értékészlete részhalmaza S^1 -nek, tehát $\chi : G \rightarrow S^1$ leképezés. Mert ha $\chi(g)$ komplex szám $|\chi(g)|$ abszolút értéke nagyobb 1-nél, akkor

$$|\chi(g)| < |\chi(g+g)| < |\chi(g+g+g)| < \dots$$

ellentmond annak, hogy G véges. Hasonlóan látható hogy $\chi(g)$ abszolút értéke nem kisebb 1-nél. A (6) egyenlőség az alábbi (A), (B) és (C) következményeket eredményezi.

(A) (i) Minden $g \in G$ esetén, $\chi(g)$ az egyik $|G|$ -edik gyöke az 1 számnak. Itt $|G|$ jelöli G elemeinek a számát.

Az (A)(i) állítás alapján kapjuk hogy

(A) (ii) $\chi : G \rightarrow S^1$ csoport homomorfizmus a $(G, +)$ additív csoportból az $(S^1, \cdot)$ multiplikatív csoportba.

(B) Merőlegesség (Schur lemmája) Ha χ_i és χ_j két irreducibilis reprezentációja G -nek, akkor

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij} \quad (7)$$

ahol a felülhúzás a komplex szám konjugáltjának a képzését jelöli, azaz $\bar{c}$ jelöli a c komplex szám konjugáltját.

(C) Pontosan $|G|$ darab olyan χ függvény létezik amely kielégíti a (6) egyenlőséget.

A (C) állítás alapján ezeket a függvényeket meg tudjuk címkézni a G csoport elemeivel. Legyen $\{\chi_g | g \in G\}$ tetszőleges ilyen megcímkézés.

Igazoljuk (A) és (B) állításokat!

A H csoport elemeinek a számát a H csoport rendjének nevezzük.

Tétel 11.1 Lagrange tétele. *Részcsoport rendje osztója az őt tartalmazó csoport rendjének.*

Állítás 11.2 $\chi(e) = 1$, ahol e a G egységeleme. Minden $g \in G$ esetén $\chi(\sum_{i=1}^{|G|} g) = 1$.

A (6) egyenlőség alapján $\chi(e) = 1$. Ugyanis $\chi(e) = \chi(e + e) = \chi(e)\chi(e)$. Tehát $\chi(e) = \chi(e)\chi(e)$. Ezért $\chi(e) = 1$.

Állítás 11.3 Tegyük fel hogy $g \neq e$. Létezik $\ell \geq 2$ úgy hogy $e = \sum_{i=1}^{\ell} g$ és $e, g, \sum_{i=1}^2 g, \sum_{i=1}^3 g, \dots, \sum_{i=1}^{\ell-1} g$ különböző elemei G -nek.

Bizonyítás Az $e, g, \sum_{i=1}^2 g, \sum_{i=1}^3 g, \dots, \sum_{i=1}^n g$ sorozatban először ismétlődik valamely elem:

$$\sum_{i=1}^k g = \sum_{i=1}^n g, \quad k < n.$$

Mindkét oldalhoz hozzáadjuk a $\sum_{i=1}^k g$ elem $-\sum_{i=1}^k g$ inverzét. Kapjuk hogy $e = \sum_{i=1}^{n-k} g$. Legyen $\ell = n - k$. $\square$

A fenti állítás alapján $\{e, g, \sum_{i=1}^2 g, \sum_{i=1}^3 g, \dots, \sum_{i=1}^{\ell-1} g\}$ a G -beli összeadás műveletével G -nek egy részcsoportját alkotják.

A fentiek alapján

$$\chi(\sum_{i=1}^{\ell} g) = \chi(e) = 1.$$

Lagrange tétele alapján kapjuk hogy ℓ osztója $|G|$ -nek. Tehát $|G| = \ell \cdot k$ és így

$$\chi(\sum_{i=1}^{|G|} g) = \chi(\sum_{i=1}^k (\sum_{i=1}^{\ell} g)) = (\chi(e))^k = 1.$$

Ezért $\chi(\sum_{i=1}^{|G|} g) = 1$.

$\square$

A (6) egyenlőség és a 11.2 állítás alapján $\chi(g)$ az egyik $|G|$ -edik gyöke az 1 számnak, azaz $\chi(g)^{|G|} = 1$. Ezért $\chi(g)$ abszolútértéke 1. Mivel $\chi(g)$ abszolútértéke 1, az ő konjugáltjának is 1 az abszolútértéke. A komplex számok szorzatának definíciója szerint $\chi(g)\overline{\chi(g)} = 1$.

$$\overline{\chi(g)} = \frac{1}{\chi(g)}.$$

Továbbá $1 = \chi(e) = \chi(g + (-g)) = \chi(g) \cdot \chi(-g)$. Tehát

$$\chi(-g) = \frac{1}{\chi(g)}.$$

A fentiek alapján:

$$\overline{\chi(g)} = \chi(-g). \quad (8)$$

Legyen χ_1 és χ_2 két irreducibilis reprezentációja G -nek! Legyen $g, h \in G$ tetszőleges, és $\tilde{g} = h + g$, ezzel az egyenlőséggel bevezetett változóval számolunk:

$$\chi_1(h) \sum_{g \in G} \chi_1(g) \chi_2(-g) = \sum_{g \in G} \chi_1(h + g) \chi_2(-g) =$$

$$\sum_{\tilde{g} \in G} \chi_1(\tilde{g}) \chi_2((- \tilde{g}) + h) =$$

$$\left[\sum_{\tilde{g} \in G} \chi_1(\tilde{g}) \chi_2(-\tilde{g}) \right] \chi_2(h) =$$

$$\chi_2(h) \sum_{\tilde{g} \in G} \chi_1(\tilde{g}) \chi_2(-\tilde{g})$$

A fentiek alapján, az összegzés $\tilde{g}$ futóindexe helyébe g -t írunk:

$$\chi_1(h) \sum_{g \in G} \chi_1(g) \chi_2(-g) = \chi_2(h) \sum_{g \in G} \chi_1(g) \chi_2(-g)$$

$$[\chi_1(h) \sum_{g \in G} \chi_1(g) \chi_2(-g)] - [\chi_2(h) \sum_{g \in G} \chi_1(g) \chi_2(-g)] = 0$$

Eképpen (8) alapján minden $h \in G$ esetén:

$$(\chi_1(h) - \chi_2(h)) \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = 0.$$

Ha $\chi_1 \neq \chi_2$, akkor valamely $h \in G$ esetén $\chi_1(h) - \chi_2(h) \neq 0$. Következésképpen

$$\sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = 0.$$

Tegyük fel hogy $\chi_1 = \chi_2 = \chi$. Akkor

$$\sum_{g \in G} \chi(g) \overline{\chi(g)} = \sum_{g \in G} \chi(g) \chi(-g) = \sum_{g \in G} \chi(e) = \sum_{g \in G} 1 = |G|$$

Ezzel igazoltuk (7)-t, azaz (B)-t (Schur lemmáját).

Definíció 11.4 A G feletti Fourier transzformáció áthelyező mátrixa az alábbi $|G| \times |G|$ méretű $\mathcal{F}$ mátrix

$$[\mathcal{F}_{g,k}] = \frac{1}{\sqrt{|G|}} \chi_g(k) \quad g, k \in G. \quad (9)$$

Itt feltesszük hogy G elemei meg vannak számozva az $1, 2, \dots, |G|$ számokkal és az $\mathcal{F}$ mátrix i -edik sorát G i -edik elemével címkézzük meg. Hasonlóan az $\mathcal{F}$ mátrix j -edik oszlopát G j -edik elemével címkézzük meg. Ezután a sorokra és oszlopokra a G -beli címkéjükkel hivatkozunk.

Látjuk hogy az $\mathcal{F}$ mátrix g -edik sora az $\frac{1}{\sqrt{|G|}}\chi_g$ függvény értékeinek a felsorolása. A (B) állítás alapján $\mathcal{F}$ mátrix unitér tetszőleges $(G, +)$ csoport esetén. Emlékezzünk hogy az U $n \times n$ -es mátrixot unitérnek nevezzük ha $U^\dagger U = U U^\dagger = I_n$, ahol I_n az $n \times n$ -es egység mátrix.

Tekintsük a $|G|$ dimenzós $\mathcal{H}_{|G|}$ Hilbert teret! Címkezzük meg a bázis elemeit G elemeivel! Tehát a bázis: $\{ |g\rangle | g \in G \}$. Minden $k \in G$ esetén, tekintsük az

$$U(k) : |b\rangle \rightarrow |b + k\rangle \quad k, b \in G. \quad (10)$$

léptető függvényt. Minden $k, l \in G$ esetén, $U(k)U(l) = U(l)U(k)$ mert $(G, +)$ Ábel csoport.

Definíció 11.5 Legyen

$$(\forall k \in G) \quad |\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\chi_k(g)} |g\rangle. \quad (11)$$

Átjelölve a változókat:

$$(\forall g \in G) \quad |\chi_g\rangle = \frac{1}{\sqrt{|G|}} \sum_{k \in G} \overline{\chi_g(k)} |k\rangle. \quad (12)$$

(B) alapján a $|\chi_k\rangle$ állapotok egy ortonormális bázist alkotnak a $\mathcal{H}_{|G|}$ Hilbert térben. Mert tetszőleges $i, j \in G$ esetén,

$$(|\chi_i\rangle, |\chi_j\rangle) = \langle \chi_i | \chi_j \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} \langle g | g \rangle = \delta_{ij}.$$

Most a $\mathcal{H}_{2^n}$ Hilbert teret tekintjük, azaz $N = 2^n$.

Állítás 11.6 A $\mathcal{H}_{2^n}$ Hilbert tér felett ($N = 2^n$)

$$U(b)(|\chi_k\rangle) = e^{\chi_k(b)}|\chi_k\rangle \quad b, k \in G.$$

Így a $\{ |\chi_g\rangle | g \in G \}$ állapothalmaz az $U(k)$, $k \in G$ léptető függvények közös sajátvektor bázisa. Ezt a bázist Fourier bázisnak is hívjuk. Az $\mathcal{F}$ Fourier transzformáció egy unitér operátor a $\mathcal{H}_{|G|}$ Hilbert tér felett. A (12) és (9) egyenlőségek és (B) alapján kapjuk hogy

$$\mathcal{F}|\chi_g\rangle = |g\rangle. \quad (13)$$

Ezek szerint a Fourier transzformáció felcseréli a Hilbert tér bázisát a Fourier bázissal.

Jelölje $\mathbf{Z}_q$ az egész számok mod q additív csoportját.

Állítás 11.7 Minden véges G Ábel csoporthoz léteznek $r, m_1, m_2, \dots, m_r$ természetes számok úgy hogy G izomorf a $\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \dots \times \mathbf{Z}_{m_r}$ direkt szorzattal definiált Ábel csoporttal. Azaz

$$G \cong \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \dots \times \mathbf{Z}_{m_r} \quad (14)$$

Úgy is megadhatjuk az $r, m_1, m_2, \dots, m_r$ természetes számokat hogy m_i osztója m_{i+1} -nek. Ekkor az m_i számok egyértelműen adóttak.

Tegyük fel hogy a G Ábel csoportot a (14) alakban adjuk meg. Akkor explicit módon meg tudjuk adni G irreducibilis reprezentációit, és megkapjuk G irreducibilis reprezentációinak G elemeivel való címkézését.

Először tegyük fel hogy $G \cong \mathbf{Z}_m$. Azt is írhatjuk hogy $G = \mathbf{Z}_m$. Most G elemei megegyeznek a $\{0, 1, \dots, m-1\}$ halmaz elemeivel. Tekintsük a $\tau : G \times G \rightarrow S^1$ leképezést, ahol

$$\tau : (a, b) \mapsto e^{2\pi i \frac{ab}{m}}. \quad (15)$$

A $\tau : G \times G \rightarrow S^1$ leképezés felhasználásával csoport homomorfizmusokat definiálunk. Minden $a \in G$ esetén tekintsük a $\chi_a : G \rightarrow S^1$ függvényt, ahol

$$\chi_a(b) = \tau(a, b) = e^{2\pi i \frac{ab}{m}}. \quad (16)$$

Állítás 11.8 Minden $a \in G$ esetén $\chi_a : G \rightarrow S^1$ kielégíti a (6) feltételt.

A (C) állítás szerint $|G|$ darab χ olyan függvény létezik amely kielégíti a (6) egyenlőséget. A 11.8 állítás alapján ezek a $\chi_a : G \rightarrow S^1$, $a \in G$, függvények. Így egy explicit képletet kaptunk amely megadja az irreducibilis reprezentációit G -nek. Most már be tudjuk bizonyítani a 11.6 állítást.

Másodszor tekintsük az általános esetet:

$$G = \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \dots \times \mathbf{Z}_{m_r}.$$

Tekintsük a $\tau : G \times G \rightarrow S^1$ leképezést:

$$\tau : ((a_1, \dots, a_r), (b_1, \dots, b_r)) \mapsto \exp(2\pi i [\frac{a_1 b_1}{m_1} + \frac{a_2 b_2}{m_2} + \dots + \frac{a_r b_r}{m_r}]). \quad (17)$$

A $\tau : G \times G \rightarrow S^1$ leképezés felhasználásával csoport homomorfizmusokat definiálunk. Ismét minden $g_1 \in G$ esetén tekintsük a

$\chi_{g_1} : G \rightarrow S^1$ függvényt, ahol

$$\chi_{g_1}(g_2) = \tau(g_1, g_2) \quad (18)$$

Állítás 11.9 Minden $g_1 \in G$ esetén $\chi_{g_1} : G \rightarrow S^1$ kielégíti a (6) feltételt.

