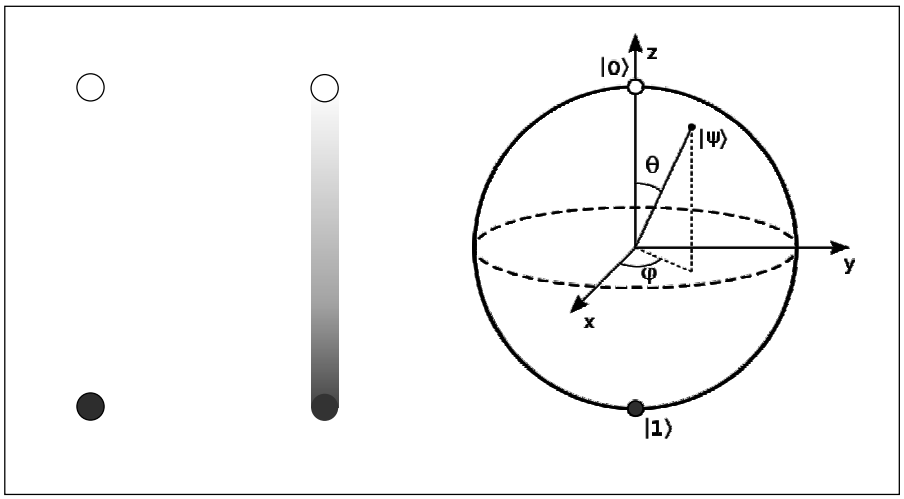
Kodowanie, Kompresja, Kryptografia

Konspekt VII, 12.VI.2023

Informacja kwantowa

Nośnik informacji — qubit: stan dwupoziomowego układu kwantowego



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad \alpha,\beta \in \mathbb{C}, \;\; |\alpha|^2 + |\beta|^2 = 1\,.$$

Postulaty mechaniki kwantowej

I. Z każdym izolowanym układem kwantowym S skojarzona jest zespolona przestrzeń wektorowa $\mathcal{H}_S$ z iloczynem skalarnym (przestrzeń Hilberta) zwana przestrzenią stanów układu. Stan układu jest w każdej chwili wyczerpująco opisany przez pewien unormowany wektor $|\psi\rangle \in \mathcal{H}_S, \;\; \| \, |\psi\rangle \, \| = 1.$

II. Ewolucja izolowanego układu kwantowego opisana jest przez unitarną transformację w $\mathcal{H}_S$. Jeśli w chwili t_1 układ znajduje się w stanie $|\psi_1\rangle$, a w chwili t_2 w stanie $|\psi_2\rangle$, wtedy stany te powiązane są relacją

$$|\psi_2\rangle = U\,|\psi_1\rangle$$

gdzie U jest operatorem unitarnym, $U^*U = I$, zależnym jedynie od t_1 i t_2.

III. Przestrzenią stanów układu złożonego z podukładów A i B jest przestrzeń Hilberta będąca iloczynem tensorowym przestrzeni odp. podukładów

$$\mathcal{H}_{AB} \;=\; \mathcal{H}_A \otimes \mathcal{H}_B$$

IV. Pomiary kwantowe opisane są rodziną $\{W_m\}$ operatorów pomiaru, działających na przestrzeni $\mathcal{H}$ układu. Zbiór indeksów m odpowiada możliwym wynikom pomiaru. Jeśli pomiar wykonany jest w stanie ψ, wówczas wynik m pojawia się z prawdopodobieństwem

$$p_m \;=\; \langle\psi|\; W_m^* W_m \;|\psi\rangle \;\;,$$

a stan układu bezpośrednio po pomiarze będzie miał postać

$$\frac{1}{\sqrt{p_m}} W_m \;|\psi\rangle \;\;.$$

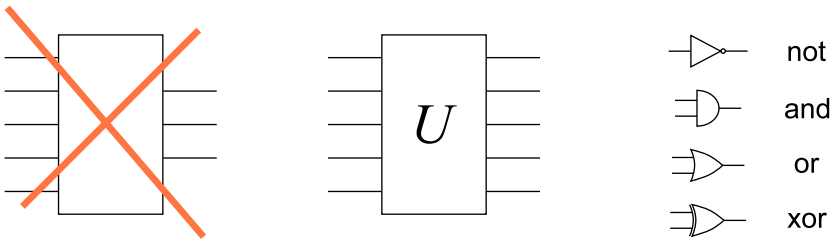
Operatory pomiaru tworzą układ zupełny

$$\sum_m W_m^* W_m \;=\; I$$

co odpowiada zupełności układu prawdopodobieństw $\sum_m p_m = 1$.