Így egy explicit képletet kaptunk amely megadja az irreducibilis reprezentációit G -nek. A képletben G elemeit megadó (reprezentáló) r darab egész számból álló sorozatok szerepelnek.

Példák.

1. Példa. Legyen $n \geq 1$. Tekintsük a $G = (\mathbf{Z}_2)^n$ csoportot! Ez n darab $\mathbf{Z}_2$ csoport direkt szorzata. $(\mathbf{Z}_2)^n$ -t úgy tekinthetjük mint a bitekből álló n hosszú sztringek halmazát. A szorzást bitenként hajtjuk végre. Definiáljuk tetszőleges $\sigma = s_1 s_2 \dots s_n \in (\mathbf{Z}_2)^n$ és $\nu = t_1 t_2 \dots t_n \in (\mathbf{Z}_2)^n$ szavakra, a $\sigma \cdot \nu \in \{0, 1\}$ értéket:

$$\sigma \cdot \nu = s_1 t_1 + s_2 t_2 + \dots + s_n t_n \text{ mod } 2.$$

A (17), (18) és (9) egyenlőségekből következik hogy

$$[\mathcal{F}_{\sigma, \nu}] = \frac{1}{\sqrt{|G|}} \chi_{\sigma}(\nu) \quad \sigma, \nu \in G.$$

Tehát

$$[\mathcal{F}_{\sigma, \nu}] = \frac{1}{\sqrt{2^n}} \exp(i 2\pi \frac{\sigma \cdot \nu}{2}) \quad \sigma, \nu \in G.$$

Tehát

$$[\mathcal{F}_{\sigma, \nu}] = \frac{1}{\sqrt{2^n}} (-1)^{\sigma \cdot \nu}.$$

Tehát ebben az esetben a Fourier transzformáció mátrixa megegyezik a Hadamard-Walsh transzformáció mátrixával. Tehát

ebben az esetben a Fourier transzformáció megegyezik a Hadamard-Walsh transzformációval.

2. Példa. Tekintsük a $G = \mathbf{Z}_{2^n}$ csoportot! Legyen $\mathcal{F}$ $G \times G$ -s mátrix a Fourier transzformáció mátrixa. Most a (15) és (18) egyenlőségek alapján

$$[\mathcal{F}_{a,b}] = \frac{1}{\sqrt{|G|}} \chi_a(b) \quad a, b \in G.$$

Tehát

$$[\mathcal{F}_{a,b}] = \frac{1}{\sqrt{2^n}} \exp(i2\pi \frac{ab}{2^n}) \quad a, b = 0, 1, 2, \dots, 2^n - 1. \quad (19)$$

Ez a kvantum Fourier transzformáció mátrixának képlete $N = 2^n$ esetén.

A Fourier transzformáció unitér mátrixa $|G|$ hosszú ($|G|$ darab komponensből álló) vektorokat transzformál át $|G|$ hosszú vektorokba. Egy ilyen $|G|$ hosszú vektort megadhatunk egy

$$f : G \rightarrow C$$

függvénnyel és a vektor pedig $f = (f(g_1), f(g_2), \dots, f(g_{|G|}))$ alakú. Az f Fourier transzformáltja egy $|G|$ hosszú $\tilde{f}$ vektor. $\tilde{f} = (\tilde{f}(g_1), \tilde{f}(g_2), \dots, \tilde{f}(g_{|G|}))$. A fenti jelölés felhasználásával $\tilde{f}$ -et az alábbi alakban írjuk fel.

$$\tilde{f}(k) = \sum_{g \in G} \mathcal{F}_{kg} f(g) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi_k(g) f(g), \quad k \in G. \quad (20)$$

Legyen H tetszőleges részcsoportha a G csoportnak! H -nak az I indexét a következő módon definiáljuk:

$$I = \frac{|G|}{|H|}.$$

Legyenek

$$k_1 + H, k_2 + H, \dots, k_I + H$$

a H részcsoporthoz összes mellékosztálya. Itt

$$k + H = \{ k + h \mid h \in H \}.$$

Ismert hogy G diszjunkt úniója a fenti mellékosztályoknak.

Eképpen G elemeit egyértelműen írhatjuk $g = k_i + h$ alakban.

Amikor g értékül felveszi (befutja) a G halmaz összes elemét, akkor i értékül felveszi az $\{1, \dots, I\}$ halmaz összes elemét. Minden $i = 1, 2, \dots, I$ esetén, h értékül felveszi H összes elemét.

Minden $i = 1, 2, \dots, I$ esetén, definiáljuk az f_i függvényt!

Legyen

$$f_i : H \rightarrow C, \text{ ahol } f_i(h) = f(k_i + h), h \in H.$$

A (20) és (6) egyenlőségek alapján:

$$\tilde{f}(l) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g) \chi_l(g) = \frac{1}{\sqrt{|G|}} \sum_{i=1}^I \sum_{h \in H} f(k_i + h) \chi_l(k_i + h) = \quad (21)$$

$$\frac{1}{\sqrt{|G|}} \sum_{i=1}^I \chi_l(k_i) \sum_{h \in H} f_i(h) \chi_l(h) \quad (22)$$

A 11.8 állítás alapján kapjuk a következő állítást. Minden $l \in G$ esetén a $\chi_l : G \rightarrow S^1$ leképezés megszorítása a H részcsoporthoz kielégíti a (6) feltételt. Ezért minden $l \in G$ esetén a $\chi_l : G \rightarrow S^1$ leképezés megszorítása a H részcsoporthoz irreducibilis reprezentációja H -nak. Ezért a (22) egyenlőség belsejében lévő H feletti összeg az f_i függvénynek a H részcsoporthoz vett Fourier

transzformáltjának a kiértékelése. Így a (22) egyenlőség felbontja a G csoporton vett Fourier transzformációt I darab, a H részcsoporthon vett Fourier transzformáció kiértékelésére. (Ez $O(|H|^2 \times I)$ darab művelet.) Az így kapott I darab részösszeg lineáris kombinációját vesszük: a $\chi_l(k_i)$ együtthatóval szorozzuk az i -edik részösszeget, $i = 1, \dots, I$. Ezt minden egyes $l \in G$ elemre megcsináljuk. (Ez $O(|G| \times I)$ darab művelet.) Tehát az elvégzett műveletek száma:

$$O(|H|^2 \times I + |G| \times I) = O(|G|(|H| + I)). \quad (23)$$

Itt felhasználtuk hogy $I = \frac{|G|}{|H|}$. Ez általában kevesebb mint a $O(|G| \cdot |G|)$ darab művelet amely a mátrix szorzás költsége amikor hagyományos módon, mátrix szorzással számoljuk ki a Fourier transzformációt a G csoporton. Például ha úgy választjuk meg a H -t hogy I kicsi, mondjuk $I = 2$, akkor $|H| = \frac{1}{2}|G|$ és így a (23) egyenlőség alapján megközelítőleg megfelezzük a futási időt.

Ezt az előnyt megnöveljük a konstrukció ismételtetésével. Tekintünk egy rész-csoportokból álló tornyot és azon ismételtetjük a konstrukciót. Tekintsük a leghosszabb

$$\{0\} \subset H_n \subset \dots \subset H_2 \subset H_1 \subset G$$

részcsoporthoz tartozó tornyot! A fenti eljárás ismételtetésével a Fourier transzformációt a G csoporton kifejezzük a H_n kicsiny részcsoporthon számolt a Fourier transzformációval.

Példa

Legyen $G = \mathbf{Z}_{2^n}$! Legyen $n \geq 2$ és

$W_{2^{n-1}} = \{ 0, 2, 4, \dots, 2^n - 2 \}$ az összes páros szám $\mathbf{Z}_{2^n}$ -ben!

Legyen $W_{2^{n-2}} = \{ 0, 4, 8, \dots, 2^n - 4 \}$ az összes 4-gyel osztható szám $\mathbf{Z}_{2^n}$ -ben!

Legyen $W_{2^{n-3}} = \{ 0, 8, 16, \dots, 2^n - 8 \}$ az összes 8-cal osztható szám $\mathbf{Z}_{2^n}$ -ben!

És így tovább.

Végül legyen $W_2 = \{ 0, 2^{m-1} \}$!

Így kapjuk a

$$\{ 0 \} \subset W_2 \subset \dots \subset W_{2^{n-3}} \subset W_{2^{n-2}} \subset W_{2^{n-1}}$$

részcsoporthoronyot. Itt 0 az egységelem.

Figyeljük meg hogy $W_{2^{n-1}}$ izomorf $\mathbf{Z}_{2^{n-1}}$ -gyel! Továbbá $W_{2^{n-2}}$ izomorf $\mathbf{Z}_{2^{n-2}}$ -vel! És így tovább. Végül kapjuk hogy W_2 izomorf $\mathbf{Z}_2$ -vel! Ennek a megjegyzésnek a tükrében beszélhetünk a $W_{2^{n-1}}$ csoport páros elemeiről. Ilyenkor mindig $\mathbf{Z}_{2^{n-2}}$ -re gondolunk, mivel $W_{2^{n-1}}$ csoport páros elemei alkotta részcsoporthorony izomorf $\mathbf{Z}_{2^{n-2}}$ -vel. Hasonló a helyzet a páratlan elemek alkotta részcsoporthoronyra. Beszélhetünk a $W_{2^{n-1}}$ csoport páratlan elemeiről. Ilyenkor is mindig $\mathbf{Z}_{2^{n-2}}$ -re gondolunk.

Tekintsük a fenti láncban az általános helyet: $W_{2^{m-1}} \subset W_{2^m}$. Jelölje FT_{2^m} a Fourier transzformációt W_{2^m} felett! Legyen $\omega = \exp(\frac{2\pi i}{2^m})$. Most W_{2^m} irreducibilis reprezentációi:

$$\chi_j(k) = (\omega^j)^k \quad j, k = 0, 1, \dots, 2^m - 1 \quad (24)$$

Lásd (15) és (16) egyenlőségeket.

Most a (21) első egyenlőségében kiírjuk az $g \in G$ -összeget explicit módon. Így kapjuk hogy minden $j = 0, 1, \dots, 2^m - 1$

esetén

$$\begin{aligned}
\tilde{f}(j) &= \sum_{k=0}^{2^m-1} f(k) \frac{\chi_j(k)}{\sqrt{2^m}} = \\
&= \frac{1}{\sqrt{2}} \left(\sum_{k=0}^{2^{m-1}-1} f(2k) \frac{\omega^{j2k}}{\sqrt{2^{m-1}}} + \omega^j \sum_{k=0}^{2^{m-1}-1} f(2k+1) \frac{\omega^{j2k}}{\sqrt{2^{m-1}}} \right) \quad (25) \\
&= \frac{1}{\sqrt{2}} \left(\sum_{k=0}^{2^{m-1}-1} f(2k) \frac{\chi_j(2k)}{\sqrt{2^{m-1}}} + \omega^j \sum_{k=0}^{2^{m-1}-1} f(2k+1) \frac{\chi_j(2k)}{\sqrt{2^{m-1}}} \right).
\end{aligned}$$

A fenti egyenlőség jobb oldalának az első tagja mutatja az f függvényt a W_{2^m} páros részosztályán (azaz W_{2^m} páros elemein), a második tagja mutatja az f függvényt a W_{2^m} páratlan részosztályán (azaz W_{2^m} páratlan elemein).

Megjegyezzük hogy $W_{2^{m-1}}$ irreducibilis reprezentációi a (24)-ben megadott függvények, azzal a módosítással hogy ω helyébe $\omega^2 = \exp(\frac{2\pi i}{2^{m-1}})$ -t helyettesítünk. (Jegyezzük meg hogy $((\omega^2)^{2^{m-1}} = 1)$. Azaz $W_{2^{m-1}}$ irreducibilis reprezentációi:

$$\chi_\ell(k) = ((\omega^2)^\ell)^k = (\exp(\frac{2\pi i}{2^{m-1}})^\ell)^k \quad \ell, k = 0, 1, \dots, 2^{m-1} - 1$$

Eképpen a fenti egyenlőség jobb oldalának két k -összege rendre az $FT_{2^{m-1}}$ transzformáltja az f függvény páros helyen felvett értékeinek, és az $FT_{2^{m-1}}$ transzformáltja az f függvény páratlan helyen felvett értékeinek. Legyen ℓ az f függvény argumentumában lévő változó! Mivel ℓ végigfut a $\ell = 0, 1, \dots, 2^m - 1$ értékeken, végigmegyünk a fenti egyenlőség jobb oldalában lévő két $FT_{2^{m-1}}$ transzformáció összesen 2^m darab komponensén. Most a $\{0, 1, \dots, 2^m - 1\}$ halmazt két részre osztjuk, az első részen ℓ

fut végig, a másodikon $\ell + 2^{m-1}$ fut végig. Úgy szorítjuk meg ℓ -t hogy ℓ végigfut a $0, 1, \dots, 2^{m-1} - 1$ értékeken, $\ell + 2^{m-1}$ végigfut a $2^{m-1}, \dots, 2^m - 1$ értékeken. Most $\tilde{f}(\ell)$ és $\tilde{f}(\ell + 2^{m-1})$ előfordulnak a fenti egyenlőség jobb oldalában a két $FT_{2^{m-1}}$ transzformáció ℓ -edik komponensében rendre az alábbi együtthatókkal:

$$\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\omega^j, \text{ (ezek } \tilde{f}(\ell) \text{ együtthatói)}$$

és

$$\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\omega^{j+2^{m-1}} (= -\frac{1}{\sqrt{2}}\omega^j). \text{ (ezek } \tilde{f}(\ell + 2^{m-1}) \text{ együtthatói)}$$

Ugyanis, vegyük észre hogy

$$\frac{1}{\sqrt{2}}\omega^{j+2^{m-1}} = \frac{1}{\sqrt{2}}\omega^{2^{m-1}}\omega^j = \frac{1}{\sqrt{2}}(\exp(\frac{2\pi i}{2^m}))^{2^{m-1}}\omega^j = \frac{1}{\sqrt{2}}\exp(\pi i)\omega^j = -\frac{1}{\sqrt{2}}\omega^j.$$

Ezért a (25) egyenlőséget az alábbi alakban írhatjuk fel:

$$\tilde{f}(j) = \frac{1}{\sqrt{2}}(FT(f_{ps})_{j.komp} + \omega^j \cdot FT(f_{ptn})_{j.komp})$$

$$\tilde{f}(j+2^{m-1}) = \frac{1}{\sqrt{2}}(FT(f_{ps})_{j.komp} - \omega^j \cdot FT(f_{ptn})_{j.komp}) \quad (26)$$

Azaz minden $j = 0, 1, 2, \dots, 2^{m-1} - 1$ esetén

$$\tilde{f}(j) = \frac{1}{\sqrt{2}}(FT(f_{ps})_j + \omega^j \cdot FT(f_{ptn})_j)$$

$$\tilde{f}(j + 2^{m-1}) = \frac{1}{\sqrt{2}}(FT(f_{ps})_j - \omega^j \cdot FT(f_{ptn})_j)$$

itt f_{ps} vektor jelenti f -nek 2^{m-1} darab páros helyen felvett értékét, $f_{ps} = (f(0), f(2), \dots, f(2^{m-1} - 2))$.

f_{ptn} vektor jelenti f -nek 2^{m-1} darab páratlan helyen felvett értékét, $f_{ptn} = (f(1), f(3), \dots, f(2^{m-1} - 1))$.

11.1. A véges Ábel csoport feletti Fourier transzformáció megvalósítása kvantum áramkörrel

Most áttérünk a kvantum számításra. Az $f(j)$, $j = 0, 1, \dots, 2^m - 1$, adat értékeket, azaz az $f = (f(1), f(2), \dots, f(2^m - 1))$ vektort az $|f\rangle$ állapotban tároljuk a következő módon. Az $|f\rangle$ állapotot m darab qubit összefonódása eredményeként kapjuk, az $f(j)$, $j = 0, 1, \dots, 2^m - 1$, adat értékek az előbbi m darab qubit amplitúdóiban vannak tárolva. Írjuk fel a j számot m darab bit sorozataként:

$$j_{m-1}j_{m-2} \dots, j_1j_0$$

Azaz a 2-es számrendszerben, azzal a módosítással hogy a szám előtt elegendő sok 0 áll hogy a szám hossza m legyen. A qubiteket jobbról balra számozzuk meg. Most az $|f\rangle$ állapotot így írjuk fel:

$$|f\rangle = \sum_{j_0=0,1} \sum_{j_1=0,1} \dots \sum_{j_{m-1}=0,1} f(j_{m-1}j_{m-2} \dots j_1j_0) |j_{m-1}\rangle \dots |j_1\rangle |j_0\rangle \quad (27)$$

Figyeljük meg hogy ha $|j_0\rangle, \dots, |j_{m-1}\rangle$ sorra felveszik a $|0\rangle$ és $|1\rangle$ értékeket, akkor a

$|j_{m-1}\rangle \dots |j_1\rangle |j_0\rangle$ állapotvektor sorra felveszi a $|0\rangle, |1\rangle, \dots, |2^m - 1\rangle$ értékeket.

A qubiteket jobbról balra megszámozzuk a $0, 1, \dots, m - 1$ számokkal. Tekintsük a (25) egyenlőség jobb oldalát! Az itt

szereplő összeg két tagjában két $FT_{2^{m-1}}$ transzformáció szerepel. Az első a páros számmal számozott, a második a páratlan számmal számozott komponenseken számol. Ezt a két $FT_{2^{m-1}}$ transzformációt egyetlen $FT_{2^{m-1}}$ művelettel hajtjuk végre az $m-1, m-2, \dots, 2, 1$ sorszámú qubiteken. Kimarad a 0 sorszámú qubit. Ennek a qubitnek a $|0\rangle$ vagy $|1\rangle$ értéke határozza meg hogy a páros pozíciókon vagy a páratlan pozíciókon számolunk. Ha a 0 sorszámú – azaz az utolsó – qubitnek az értéke $|0\rangle$ akkor a páros pozíciókon számolunk. Gondoljunk a tenzor szorzat definíciójára. (A pozíciók sorszámozása 0-val kezdődik, ezért a legelső dimenzió páros sorszámú, a következő pozíció pedig páratlan sorszámú.)

$FT_{2^{m-1}}(f_{ps})$ állapotvektor i -edik komponense a (25) jobb oldalán álló kifejezés $2i$ -edik dimenziójának az amplitúdója, azaz a jobb oldalon álló állapotvektor $2i$ -edik komponense. (Itt az ℓ -edik dimenzió a 2^m dimenziós Hilbert tér $|\ell\rangle$ bázis vektora, $\ell = 0, 1, \dots, 2^{m-1}$. Tehát az ℓ -edik dimenzió amplitúdója a 2^m dimenziós Hilbert tér $|\ell\rangle$ bázis vektorának az amplitúdója, $\ell = 0, 1, \dots, 2^{m-1}$.)

Hasonlóan $FT_{2^{m-1}}(f_{ptn})$ állapotvektor i -edik komponense a $2i+1$ -edik dimenzió amplitúdója, azaz a jobb oldalon álló állapotvektor $2i+1$ -edik komponense. Ugyanis a 0 sorszámú $|j_0\rangle$ qubit értéke $|1\rangle$.

Most végrehajtjuk a két $FT_{2^{m-1}}$ transzformáció lineáris újra kombinálását. A (26) egyenlőség mutatja hogy

(a) végrehajtjuk az alábbi unitér operációt

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \omega^j \\ 1 & -\omega^j \end{pmatrix}$$

a $(2j, 2j + 1)$ dimenziókon $j = 0, 1, \dots, 2^{m-1}$. Ezután

(b) A visszkapott vektort újra rendezzük. A következő permutációt hajtjuk végre rajta.

$(2j, 2j + 1) \mapsto (j, j + 2^{m-1})$, $j = 0, 1, 2, \dots, 2^{m-1} - 1$.
ennek hatására $\tilde{f}(j)$ a j -edik dimenzió amplitúdója lesz.

Először az (a) lépést tekintjük. Megjegyezzük hogy

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \omega^j \\ 1 & -\omega^j \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \omega^j \end{pmatrix} = H \cdot B_j$$

B_j mátrixa:

$\begin{pmatrix} 1 & 0 \\ 0 & \omega^j \end{pmatrix}$. A B_j műveletet alkalmazzuk a $(2j, 2j + 1)$ -edik dimenziókra! A $2j$ (páros) dimenziót változatlan marad. Az ω^j fázis eltolást alkalmazzuk a $2j + 1$ -edik (páratlan) dimenzióra. Ezt az összes j értékre egyszerre végezzük el a következő módon. A C_p két qubites irányított kvantum kaput alkalmazzuk a 0 sorszámú qubitre és a p sorszámú qubitre minden $p = 1, 2, \dots, m - 1$ esetén. A C_p kapu az $\omega^{2^{p-1}}$ fázis eltolást valósítja meg a p sorszámú qubitre ha mind a 0 sorszámú mind a p sorszámú qubit értéke $|1\rangle$. Tehát mind a 0 sorszámú qubit mind a p sorszámú qubit irányító qubit és a p sorszámú qubit egyúttal cél qubit is. A 0 sorszámú és a p sorszámú qubit standard bázisa felett C_p

mátrixa:

$$C_p = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega^{2^{p-1}} \end{pmatrix}.$$

A C_p művelet $m - 1$ -szeri alkalmazása az ω^j fázis eltolást eredményezi a $2j+1$ -edik (páratlan) dimenzióra, $j = 0, 1, \dots, m-1$. Ugyanis, az a követelmény hogy a nulladik qubit értéke legyen 1, kiválasztja a páratlan pozíciókat. A C_p -ben szereplő $\omega^{2^{p-1}}$ fázis eltolás felépíti az ω^j fáziseltolást egymás után több lépésben – bitenként – a j szám bináris alakjában szereplő minden egyes olyan helyiértékre ahol 1 szám áll. Tekintsük az összes olyan j számot amelynek a bináris alakjában a p -edik helyen 1 áll. (Exponenciálisan sok ilyen j szám van.) Ezek a j számok egyszerre vannak kezelve.

Végül a 0 sorszámú qubitre alkalmazott H Hadamard transzformáció azt eredményezi hogy egyidejűleg alkalmazzuk a H Hadamard transzformációt minden egyes $(2j, 2j + 1)$ alakú párra ahol a fennmaradó $1, \dots, m - 1$ sorszámú qubitek összes lehetséges értékei adják j bináris alakját.

Emlékezzünk hogy a $H \cdot B_j$ mátrix és egy ket vektor szorzását úgy valósítjuk meg hogy először B_j -vel szorozzuk a ket vektort majd H -val. Hiszen bal oldalon van a $H \cdot B_j$ szorzat mátrix és jobb oldalon van a ket vektor.

Tekintsük a (b) lépés megvalósítását! A következő permutációt hajtjuk végre a Hilbert térbeli dimenzió sorszámokon.

$$(2j, 2j + 1) \mapsto (j, j + 2^{m-1}), j = 0, 1, 2, \dots, 2^{m-1} - 1.$$

Azaz

$$2j \mapsto j, j = 0, 1, 2, \dots, 2^{m-1} - 1. \text{ (páros dimenzió sorszámokra)}$$

$$2j+1 \mapsto (j+2^{m-1}), j = 0, 1, 2, \dots, 2^{m-1} - 1. \text{ (páratlan dimenzió sorszámokra)}$$

Ezt a permutációt az alábbi ciklikus permutációval valósítjuk meg. A Hilbert térbeli dimenzió sorszámot ciklikusan permutáljuk a következő módon.

$$i_{m-1}i_{m-2} \dots i_1i_0 \mapsto i_0i_{m-1}i_{m-2} \dots i_1$$

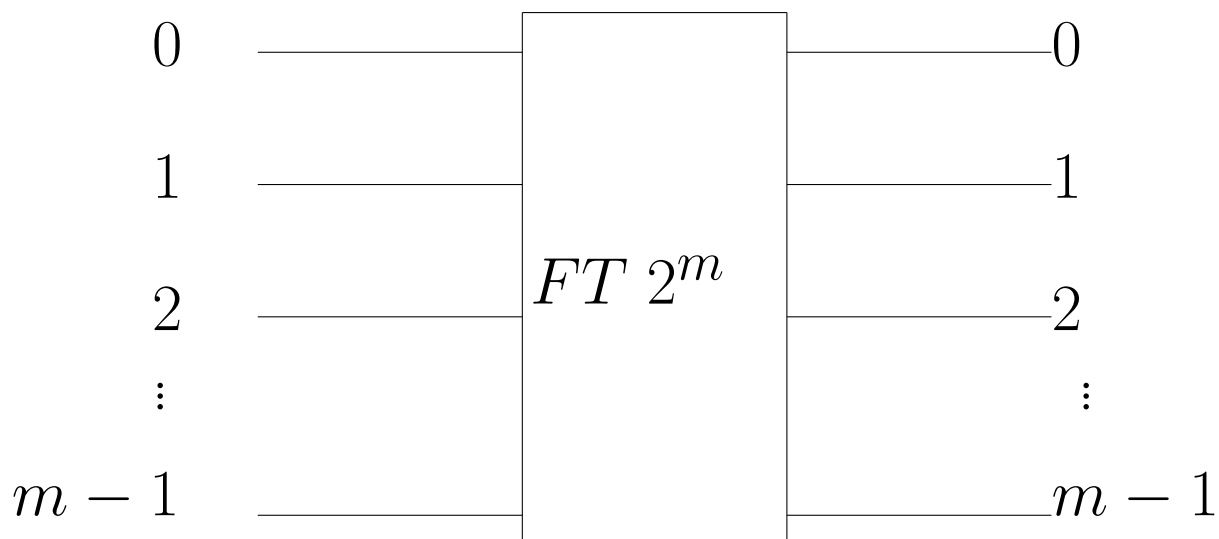
Tehát az $i_{m-1}i_{m-2} \dots i_1i_0$ dimenzió sorszámból $i_0i_{m-1}i_{m-2} \dots i_1$ dimenzió sorszám lesz.

- Ha a dimenzió sorszám páros, (azaz $i_0 = 0$), akkor a fenti permutáció eredményeként a fenti dimenzió sorszám értéke felére csökken.

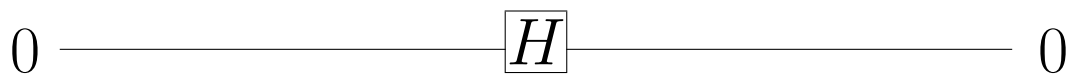
- Ha a dimenzió sorszám páratlan, (azaz $i_0 = 1$), akkor a fenti permutáció eredményeként a fenti dimenzió sorszám értéke a következő módon alakul. Amikor i_0 -t levágjuk a sztring végéről, akkor 0-t írunk a sztring végére. A visszamaradt bináris sztring részlet páros értékű, a jobbra csúsztatás megfelel az értékét és a szó végi 0-t törli. Ezután i_0 a baloldalra kerül, a bináris sztring 2-es számrendszer belüli értéke 2^{m-1} -gyel nő.

A fenti ciklikus permutációt egyszerűen megvalósítjuk: újra rendezzük az output vezetékeket. Lásd az 74. ábrát.

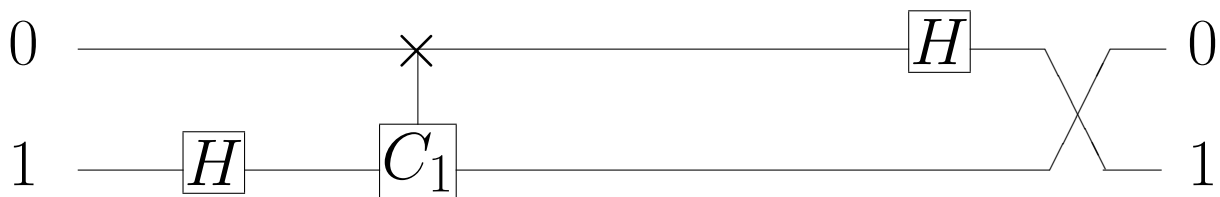
Két qubit cseréjét 3 darab CNOT kapuval valósítjuk meg, lásd 34. ábra. Az összes cserét $3(n - 1)$ darab CNOT kapuval valósítjuk meg.



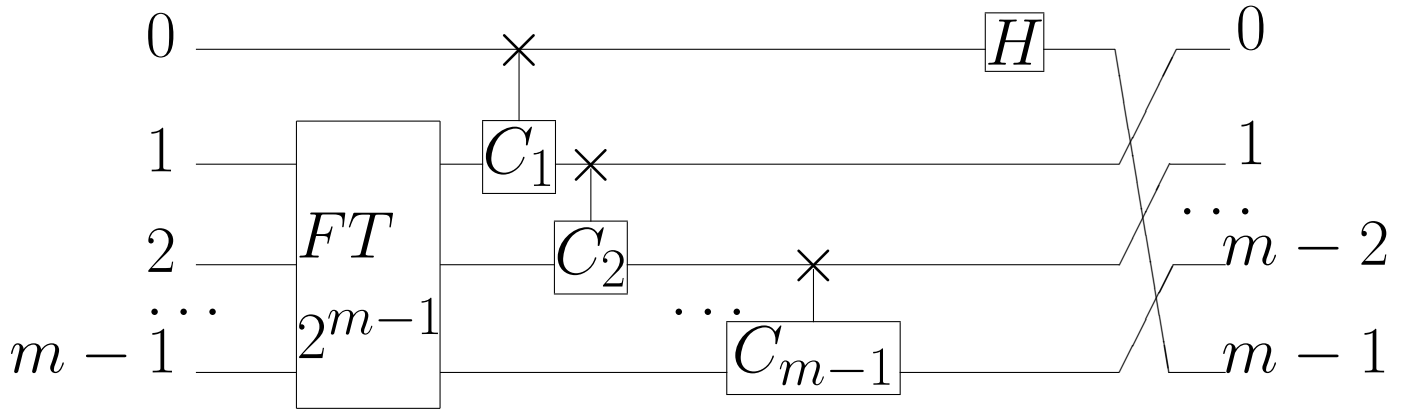
71. ábra. $QFT\ 2^m$



72. ábra. $QFT\ 2$



73. ábra. $QFT\ 4$



74. ábra. $QFT\ 2^m$

A fenti eljárást megismételjük: $FT_{2^{m-1}}$ -et számítjuk ki $FT_{2^{m-2}}$ felhasználásával. És így tovább.

Jelölje $Q(2^m)$ az $FT(2^m)$ transzformációnak a fenti algoritmus-sal való megvalósításnak a művelet számát, $m = 1, 2, 3, \dots$. A fentiek alapján azt kapjuk hogy

$$Q(2^m) = Q(2^{m-1}) + O(m), \quad m \geq 2$$

Ebből azt kapjuk hogy

$$Q(2^n) = O(n^2).$$

Az 74. ábra megmutatja hogyan építhetjük fel az $FT(2^m)$ transzformációt kiszámító kvantum áramkört, ahol $m \geq 0$ tetszőleges természetes szám. $m = 0$ -ra használjuk $FT(1)$ áthelyező mátrixát, lásd (19). A mátrix képletének tanulmányozása alapján kapjuk hogy ez a Hadamard transzformáció áthelyező mátrixa. Ehhez az áthelyező mátrixhoz megkonstruáljuk a kvantum áramkört. Ez a Hadamard kapu.

Tegyük fel hogy már megépítettük az $FT(2^{m-1})$ transzformációt kiszámító kvantum áramkört, ahol $m \geq 1$ tetszőleges természetes szám. Az $FT(2^m)$ transzformációt kiszámító kvantum számítógép

ábráját látjuk az 74. ábrán. A téglalapban van az $FT(2^{m-1})$ transzformációt kiszámító kvantum áramkör.

Állítás 11.10 Legyen $M = 2^m$! A $\mathbf{Z}_M$ monoid feletti kvantum Fourier transzformáció az alábbi unitér operátort valósítja meg:

$$QFT : H_M \rightarrow H_M$$

$$|x\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{y \in \mathbf{Z}_M} \omega^{xy} |y\rangle,$$

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

Bizonyítás. Tudjuk hogy a QFT áthelyező mátrixa:

$$[QFT_{b,c}] = \frac{1}{\sqrt{M}} \omega^{bc} \quad b, c = 0, 1, 2, \dots, 2^m - 1.$$

Lásd (19).

□

12. Shornak a prímtényezős felbontást kiszámoló algoritmus

Definíció 12.1 Legyen $H \subseteq \mathbf{R}$. Az $f : H \rightarrow \mathbf{R}$ függvényt periodikusnak mondjuk, ha létezik olyan $p > 0$ konstans, hogy minden x -re, ahol $x \in \mathbf{R}$, fennáll az $x+p \in H$ eleme reláció és az $f(x) = f(x+p)$ egyenlőség. Ha p a legkisebb olyan szám, amelyre ez teljesül, akkor a p konstans az f függvény periódusának nevezzük.

Ha a periodikus függvény képét p hosszú vektorral eltoljuk, akkor a függvény képe önmagába megy át.

Egy periodikus függvényt elég a periódusának megfelelő intervallummal vizsgálni. Egy ilyen vizsgálatból a függvény minden

jellemzőét megállapíthatjuk.

Shornak a prímtényezős felbontást kiszámoló algoritmusa

Input: egy N természetes szám.

Output: az N természetes számnak egy valódi osztója.

Műveletek száma: $O((\log N)^3)$

Vázlatos áttekintés:

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

Ez az algoritmus felhasználja

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

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

Definíció 12.2 Legyenek N és p pozitív egész számok. Azt mondjuk hogy p valódi osztója az N számnak ha

1. $N = pq$ valamely q pozitív egész számra,
2. $p \neq 1$, és
3. $p \neq N$.

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

Definíció 12.3 Legyenek N és q relatív prím természetes számok. A q szám modulo N multiplikatív rendje az a legkisebb k pozitív egész szám amelyre

$$q^k \equiv 1 \pmod{N}.$$

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

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

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

$$\text{Tehát } 11^2 \equiv 16 \pmod{21}.$$

$$k = 3: 11^3 = 11 \times 11^2,$$

$$11 \times 16 \pmod{21} = 176 \pmod{21} = 8.$$

$$\text{Tehát } 11^3 \equiv 8 \pmod{21}.$$

$$k = 4: 11^4 = 11 \times 11^3 \equiv 11 \times 8 \pmod{21} = 88 \pmod{21} = 4.$$

$$\text{Tehát } 11^4 \equiv 4 \pmod{21}.$$

$$k = 5: 11^5 = 11 \times 11^4 \equiv 11 \times 4 \pmod{21} = 44 \pmod{21} = 2.$$

$$\text{Tehát } 11^5 \equiv 2 \pmod{21}.$$

$$k = 6: 11^6 = 11 \times 11^5 \equiv 11 \times 2 \pmod{21} = 22 \pmod{21} = 1.$$

$$\text{Tehát } 11^6 \equiv 1 \pmod{21}.$$

Tehát a 11 szám modulo 21 multiplikatív rendje 6.

Sok számolást igényel q^k kiszámítása amikor k sok értéket vesz fel.

Vegyük észre hogy k -nal csupán bizonyos értékeire kell kiszámolnunk q^k -t. Valóban írjuk fel k 2-es számrendszerbeli alakját:

$$k = k_{m-1}2^{m-1} + k_{m-2}2^{m-2} + \dots + k_12^1 + k_0$$

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

$$q^k = q^{k_{m-1}2^{m-1}} \times q^{k_{m-2}2^{m-2}} \times \dots \times q^{k_12^1} \times q^{k_0}$$

Ahhoz hogy kiszámítsuk q^k -t szükségünk van a $q^{2^1}, q^{2^2}, \dots, q^{2^{m-1}}$

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

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

Eképpen

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

Megmutatjuk hogy az N szám egy valódi osztójának a keresése visszavezethető valamely q szám modulo N multiplikatív rendjének a kiszámítására. Itt a q számot

véletlenszerűen választjuk ki az $\{2, \dots, N-1\}$ halmazból. A q szám modulo N multiplikatív rendjének a segítségével keresünk egy r pozitív egész számot úgy hogy

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

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

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

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

Például amikor $N = 21$, akkor az $r = 8$ értékválasztás megfelelő.

1. és 2. feltételek teljesülnek. $r^2 - 1 = 63 = 3 \times 21$. Figyeljük meg hogy $r - 1 = 7$ valódi osztója $N = 21$ -nek.

Valódi osztót kiszámoló algoritmus

1. lépés: Ha N páros akkor visszaadjuk $p = 2$ -t.
2. lépés: ha N prím szám akkor visszaadjuk N -t, lásd Állítás 17.2.
3. lépés: Egyenletes eloszlással véletlenszerűen válasszunk ki egy q számot, $2 \leq q \leq N - 1$. Ha $p = \text{lnko}(q, N) > 1$ akkor adjuk vissza a p számot. Különben menjünk a 4. lépésre.
4. lépés: Számoljuk ki a q szám modulo N multiplikatív rendjét. Legyen k a q szám modulo N multiplikatív rendje! Ha k nem páros, akkor menjünk a 3. lépésre.
5. lépés: Legyen $k = 2m$ alakú. Legyen $r = (q^m \bmod N)$. Most $1 \leq r < N$. Határozzuk meg az r számot. Ha $1 < p = \text{lnko}(r - 1, N) < N$, akkor adjuk vissza a p számot. Ha $1 < p = \text{lnko}(r + 1, N) < N$, akkor adjuk vissza a p számot. Különben (ha nem találtunk N -nek valódi osztóját akkor) menjünk a 3. lépésre.

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

A q szám modulo N multiplikatív rendjének definíciója és az r szám definíciója alapján N nem osztója az $r - 1$ számnak. Viszont N osztója lehet az $r + 1$ számnak. Így előfordulhat hogy $1 = \text{lnko}(r - 1, N)$ és $\text{lnko}(r + 1, N) = N$. Ez 'pech', mert így nem kapunk N -nek valódi osztóját. Ha 'szerencsénk van', akkor

k páros és N nem osztója az $r + 1$ számnak. Ekkor azt kapjuk hogy

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

Mennyi annak a valószínűsége hogy 'szerencsénk van'? Legalább $\frac{1}{2}$. A [8] könyv 63. oldalán található Corollary 4.2.1 mondja ki az alábbi állítást.

Állítás 12.4 Legyen N páratlan szám és ne legyen prímszám. Egyenletes eloszlással véletlenszerűen válasszunk ki egy q számot, $2 \leq q \leq N - 1$. Legalább $\frac{1}{2}$ annak a valószínűsége hogy a fentiekben kiszámolt k szám páros és N nem osztója az $r + 1$ számnak.

Legyenek N és q pozitív egész számok! Tekintsük az

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

függvényt!

Állítás 12.5 Legyenek N és q relatív prím természetes számok.

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

A fenti állítás tükrében meghatározzuk az

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

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

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

Állítás 12.6 Létezik hagyományos eljárás amely kiszámítja adott x helyen az

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

függvény értéket $poly(\log N)$ időben.

Bizonyítás. x bináris alakját tekintjük. Vegyük észre, hogy $q^{2^i} \cdot q^{2^i} = q^{2^{i+1}}$. Ezért kiszámítjuk a

$$q^{2^i} \bmod N \quad i = 1, 2, \dots$$

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

□

13. Adott függvény periódusának a kiszámítása felhasználva a kvantum Fourier transzformációt

$\mathbf{Z}_N$ jelöli az egészek mod N additív Ábel csoportját.

Feladat. Adott egy N egész szám és egy $f : \{ 0, 1, 2, \dots, \} \rightarrow \{ 0, 1, 2, \dots, \}$ leképezés úgy hogy

1. létezik egy $a \leq N$ periódusa f -nek, és
2. minden $x, y \in \mathbf{Z}$ esetén, $f(x) = f(y)$ akkor és csak akkor ha $x - y$ többszöröse az a periódusnak.

A fenti feltételek mellett találjuk meg az a természetes számot!

Megjegyezzük hogy a 2. feltétel szerint a $\{ 0, 1, 2, \dots, \}$ értelmezési tartomány tetszőleges a periódus hosszú intervallumán

(szakaszán) az f függvény injektív.

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

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

Most kettő esetet különböztetünk meg.

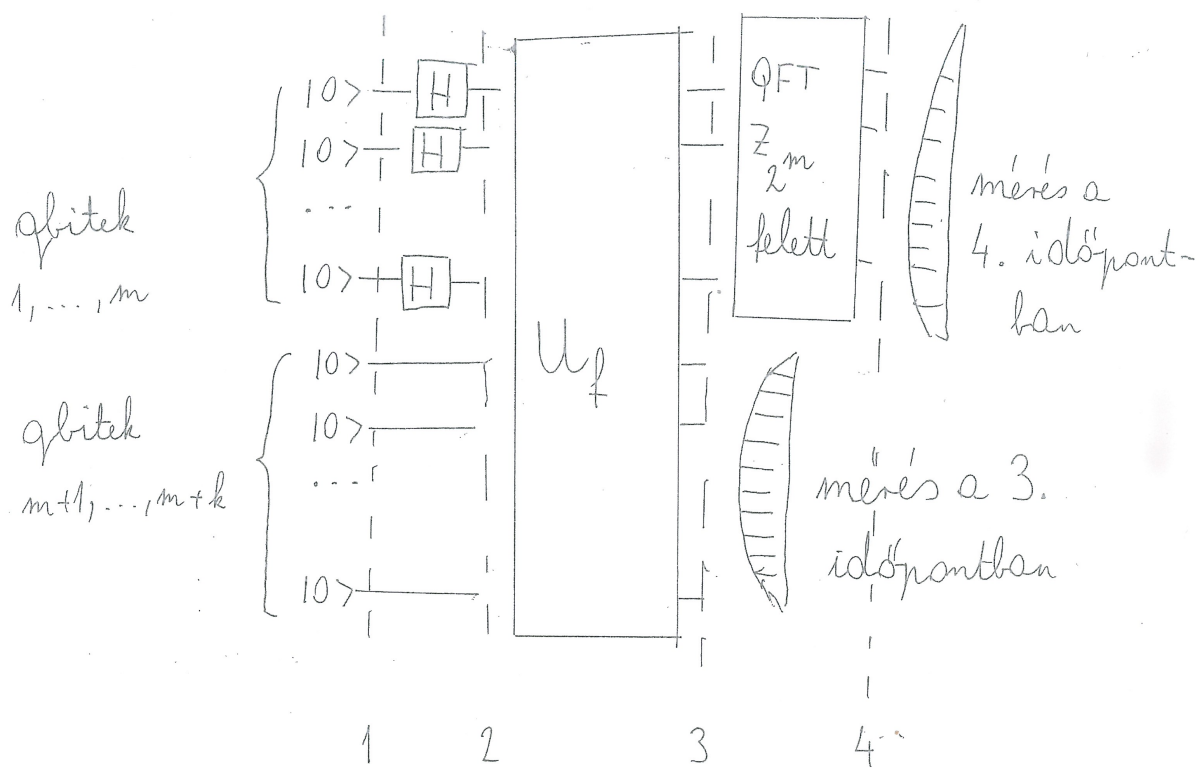
Első eset: az a periódus osztója az M számnak. (Ennek igen kicsi a valószínűsége. Hiszen ekkor a a 2 szám hatványa.) Tekintsük a 75 ábrán látható quantum áramkört!

Először tekintsük az első m qubitet!

$$\begin{aligned} & (H \otimes H \otimes H \otimes \dots \otimes H)(|0\rangle|0\rangle|0\rangle \dots |0\rangle) = \\ & \frac{1}{2^{\frac{m}{2}}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) = \\ & \frac{1}{2^{\frac{m}{2}}} \left(\sum_{x=0}^{2^m-1} |x\rangle \right). \end{aligned}$$

Adjunk k qubites regisztert (azaz k qubitet) a kvantum áramkörhöz. Mindegyik hozzáadott qubit a $|0\rangle$ állapotban van. Tehát az áramkör 2. pontján az első m qubit (az első regiszter) $\mathbf{Z}_M$ összes elemének egyenlő együtthatóval vett lineáris kombinációja: $\frac{1}{2^{\frac{m}{2}}} \sum_{x=0}^{2^m-1} |x\mathbf{0}\rangle$.

Tegyük fel hogy az U_f áramkör számítja ki az f függvényt, és az eredményt a második regiszterben kapjuk meg. Az első m



75. ábra. Az f függvény periódusának a kiszámítása kvantum áramkörrel

input qubit értéke közvetlenül az outputra kerül (azaz az első m output qubitbe).

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

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

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

valamely véletlen $x \in \mathbf{Z}_M$ esetén. Ugyanis

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

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

Az első m input qubit állapotvektora a 3. időpontban:

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

Az $\sqrt{\frac{a}{M}}$ szorzótényezőt hogyan kapjuk? Képezzük a

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

vektor önmagával vett belső szorzatát (a normáját). Az eredmény: $\frac{M}{a}$. Idézzük fel hogy a kvantum állapotot egy olyan $\mathcal{H}_M$ Hilbert térbeli vektorral ábrázoljuk aminek a normája 1.

Emlékezzünk az alábbi állításra, lásd (20), (24):

Állítás 13.1 Legyen $M = 2^m$! A $\mathbf{Z}_M$ monoid feletti kvantum Fourier transzformáció az alábbi unitér operátort valósítja meg:

$$QFT : H_M \rightarrow H_M$$

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

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

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

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

A QFT átttranszformálja az első m qubitet a

$$\frac{\sqrt{a}}{M} \sum_{j=0}^{\frac{M}{a}-1} \left(\sum_{y \in \mathbf{Z}_M} \omega^{(x+ja)y} \right) |y\rangle = \quad (28)$$

$$\frac{\sqrt{a}}{M} \sum_{y \in \mathbf{Z}_M} \left(\sum_{j=0}^{\frac{M}{a}-1} \omega^{(x+ja)y} \right) |y\rangle = \frac{\sqrt{a}}{M} \sum_{y \in \mathbf{Z}_M} \omega^{xy} \left(\sum_{j=0}^{\frac{M}{a}-1} \omega^{jay} \right) |y\rangle \quad (29)$$

állapotba valamely $x \in \mathbf{Z}_M$ véletlen számra. Az első formula felírásakor felhasználtuk hogy a QFT lineáris leképezést valósít meg ezért a QFT a

$$\sum_{j=0}^{\frac{M}{a}-1}$$

összegzés mögé bevihető. Vizsgáljuk meg az $|y\rangle$ bázis állapotok ($y \in \mathbf{Z}_M$) együtthatóit! Mivel M többszöröse a -nek, azt kapjuk hogy ha $\omega^{ay} \neq 1$ azaz ha $y \notin \{0, \frac{M}{a}, \frac{2M}{a}, \dots, \frac{(a-1)M}{a}\}$, akkor

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

Ebből azt kapjuk hogy a (29) egyenlőségben azon $|y\rangle$ bázis állapotok együtthatói (valószínűségi amplitúdói) ahol y nem többszöröse $\frac{M}{a}$ -nek egyenlőek 0-val.

Mivel M többszöröse a -nek, azt kapjuk hogy ha $\omega^{ay} = 1$ azaz ha

$y \in \{0, \frac{M}{a}, \frac{2M}{a}, \dots, \frac{(a-1)M}{a}\}$, akkor

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

Ezért a (29) egyenlőségben szereplő állapot az

$$\left\{ |0\rangle, \left|\frac{M}{a}\right\rangle, \dots, \left|(a-1)\frac{M}{a}\right\rangle \right\}$$

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

Az így kapott állapotot megmérjük. Eképpen a mérés véletlenszerűen egyenletes eloszlással adja az

$|y\rangle = |c\frac{M}{a}\rangle$ állapotot, ahol $0 \leq c \leq (a - 1)$.

A kapott

$|y\rangle = |c\frac{M}{a}\rangle$ állapot címkéje $y = c\frac{M}{a}$,

továbbá $0 \leq c \leq (a - 1)$ véletlenszerűen egyenletes eloszlással.

Tehát

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

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

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

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

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

Mennyi a valószínűsége annak hogy $lnko(c, a) = 1$? A számelmélet szerint nagy a számra az a -nél kisebb egyenlő, a -hez relatív prím számok száma megközelítőleg:

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

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

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

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

$$|y\rangle = |c \frac{M}{a}\rangle \text{ állapototra teljesül hogy } \ln ko(c, a) = 1$$

és így sikerül meghatározni az a számot.

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

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

Tekintsünk a $\frac{c}{a}$ -tól különböző $\frac{u}{v}$ törtet amelyek nevezője legfeljebb N . Mivel $\frac{c}{a}$ nevezője is legfeljebb N , a két tört különbségének a kiszámításához kiszámolt közös nevező legfeljebb N^2 . Ezért a két tört különbségének az abszolút értéke legalább $\frac{1}{N^2} > \frac{1}{M}$. Ezért

$$|\frac{y}{M} - \frac{u}{v}| > \frac{1}{2M}.$$

Így $\frac{c}{a}$ az az egyértelműen meghatározott tört amelynek a nevezője legfeljebb N és $\frac{y}{M}$ -től vett távolsága (a különbség abszolútértéke) kisebb mint $\frac{1}{2M}$. A $\frac{c}{a}$ szám értékét meg tudjuk határozni polinom időben, úgy hogy az $\frac{y}{M}$ törtet lánc törttel közelítjük. Ismét tegyük

fel hogy $\text{lnko}(c, a) = 1$! Most ki tudjuk számolni a értékét. Ha $\text{lnko}(c, a) \neq 1$, akkor lásd az első esetet.

Az első esethez hasonlóan kapjuk az alábbiakat. Tekintsünk tetszőleges 1-hez közeli p valószínűséget. A fenti eljárást $O(\log \log N)$ -szer elvégezve, p -nél nagyobb a valószínűsége annak hogy a fenti módon véletlenszerűen kapott $|y\rangle = |c \frac{M}{a}\rangle$ állapotra teljesül hogy $\text{lnko}(c, a) = 1$ és így sikerül meghatározni az a számot.

13.1. Fázis megbecsülése Simon algoritmusával

Az $\oplus$ műveletet bináris n -esekre terjesztjük ki: bitenként végezzük el. Például: $01010 \oplus 11100 = 10110$.

Simon az alábbi módon fogalmazta újra a fázis megbecsülésének a problémáját.

Adott egy

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^m, m \geq n$$

függvény. Az f függvény bináris n -eseket képez bináris m -esekbe.

Tudjuk hogy

(a) f injektív vagy

(b) létezik egy nemtriviális (azaz a nulla vektortól különböző) $s \in \{0, 1\}^n$ úgy hogy minden $x \neq x'$ esetén, $f(x) = f(x')$ akkor és csak akkor ha $x' = x \oplus s$.

Szemléletesen: ha egy elemnek van őse, akkor őt képelemnek hívjuk. Vagy minden egyes képelemnek egy őse van vagy minden egyes képelemnek két őse van.

El akarjuk dönteni hogy (a) és (b) közül melyik igaz. Ha (b) igaz, akkor meg akarjuk határozni s értékét.

Példa. legyen $n = m = 3$. Az alábbi függvény kielégíti a (b) feltételt.

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

Itt $s = 110$.

Hagyományos számítógéppel az alábbi módon járunk el. Tekintsünk egy f függvényt amelyet egy fekete doboz számol ki. A fekete doboz által kiszámított értékeket megvizsgálhatjuk, de a fekete doboz programjának a kódját nem. Meg akarjuk határozni az $f(x)$ függvény s fázisát. Ez egy orákulum probléma. A megoldás menete: Minden $s \in \{0, 1\}^n$ szóra (s különbözik a nulla vektortól), minden $x \in \{0, 1\}^n$ szóra, az orákulumnak odaadjuk az x és s szavakat. Az orákulum visszaadja az $f(x)$ és $f(x + s)$ szavakat. Mi összehasonlítjuk őket, azaz megnézzük hogy $f(x) = f(x + s)$ teljesül-e. Ezt addig folytatjuk amíg megállapítjuk hogy (a) igaz, vagy megállapítjuk hogy (b) igaz és megkapjuk az s értékét. Hagyományos számítógéppel expo-

nenciális időt igényel a számolás.

Tekintsük az alábbi eljárást: A probléma megoldásához két regisztert használunk fel. Az első regiszter n darab qubitből áll, a második regiszter m darab qubitből áll. Mindkét regiszter kezdő értéke n darab $|0\rangle$ qubit.

1. lépés: Alkalmazzuk a QFT-t az első regiszterre. A kapott eredmény:

$$2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} |x, \mathbf{0}\rangle.$$

2. lépés: Számítsuk ki $f(x)$ -et a második regiszterben U_f alkalmazásával. Így kapjuk a

$$2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$$

kvantum állapotot.

3. lépés: Alkalmazzuk a Hadamard transzformációt az első regiszterre. Így kapjuk a

$$2^{-n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y, f(x)\rangle$$

kvantum állapotot. Ebben a kifejezésben $x = (x_0 \ x_1 \ \dots, \ x_{n-1})$ és $y = (y_0 \ y_1 \ \dots, \ y_{n-1})$ n hosszú bináris sztringek és

$$x \cdot y = x_0 y_0 + x_1 y_1 + \dots + x_{n-2} y_{n-2} + x_{n-1} y_{n-1}.$$

4. lépés: Megmérjük a

$$2^{-n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y, f(x)\rangle$$

kvantum állapotot. Az $|(y, f(x))\rangle$ állapotot kapjuk eredményül. valamely $x \in \{0, 1\}^n$ és $y \in \{0, 1\}^n$ -re.

$n - 1$ -szer hajtjuk végre a fenti számolási lépéseket.

Ekkor kapjuk a $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ értékeket. Keresünk egy ismeretlen s^* sztringet úgy hogy minden egyes $i = 1, 2, \dots, n$ -re az $y^{(i)}$ értéknek a skalár szorzata az ismeretlen s^* sztringgel páros számot ad. Ezért egy (ER) lineáris egyenletrendszert írunk fel. Az (ER) lineáris egyenletrendszer az alábbi alakú egyenletekből áll:

$$y^{(i)} \cdot s^* = y_0^{(i)} s_0^* + y_1^{(i)} s_1^* + \dots + y_{n-2}^{(i)} s_{n-2}^* + y_{n-1}^{(i)} s_{n-1}^* \equiv 0 \pmod{2},$$

$$i = 1, 2, \dots, n.$$

Tehát az alábbi (ER) lineáris egyenletrendszert kapjuk:

$$y^{(1)} \cdot s^* \equiv 0 \pmod{2}$$

$$y^{(2)} \cdot s^* \equiv 0 \pmod{2}$$

...

$$y^{(n)} \cdot s^* \equiv 0 \pmod{2}$$

Tekintsük a $\mathbf{Z}_2 = (\{0, 1\}, \oplus, 0, \cdot, 1)$ testet. A fenti (ER) lineáris egyenletrendszert természetes módon tekinthetjük a $\mathbf{Z}_2$ test feletti lineáris egyenletrendszernek. (Az egyes egyenleteket a következő módon alakítjuk át. A jobb oldalra 0-t írunk. Az összeadás helyébe az $\oplus$ műveletet helyettesítjük.) Ezért a továbbiakban az (ER) lineáris egyenletrendszert egy $\mathbf{Z}_2$ feletti lineáris egyenletrendszernek tekintjük. Az (ER) lineáris egyenletrendszert megoldjuk $\mathbf{Z}_2$ felett, és így megkapjuk s^* értékét. A valós számok feletti lineáris egyenletrendszerek megoldásához hasonlóan járunk el.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ lineárisan függetlenek akkor megold-

juk az (ER) lineáris egyenletrendszert és megkapjuk az (ER) lineáris egyenletrendszer nemtriviális (nullavektortól különböző) s^* megoldását. Most az (a) és (b) esetet a következő módon különböztetjük meg: Kiszámoljuk az $f(\mathbf{0})$ és $f(s^*)$ értékeket. Ha $f(\mathbf{0}) \neq f(s^*)$, akkor (a) teljesül. Ha $f(\mathbf{0}) = f(s^*)$, akkor (b) teljesül, és s megegyezik az s^* megoldással.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ nem lineárisan függetlenek, akkor megismételjük az egész eljárást.

Magyarázat

Állítás 13.2 Az $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ vektorok lineárisan függetlenek akkor és csak akkor ha létezik pontosan egy nemtriviális (nullavektortól különböző) s^* megoldása a fenti egyenletrendszernek.

Állítás 13.3 Legyen u tetszőleges n hosszúságú, nulla vektortól különböző vektor. Válasszunk véletlenül n darab n hosszúságú $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ vektort úgy hogy

$$u \cdot y_i \equiv 0 \pmod{2}, i = 1, 2, \dots, n.$$

Ekkor legalább $\frac{1}{4}$ a valószínűsége annak hogy az $y_1, y_2, \dots, y_n$ vektorok lineárisan függetlenek.

A 13.3 állítás alapján elegendő $O(n)$ -szer végrehajtani az 1, 2, 3 és 4 lépéseket.

Először tegyük fel hogy (b) teljesül. Most létezik egy nemtriviális (azaz a nulla vektortól különböző) $s \in \{0, 1\}^n$ úgy hogy minden $x \neq x'$ esetén, $f(x) = f(x')$ akkor és csak akkor ha $x' = x \oplus s$. Minden y, x párra, az $|yf(x)\rangle$ és $|yf(x \oplus s)\rangle$ egyenlőek egymással.

Ennek az állapotnak az amplitúdóját jelöljük $\alpha(x, y)$ -nal! Most kiszámoljuk az $\alpha(x, y)$ amplitúdót.

Figyeljük meg hogy ha $y \cdot s \equiv 0 \pmod{2}$ akkor

$$(x \oplus s) \cdot y \pmod{2} = (x \cdot y) \oplus (s \cdot y) \pmod{2} = (x \cdot y) \pmod{2}.$$

Fordítva, ha $(x \oplus s) \cdot y \pmod{2} = (x \cdot y) \pmod{2}$, akkor $y \cdot s \equiv 0 \pmod{2}$.

A fenti összefüggés alapján két esetet különböztetünk meg.

Ha $y \cdot s \equiv 0 \pmod{2}$ azaz $(x \oplus s) \cdot y \equiv x \cdot y \pmod{2}$ akkor

$$\alpha(x, y) = 2^{-n}((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) = 2^{-n+1}(-1)^{x \cdot y} \neq 0.$$

Ha $y \cdot s \not\equiv 0 \pmod{2}$ azaz $(x \oplus s) \cdot y \not\equiv x \cdot y \pmod{2}$ akkor

$$\alpha(x, y) = 2^{-n}((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) = 0.$$

Tegyük fel hogy n -szer hajtjuk végre az 1, 2, 3 és 4 lépéseket. Ekkor kapjuk a $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ értékeket. A (b) feltételben definiált számunkra ismeretlen $s \in \{0, 1\}^n$ sztringre teljesül hogy minden egyes $i = 1, 2, \dots, n$ -re az $y^{(i)}$ értéknek a skalár szorzata az s sztringgel páros számot ad. Tehát s kielégíti az (ER) lineáris egyenletrendszert.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ lineárisan függetlenek, akkor felírjuk az (ER) lineáris egyenletrendszert. Az egyenletrendszert megoldjuk meg $\mathbf{Z}_2$ felett, és így megkapjuk az s^* megoldás értékét. Most s megegyezik az s^* megoldással. Ezért $f(\mathbf{0}) = f(s) = f(s^*)$. Kiszámoljuk az $f(\mathbf{0})$ és $f(s^*)$ értékeket. A fentiek alapján $f(\mathbf{0}) = f(s^*)$.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ nem lineárisan függetlenek, akkor megismétljük az egész eljárást.

Másodszor tegyük fel hogy (a) teljesül, azaz f injektív. n -

szer végrehajtjuk az 1, 2, 3 és 4 lépéseket. Ekkor kapjuk a $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ értékeket.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ lineárisan függetlenek, akkor felírjuk az (ER) lineáris egyenletrendszert. Az egyenletrendszert megoldjuk meg $\mathbf{Z}_2$ felett, és így megkapjuk az s^* megoldás értékét. Kiszámoljuk az $f(\mathbf{0})$ és $f(s^*)$ értékeket. Mivel f injektív, $f(\mathbf{0}) \neq f(s^*)$.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ nem lineárisan függetlenek, akkor megismételjük az egész eljárást.

Tehát az (a) és (b) esetet a következő módon különböztetjük meg: n -szer végrehajtjuk az 1, 2, 3 és 4 lépéseket. Ekkor kapjuk a $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ értékeket.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ lineárisan függetlenek, akkor felírjuk az (ER) lineáris egyenletrendszert. Az egyenletrendszert megoldjuk meg $\mathbf{Z}_2$ felett, és így megkapjuk az s^* megoldás értékét. Kiszámoljuk az $f(\mathbf{0})$ és $f(s^*)$ értékeket. Ha $f(\mathbf{0}) \neq f(s^*)$, akkor (a) teljesül. Ha $f(\mathbf{0}) = f(s^*)$, akkor (b) teljesül. Most s megegyezik az s^* megoldással.

- Ha $y^{(1)}, y^{(2)}, \dots, y^{(n)}$ nem lineárisan függetlenek, akkor megismételjük az egész eljárást.

A 13.3 állítás alapján igazolható a következő.

Állítás 13.4 A fenti eljárás végrehajtása várhatóan $O(nt(n) + g(n))$ idő alatt történik meg. Itt a $t(n)$ és $g(n)$ jelentése a következő. Az f függvénynek tetszőleges n hosszú inputon való kiszámolásához $t(n)$ idő szükséges. Továbbá tetszőleges n egyenletből álló $\mathbf{Z}_2$ feletti egyenletrendszer megoldásához $g(n)$ idő szükséges.

séges.

14. A diszkrét logaritmus kiértékelési probléma

Legyen p egy prímszám!

Tetszőleges $m \geq 2$ egész esetén az egész számok $\mathbb{Z}$ halmaza m diszjunkt osztály uniójára bomlik fel, mégpedig úgy, hogy $0 \leq i < m$ esetén az i -dik osztályban $k \cdot m + i$ alakú számok vannak, ahol k végigfut az egészeken (más szóval, az i -dik osztályba az m -mel osztva i maradékot adó számok tartoznak). Ezeket az osztályokat m szerinti, vagy másképpen modulo m (rövid jelölése: $\text{mod } m$) maradékosztályoknak nevezzük. A maradékosztályok jelentősége az, hogy ha két szám azonos maradékosztályba esik (modulo m), akkor kongruensek egymással modulo m , ha pedig különböző maradékosztályból valók, akkor nem kongruensek.

Egy *modulom* maradékosztályból kiválasztott tetszőleges a elemet a maradékosztály reprezentáns elemének nevezzük, s azt mondjuk, hogy a reprezentálja a maradékosztályt.

$\mathbb{Z}_{p-1}$ jelöli az egész számok modulo $p - 1$ additív csoportját. Azaz a tartóhalmaz a

$$\{ [0]_{\equiv \text{mod } p-1}, [1]_{\equiv \text{mod } p-1}, \dots, [p-2]_{\equiv \text{mod } p-1} \}.$$

$\mathbb{Z}_p^*$ jelöli az $\{ 1, 2, \dots, p-1 \}$ multiplikatív csoportot, ahol a csoport művelet a szorzás modulo p , és 1 az egységelem. $\mathbb{Z}_{p-1}^*$ -ban a multiplikatív inverzet hatékonyan ki tudjuk számítani a kiterjesztett Euklidész algoritmussal. Igazoljuk hogy $\mathbb{Z}_p^*$ valóban csoport! Ehhez azt látjuk be hogy minden elemnek van inverze. Te-

kintsünk egy $x \in \{1, 2, \dots, p-1\}$ elemet. Mivel $\ln ko(x, p) = 1$, léteznek a, b egész számok úgy hogy

$$ax + bp = 1.$$

Azaz

$$ax \equiv 1 \pmod{p}$$

Tehát $(a \pmod{p})$ az inverze x -nek a $\mathbf{Z}_p^*$ csoportban.

Példa Legyen $p = 5$. $\mathbf{Z}_5^*$ jelöli az $\{1, 2, 3, 4\}$ multiplikatív csoportot, ahol a csoport művelet a szorzás modulo 5, és 1 az egységelem. Példa szorzások:

$$2 \cdot 2 = 4, 2 \cdot 3 = 1, 2 \cdot 4 = 3, 3 \cdot 3 = 4, 4 \cdot 2 = 3, 4 \cdot 3 = 2.$$

1-nek 1 az inverze, 2-nek 3 az inverze, 3-nak 2 az inverze, 4-nek 4 az inverze.

Definíció 14.1 Azt mondjuk hogy $q \in \mathbf{Z}_p^*$ a csoport generátora ha q (a csoport szorzásra nézve vett) hatványai a csoport összes elemét generálják:

$$\mathbf{Z}_p^* = \{q^0, q^1, q^2, \dots, q^{p-2}\}, q^0 = 1.$$

Eképpen minden $x \in \mathbf{Z}_p^*$ elem az alábbi alakban írható fel:

$$x = q^y \text{ ahol } y \in \mathbf{Z}_{p-1}.$$

Ekkor azt mondjuk hogy y az x diszkrét logaritmusa a p bázis felett és azt írjuk hogy

$$y = \log_p x.$$

Példa folytatása 2 a $\mathbf{Z}_5^*$ csoport generátora, mert $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$.

$$\log_5 1 = 0, \log_5 2 = 1, \log_5 4 = 2, \log_5 3 = 3.$$

$$\text{Ha } x_1 = q^{y_1} \text{ és } x_2 = q^{y_2} \text{ akkor } x_1 x_2 = q^{y_1 + y_2}.$$

Tehát ha $y_1 = \log_p x_1$ és $y_2 = \log_p x_2$, akkor $y_1 + y_2 = \log_p x_1 x_2$.

Feladat. Adott a p prímszám és a $\mathbf{Z}_p^*$ csoport q generátora. Legyen $x \in \mathbf{Z}_p^*$ tetszőleges. Számoljuk ki az $y = \log_p x$ számot.

A feladat megoldásához bevezetünk egy f függvényt és a feladatot úgy fogalmazzuk újra hogy az f függvény periódusát keressük.

Ha $x_1 = q^{y_1}$ és $x_2 = q^{y_2}$, akkor $x_1 x_2 = q^{y_1 + y_2}$. Ezért ha $\log_p(x_1) = y_1$ és $\log_p(x_2) = y_2$, akkor $\log_p(x_1 x_2) = y_1 + y_2$.

A fentiek alapján a q generátor segítségével a $\mathbf{Z}_{p-1}$ additív csoporttal reprezentáljuk a $\mathbf{Z}_p^*$ multiplikatív csoportot. Itt

$[0]_{\equiv \text{ mod } p-1}, [1]_{\equiv \text{ mod } p-1}, \dots, [p-2]_{\equiv \text{ mod } p-1}$
reprezentálja rendre a $1 = q^0, q^1, q^2, \dots, q^{p-2}$ elemeket.

Azaz a $\tau : \mathbf{Z}_{p-1} \rightarrow \mathbf{Z}_p^*, \tau([i]_{\equiv \text{ mod } p-1}) = q^i$ leképezés izomorfizmus (bijektív homomorfizmus).

Legyen a p prímszám és a q generátor adottak, és legyen $x \in \mathbf{Z}_{p-1}$ adott! Tekintsük az $f : \mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1} \rightarrow \mathbf{Z}_p^*$ leképezést, ahol minden $a, b \in \mathbf{Z}_{p-1}$ esetén,

$$f(a, b) = q^a x^{-b} \text{ mod } p.$$

Ha $y = \log_p(x)$, akkor $x = q^y$ és

$$f(a, b) = q^a x^{-b} \text{ mod } p = q^a (q^y)^{-b} \text{ mod } p = q^{a-yb} \text{ mod } p.$$

Itt a kitevőben $\mathbf{Z}_{p-1}$ -beli elemek vannak amiken $\mathbf{Z}_{p-1}$ -beli műveleteket végzünk el. Például yb egy olyan összeg aminek minden tagja y és b darab tagja van. Ebből az következik hogy

$$f(a_1, b_1) = q^{a_1 - yb_1} \text{ mod } p,$$

$$f(a_2, b_2) = q^{a_2 - yb_2} \text{ mod } p,$$

és

$$f(y, 1) \equiv q^{y-y} = 1 \text{ mod } p.$$

Igazoljuk az alábbi állítást!

Állítás 14.2 (i) $f(a_1, b_1) = f(a_2, b_2)$ akkor és csak akkor ha $(a_2, b_2) = (a_1, b_1) + \lambda \cdot (y, 1)$ valamely $\lambda \in \mathbf{Z}_{p-1}$ -re.
(ii) Az $(y, 1)$ az f függvény periódusa a $\mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1}$ halmazon.

Bizonyítás. Igazoljuk (i)-t! Tegyük fel hogy $(a_2, b_2) = (a_1, b_1) + \lambda(y, 1)$ valamely $\lambda \in \mathbf{Z}_{p-1}$ -re. Ekkor $a_2 = a_1 + \lambda y$ és $b_2 = b_1 + \lambda$.
 $f(a_2, b_2) = q^{a_1 + \lambda y - y(b_1 + \lambda)} = q^{a_1 - y b_1} = f(a_1, b_1)$.

Fordítva, tegyük fel hogy $f(a_1, b_1) = f(a_2, b_2)$. Ekkor, mivel $a_1 - y b_1$ $a_2 - y b_2$ – a két kitevő – $\mathbf{Z}_{p-1}$ eleme és q a $\mathbf{Z}_p^*$ csoport generátora, a két kitevő egyenlő egymással: $a_1 - y b_1 = a_2 - y b_2$. Tehát $a_2 - a_1 = y(b_2 - b_1)$. Legyen $\lambda \in \mathbf{Z}_{p-1}$ úgy hogy $b_2 = \lambda + b_1$! Ekkor $(a_2, b_2) = (a_1, b_1) + \lambda(y, 1)$

(ii) következik (i)-ből.

□

A $\mathcal{H}_{(p-1) \times (p-1)}$ Hilbert tér ortonormális bázisvektorait pozitív egészekből álló rendezett párok jelölik egész számok helyett, azaz $|a\rangle|b\rangle$ jelöli $|c\rangle$ helyett. A $\mathcal{H}_{(p-1) \times (p-1)}$ Hilbert terünk bázisvektorai $|a\rangle|b\rangle$ alakúak, ahol $a, b \in \mathbf{Z}_{p-1}$.

Emlékezzünk hogy $\mathbf{Z}_{p-1}$ egy véges csoport amelynek $p - 1$ eleme van. Az f függvény $(p - 1)$ darab lehetséges értékének egyenlő együtthatójú lineáris kombinációját képezzük.

$$|\phi\rangle = \frac{1}{p-1} \sum_{a \in \mathbf{Z}_{p-1}, b \in \mathbf{Z}_{p-1}} |a\rangle|b\rangle |f(a, b)\rangle.$$

Az output utolsó (azaz harmadik) regisztere tartalmazza az $|f(a, b)\rangle$ állapotvektort. Mérjük meg az output utolsó (azaz harmadik) regiszterét! (Ami az f eredményét tartalmazza.) Most ha a

$k_0 = f(a_0, b_0)$ eredményt kapjuk, akkor az output első és második regisztere a

$$|\psi\rangle = \frac{1}{\sqrt{p-1}} \sum_{k=0}^{p-2} |a_0 + ky\rangle |b_0 + k\rangle$$

periódikus állapotot tartalmazza. Azaz azon állapotok lineáris kombinációját amelyeket az f -nek inputként adva, az f függvény a $k_0 = f(a_0, b_0)$ eredményt veszi fel.

Az $\frac{1}{\sqrt{p-1}}$ szorzótényezőt hogyan kapjuk? Képezzük a

$$\sum_{k=0}^{p-2} |a_0 + ky\rangle |b_0 + k\rangle$$

vektor önmagával vett belső szorzatát (a normáját). Az eredmény: $p-1$. Idézzük fel hogy a kvantum állapotot egy olyan $\mathcal{H}_{(p-1) \times (p-1)}$ Hilbert térbeli vektorral ábrázoljuk aminek a normája 1.

Tekintsük a

$$\chi_{k_1, k_2}(a, b) = \exp(i2\pi \frac{ak_1 + bk_2}{p-1})$$

függvényt. Legyen $a = y$ és $b = 1$. Ekkor

$$\chi_{k_1, k_2}(y, 1) = \exp(i2\pi \frac{yk_1 + k_2}{p-1}).$$

Ha $yk_1 + k_2 \equiv 0 \pmod{p-1}$, akkor $k_2 \equiv -yk_1 \pmod{p-1}$ és

$$\chi_{k_1, -yk_1}(y, 1) = \exp(i2\pi \frac{yk_1 + -yk_1}{p-1}) = 1.$$

$\mathcal{F}$ jelöli a Fourier transzformációt modulo $(p-1)$ (pontosabban a $\mathbf{Z}_{(p-1)}$ monoid feletti kvantum Fourier transzformációt).

Alkalmazzuk az $\mathcal{F}$ -et az első két regiszterre! Azaz alkalmazzuk az $\mathcal{F} \otimes \mathcal{F}$ Fourier transzformációt a ψ vektorra! Az eredményül kapott vektor olyan állapotok lineáris kombinációja amelyek címkéje $(|k_1\rangle|k_2\rangle)$ (azaz a vektor $|k_1\rangle|k_2\rangle$ alakú) és

$$k_2 \equiv -yk_1 \text{ mod } (p-1).$$

A fenti lineáris kombinációban az együtthatók abszolút értéke 1. A χ_{k_1, k_2} függvény alkalmazásával adhatunk formális bizonyítást.

Állítás 14.3 $\mathcal{F} \otimes \mathcal{F}|\psi\rangle = \frac{1}{\sqrt{p-1}} \sum_{k_1=0}^{p-2} \exp(i2\pi \frac{a_0 k_1 - b_0 y k_1}{p-1}) |k_1\rangle | - yk_1 \text{ mod } (p-1) \rangle .$

Most megmérjük az állapotvektort. A kapott címkék

$$(k_1, k_2) = (k_1, -yk_1 \text{ mod } (p-1)),$$

ahol $k_1 \in \mathbf{Z}_{p-1}$ egyenletes eloszlású véletlen szám. Emlékezzünk hogy az a feladatunk hogy kiszámoljuk $y = \log_p x$ értékét a (k_1, k_2) számpáros ismeretében ami a megmért állapotot címkézi.

• Ha a mérés eredményeként véletlenül kapott $k_1 \in \mathbf{Z}_{p-1}$ relatív prím $(p-1)$ -gyel, akkor a kiterjesztett Euklideszi algoritmus-sal kiszámoljuk k_1 $\mathbf{Z}_{p-1}^*$ -beli multiplikatív inverzét, amit k_1^{-1} jelöl. (A kiterjesztett Euklideszi algoritmus futási ideje $O(\log(p-1)^2)$) [18].) Most

$$k_1 k_1^{-1} = 1 \text{ mod } (p-1).$$

Kiszámítjuk

$$y = -k_2 k_1^{-1}$$

értékét. Készen vagyunk.

- Ha $k_1 \in \mathbf{Z}_{p-1}$ nem relatív prím $(p-1)$ -gyel, akkor nem tudjuk kiszámolni y értékét a (k_1, k_2) számpáros ismeretében.

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

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

Itt $\gamma = 0.5772156\dots$ Euler konstansa Ennek megfelelően annak a valószínűsége hogy egy véletlenül választott k_1 relatív prím $(p-1)$ -gyel megközelítőleg

$$e^{\gamma} \frac{1}{\log \log (p-1)}.$$

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

Ha a p számot tízes számrendszerben ábrázoljuk n számjeggyel, akkor a leggyorsabb ismert hagyományos algoritmus a fenti feladat megoldására

$$O(\exp(n^{\frac{1}{3}}(\log n)^{\frac{2}{3}}))$$

ideig fut. Az általunk megadott kvantum algoritmus kevesebb mint $O(n^3)$ ideig fut.

15. Kvantum teleportálás teljesen összefonódott részecskékkel

Tegyük fel hogy Alice és Bob házassági ajándékként kapnak két összefonódott részecskét, amik a részecske1 és részecske2 nevet kapják. Több évvel később Bob egyedül elmegy egy hegymászó

expedícióra a Himalájába és magával viszi részecske2-t. Alice Los Angelesben marad és magánál tartja részecske1-t. Egy harmadik személy, Carol, megkéri Alice-t hogy továbbítsa egy titkos üzenetet Bobnak. Az üzenet a részecske3 állapota. Nincsen kvantum csatorna Alice és Bob között. Van hagyományos csatorna Alice és Bob között.

Feltesszük hogy részecske1 és részecske2 a

$$|\beta_0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

maximálisan összefonódott állapotban vannak. Továbbá feltesszük hogy részecske3 a

$$|c\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

állapotban van. A három részecske (most részecske3, részecske1, részecske2 sorrendben tekintjük a részecskéket) állapotát leíró állapotvektor:

$$|\xi\rangle = |c\rangle \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_1 \\ 0 \\ 0 \\ \alpha_1 \end{pmatrix}$$

más alakban:

$$|\xi\rangle = \frac{1}{\sqrt{2}}(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|100\rangle + \alpha_1|111\rangle).$$

Alice az alábbi két műveletet hajtja végre részecske1-en és részecske3-on.

1. Alice a CNOT műveletet hajtja végre részecske1-en és részecske3-on. Most részecske3 az irányító qubit és részecske1 a cél qubit. Azaz Alice a $G_{CNOT} \otimes I$ transzformációt hajtja végre az $|\xi\rangle$ állapotvektoron és áttanszformálja a quantum rendszert a $|\kappa\rangle$ állapotba.

$$\begin{aligned} \kappa &= (G_{CNOT} \otimes I)(|\xi\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |\xi\rangle \\ |\kappa\rangle &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_0 \\ \alpha_1 \\ 0 \\ 0 \\ \alpha_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_0 \\ 0 \\ \alpha_1 \\ \alpha_1 \\ 0 \end{pmatrix} \end{aligned}$$

Tehát

$$|\kappa\rangle = \frac{1}{\sqrt{2}}(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|101\rangle + \alpha_1|110\rangle).$$

2. Alice a Hadamard transzformációt alkalmazza az első qubit-re (részecske3-ra). A másodikat (részecske1-et) érintetlenül hagyja. Ez azt jelenti hogy a $|\kappa\rangle$ állapotra a $H \otimes I \otimes I$ transzformációt alkalmazza és $|\kappa\rangle$ állapotot a $|\zeta\rangle$ állapotba transzformálja.

$$|\zeta\rangle = (H \otimes I \otimes I)|\kappa\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |\kappa\rangle.$$

Tehát

$$|\zeta\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_0 \\ 0 \\ \alpha_1 \\ \alpha_1 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_1 \\ \alpha_0 \\ \alpha_0 \\ -\alpha_1 \\ -\alpha_1 \\ \alpha_0 \end{pmatrix}$$

Tehát

$$|\zeta\rangle = \frac{1}{2}[\alpha_0(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \alpha_1(|001\rangle + |010\rangle - |101\rangle - |110\rangle)].$$

A fenti kifejezésében elszigeteljük az első kettő qubitet (részecske3-at és részecske1-et).

$$|\zeta\rangle = \frac{1}{2}[|00\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle) + |01\rangle(\alpha_0|1\rangle + \alpha_1|0\rangle) + |10\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle) + |11\rangle(\alpha_0|1\rangle - \alpha_1|0\rangle)].$$

A fentiek alapján a következőket kapjuk: Amikor Alice megméri együtt az első kettő qubitet (részecske3-at és részecske1-et), akkor a következő négy, egyformán valószínű eredmény valamelyikét kapja:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

Mint tudjuk, az Alice által elvégzett mérés az első két qubitet a négy bázis állapotvektor valamelyikébe kényszeríti. Ilyen módon kvantum információt alakít át hagyományos információba. Ezután, hagyományos kommunikációs csatornán, Alice elküldi Bobnak a

mérés eredményét: 00, 01, 10 vagy 11.

Az Alice által elvégzett mérés a Bob tulajdonában lévő részecske2 qubitet az alábbi négy állapot valamelyikébe kényszeríti:

1. $|\eta_{00}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ amikor a mérés eredménye 00.
2. $|\eta_{01}\rangle = \alpha_0|1\rangle + \alpha_1|0\rangle$ amikor a mérés eredménye 01.
3. $|\eta_{10}\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle$ amikor a mérés eredménye 10.
4. $|\eta_{11}\rangle = \alpha_0|1\rangle - \alpha_1|0\rangle$ amikor a mérés eredménye 11.

Bob, az Alicetól kapott szótól függően, az alábbi táblázat szerint, a részecske2 qubitjére alkalmaz egy 1-qubites kvantum kapu által megvalósított transzformációt.

Bob által kapott szó	Bob által alk. kapu	részecske2 új értéke
00	I	$I \eta_{00}\rangle = c\rangle$
01	X	$X \eta_{01}\rangle = c\rangle$
10	Z	$Z \eta_{10}\rangle = c\rangle$
11	X utána Z	$ZX \eta_{11}\rangle = c\rangle$

Emlékezzünk:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Most a Bob tulajdonában lévő részecske2 ugyanabban az állapotban van mint részecske3 volt eredetileg. részecske3 állapota megváltozik az eljárás során, így állapot klónozás nem történt.

16. A kvantum Turing gép

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

- Q a véges állapot halmaz,
- $q_0, q_f \in Q$ rendre a kezdő állapot, és a végállapot,
- A az ábécé,
- δ a Turing gép átmenet amplitúdó függvénye.

$$\delta : Q \times A \times Q \times A \times \{-1, 0, 1\} \rightarrow \mathbf{C}_{[0,1]}$$

egy leképezés. $\delta(q_1, a_1, q_2, a_2, d)$ az amplitúdója annak hogy ha a Turing gép q_1 állapotban van és az a_1 szimbólumot olvassa akkor a_1 helyébe a_2 szimbólumot ír és a q_2 állapotba lép és az író-olvasó fejet a $d \in \{-1, 0, 1\}$ irányban elmozdítja. $\mathbf{C}_{[0,1]}$ az összes olyan komplex szám halmaza amely abszolút értéke kisebb egyenlő 1-nél.

Az átmenet amplitúdó függvény kielégíti az alábbi feltételt.

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

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

A bázis konfiguráció megfelel a hagyományos Turing gép konfigurációjának. A bázis konfigurációk egy ortonormális bázist alkotnak egy végtelen dimenziós, belső szorzattal rendelkező vektortér felett.

A kvantum Turing gép általános konfigurációja

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

alakú ahol c_i bázis konfiguráció és $\alpha_i \in \mathbf{C}$ és

$$|\alpha_1|^2 + \dots + |\alpha_m|^2 = 1$$

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

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

A δ átmenet amplitúdó függvény meghatároz egy M_δ lineáris leképezést a vektor térben. Ezt átmeneti relációnak (időbeni fejlődés leképezésnek) nevezzük. Ezt az átmeneti relációt követjük amikor a gyökérből az 1. mélységű szintre lépünk, amikor az 1.

mélységű szintről a 2. mélységű szintre lépünk. Általában amikor az i -edik szintről az $i + 1$ -edik szintre lépünk.

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

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

Azt mondjuk hogy M megáll egy K általános konfiguráción, ha K olyan bázis konfigurációk lineáris kombinációja amelyek mindegyikén megáll M . (Azaz K csak olyan bázis konfigurációkat tartalmaz amelyek mindegyikén megáll M .) Ha M megáll egy K általános konfiguráción, akkor K fenti előállításában szereplő minden egyes fenti bázis konfiguráció szalagtartalmához hozzárendeljük a konfiguráció valószínűségét. (Ha több bázis konfiguráció szalagtartalma megegyezik akkor a valószínűségek amplitúdók összeadódnak.) Így módon minden inputra egy output valószínűségek eloszlást kapunk.

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

Az M kvantum Turing gépről feltesszük a következőt: tekintsünk egy tetszőleges $x + iy$ átmenet amplitúdót ahol x és/vagy y nem racionális számok. Megköveteljük hogy x -et és y -t hatékonyan

tudjuk közelíteni racionális számokkal. Azaz adott egy hatékony algoritmus amely tetszőleges pontossággal közelíti x -et és y -t racionális számokkal.

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

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

- tetszőleges M kvantum Turing gép leírását (kódját),
- M -nek tetszőleges x inputját,
- tetszőleges k természetes számot, és
- tetszőleges $\epsilon > 0$ számot,

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

17. Számelmélet

Definíció 17.1 A prím teszt egy olyan eljárás (algoritmus) amelynek

- inputja egy tetszőleges n egész szám,
- outputja 'igen' ha n prímszám; 'nem' ha n nem prímszám.

Állítás 17.2 Adleman, Pomerance, Rumely prím tesztjének futási ideje

$$O((\log n)^{c(\log \log \log n)}) .$$

Itt c egy konstans ami nem függ n -től. Továbbá $\log \log \log n = \log(\log(\log(n)))$.

Állítás 17.3 Agrawal, Kayal, Saxena prím tesztjének futási ideje $O((\log n)^6)$.

Legyen N egy természetes szám. Tegyük fel hogy N bináris alakja L darab bitből áll. Megadunk egy hatékony klasszikus algoritmust amely eldönti hogy $N = a^b$ alakú-e valamely $a \geq 1$ és $b \geq 2$ számokra.

Állítás 17.4 Ha $N = a^b$ alakú valamely $a \geq 1$ és $b \geq 2$ számokra, akkor $b \leq L$.

Bizonyítás. Tegyük fel hogy $N > 1$. Most $a \geq 2$. Ezért $b \leq L$.

Állítás 17.5 Legyen $b \leq L$ tetszőleges. Legyen $y = \log_2 N$, $x = \frac{y}{b}$, $b \leq L$. Legyen u_1 és u_2 a két legközelebbi egész szám 2^x -hez. Azaz, legyen $u_1 \leq 2^x \leq u_1 + 1 = u_2$. Ekkor legfeljebb $O(L^2)$ darab műveletet vesz igénybe y , x , u_1 és u_2 kiszámítása, ahol $b = 1, 2, \dots, L$.

Állítás 17.6 b bináris alakja alapján a következő módon kiszámoljuk u_1^b értékét. Ismételt négyzetre emeléssel kiszámoljuk u_1^2 , u_1^4 , u_1^8 , u_1^{16} , $\dots$ értékét. Majd tekintjük azokat a helyiértékeket, ahol 1 áll. Ezekhez a helyiértékekhez tartozó u_1 hatványokat

összeszorozzuk. Hasonlóan kiszámoljuk u_2^b értékét is. Majd összehasonlítjuk u_1^b és u_2^b értékét N -nel. A fenti eljárás legfeljebb $O(L^2)$ darab műveletet vesz igénybe.

Állítás 17.7 Legyen N egy természetes szám. Tegyük fel hogy N bináris alakja L darab bitből áll. Van olyan klasszikus eljárásunk amely eldönti hogy $N = a^b$ alakú-e valamely $a \geq 1$ és $b \geq 2$ számokra. A fenti eljárás legfeljebb $O(L^3)$ darab műveletet vesz igénybe.

Bizonyítás. $b = 2, \dots, L$ minden egyes értékére rendre elvégezzük az alábbiakat:

Kiszámoljuk az $y = \log_2 N$, $x = \frac{y}{b}$ számokat. Pontosabban fogalmazva, $y = \log_2 N$, $x = \frac{y}{b}$ számok bináris tört alakú közelítéseit számoljuk ki. Ezeket a bináris tört alakú közelítéseket teszőleges pontossággal ki tudjuk számolni. x egy bináris tört alakú közelítése

$$b_0 b_1 b_2 \dots b_k . b_{k+1} b_{k+2} \dots b_\ell$$

alakú. Legyen u_1 és u_2 a két legközelebbi egész szám 2^x -hez. Azaz, legyen $u_1 \leq 2^x \leq u_1 + 1 = u_2$. Kiszámoljuk u_1 -et és u_2 -t. Ehhez x és így 2^x értékét határozzuk meg egyre pontosabban. Figyeljük meg, hogy $2^{0.1} = 2^{\frac{1}{2}}$, $2^{0.01} = 2^{\frac{1}{4}}$, $\dots$. Ezért itt felhasználjuk azt hogy

$$2^{\frac{1}{2}} = \sqrt{2}$$

$$2^{\frac{1}{4}} = \sqrt{\sqrt{2}}$$

$$2^{\frac{1}{8}} = \sqrt{\sqrt{\sqrt{2}}}$$

...

Majd kiszámoljuk u_1^b értékét és u_2^b értékét. Ezután összehasonlítjuk u_1^b és u_2^b értékét N -nel. Ha $u_1^b = N$ vagy $u_2^b = N$, akkor visszaadjuk az 'igen' szót és az $u_1^b = N$ egyenlőséget vagy az $u_2^b = N$ egyenlőséget. Ha $u_1^b = N$ vagy $u_2^b = N$ sosem teljesül az eljárás futása során (azaz $b = 2, \dots, L$ egyetlen értékére sem), akkor visszaadjuk a 'nem' szót.

Lineáris futás idejű algoritmusok ismertek

- a $\log_2$ (2 alapú logaritmus) bináris (2-es számrendszer feletti) kiszámítására,
 - bináris gyökvonásra,
- azaz ezek az algoritmusok $O(n)$ darab műveletet végeznek el ahol n bitből áll az input.

□

Hivatkozások

- [1] Taoufik AMRI, Sphere bloch.jpg,
https://commons.wikimedia.org/wiki/File:Sphere_bloch.jpg
- [2] Black, Paul & Kuhn, D. & Williams, Carl. (2002). Quantum Computing and Communication. Advances in Computers. 56. 189-244. 10.1016/S0065-2458(02)80007-9.
továbbá
P. E. Black, D. R. Kuhn, C.J. Williams, Quantum Computing and Communication - Scientific Figure on ResearchGate. Available from:
https://www.researchgate.net/figure/Double-slit-experiment-with-electrons_fig6_222547161 [accessed 10 May, 2019]

- [3] Budó Ágoston, Mátrai Tibor, Kísérleti fizika III, Tankönyvkiadó, Budapest, 1980.
- [4] Dave3457, Circular.Polarization.Circularly.Polarized.Light With.Components Left.Handed.svg
https://commons.wikimedia.org/wiki/File:Circular.Polarization.Circularly.Polarized.Light_With.Components_Left.Handed.svg
https://en.wikipedia.org/wiki/User:Dave3457/list_of_the_related_images
- [5] Artur Ekert, Richard Jozsa, Quantum Algorithms: Entanglement Enhanced Information Processing, arXiv:quant-ph/9803072 also in Phil. Trans. Roy. Soc. (Lond.) 1998, Proceedings of Royal Society Discussion Meeting „Quantum Computation: Theory and Experiment”, held in November 1997
- [6] Kevin Garapo, Mhlambululi Mafu, Francesco Petruccione, The six states spanning the Bloch sphere,
https://commons.wikimedia.org/wiki/File:Six_states_Blochq_sphere.jpg
- [7] David Harrison, The Feynman Double Slit,
<https://faraday.physics.utoronto.ca/GeneralInterest/Harrison/DoubleSlit/DoubleSlit.htm>
- [8] Mika Hirvenselo, Quantum Computing, Second Edition, Springer 2004.
- [9] Sándor Imre, Ferenc Balázs, Quantum Computing and Communications An Engineering Approach, John Wiley & Sons, 2004.
- [10] Johannes Kalliauer, Nekoja Nekoja, An illustration of the 'Double-slit experiment' in physics.
<https://commons.wikimedia.org/wiki/File:Doubleslit.svg>
- [11] A. Yu. Kitaev, A. H. Shen, M. N. Vyalıy, Classical and Quantum Computation, American Mathematical Society, Providence, Rhode Island, USA, 2002.
- [12] Logikai kapu, Wikipédia, a szabad enciklopédia,
https://hu.wikipedia.org/wiki/Logikai_kapu
- [13] Dan C. Marinescu, Gabriela M. Marinescu, Approaching Quantum Computing, Pearson Prentice Hall, Upper Saddle River, New Jersey, USA, 2005.
- [14] Bob Mellish, Wire-grid-polarizer, the English wikipedia,
<https://commons.wikimedia.org/wiki/File:Wire-grid-polarizer.svg>

és

<https://upload.wikimedia.org/wikipedia/commons/thumb/9/94/Wire-grid-polarizer.svg/1280px-Wire-grid-polarizer.svg.png>

- [15] Theresa Knott, Stern-Gerlach experiment
<https://commons.wikimedia.org/w/index.php?curid=563880>
- [16] M. A. Nielsen, I. L. Chuang, Quantum Computing and Quantum Information, Cambridge University Press, 2000.
- [17] Polarization (wave polarization),
<https://whatis.techtarget.com/definition/polarization-wave-polarization>
- [18] Modular multiplicative inverse, Wikipedia The Free Encyclopedia.
https://en.wikipedia.org/wiki/Modular_multiplicative_inverse#Extended_Euclidean_algorithm
- [19] Smite-Meister, Bloch sphere.svg,
https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg
- [20] Quantum Fourier transform,
https://en.wikipedia.org/wiki/Quantum_Fourier_transform
https://wikimedia.org/api/rest_v1/media/math/render/svg/e866e432c1e714317e67971fa7cf03bd4e7a879f
- [21] Fredkin Gate,
<https://commons.wikimedia.org/w/index.php?curid=14706620>
- [22] George Stamatiou, <https://en.wikipedia.org/w/index.php?curid=18970008>
- [23] Tatoute SternGerlach experiment,
<https://commons.wikimedia.org/w/index.php?curid=34095239>
- [24] Arun C. Thomas, Quantum Computing explained!
<https://hackernoon.com/quantum-computing-explained-a114999299ca>