Dynamika

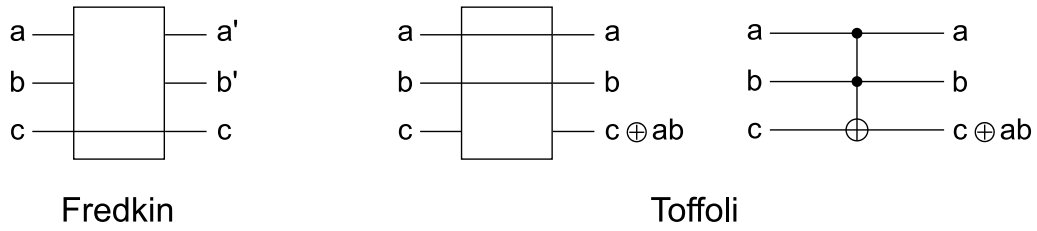
Przetwarzanie danych binarnych — układ bramek logicznych.



Mechanika kwantowa wymaga *odwracalności* operacji logicznych. Wśród bramek klasycznych tylko NOT jest odwracalna.

$$\text{Liczba wejść} \;=\; \text{liczba wyjść}$$

Uniwersalne klasyczne bramki odwracalne:

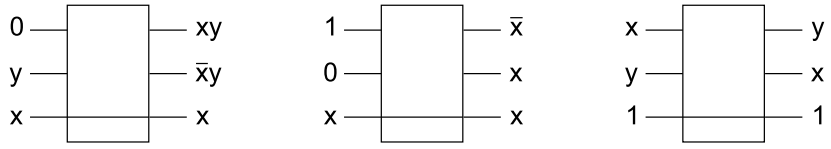


Fredkin Toffoli

1. Bramka Fredkina. Trzeci bit pełni rolę sterującą. Jeśli $c = 0$, bramka działa jak identyczność, $a' = a$, $b' = b$. Jeśli zaś $c = 1$, a zamienia się z b. Istnieje ciekawa realizacja fizyczna tej bramki: "maszyna bilardowa" (p. osobne rysunki).

   ZADANIE: *narysuj tabelkę 0–1 opisującą działanie tej bramki i przekonaj się, że jest ono odwracalne.*

   Bramka Fredkina jest *uniwersalna*, tzn. może realizować operacje AND i NOT, a więc także wszystkie inne operacje logiczne. Dodatkowo CLONE — powielenie wartości bitu i CROSS — zamiana x i y.



and not clone cross

2. Bramka Toffoliego. Bity a i b pełnią rolę kontrolną. Jeśli $ab = 0$, c pozostaje bez zmian, jeśli zaś $a = b = 1$, c podlega negacji. Bramkę tę w kontekście kwantowym nazywa się CCNOT (contrelled–controlled NOT). Jest też prostsza bramka 2×2 CNOT (controlled NOT) o podobnym działaniu, lecz tylko jednym bicie kontrolnym.

   ZADANIE: *jak wyżej przeanalizuj tabelki 0–1 dla CNOT i CCNOT pod kątem odwracalności.*
   CCNOT też jest uniwersalna, bo można przy jej pomocy zaimplementować operację NAND (która jak wiadomo jest uniwersalna): jeśli $c = 1$ to $c' = 1 \oplus ab = \overline{ab}$. Ponadto biorąc $a = 1$ i $c = 0$ otrzymamy $c' = b$ czyli sklonowane b. Nie można zrealizować nią operacji CROSS, ale można to zrobić przy pomocy 3 połączonych szeregowo bramek CNOT.

Iloczyn tensorowy, unitarna reprezentacja bramek

Iloczyn tensorowy vs. iloczyn kartezjański przestrzeni:

$$\dim(U \times V) = \dim U \; + \; \dim V, \qquad \dim(U \otimes V) = \dim U \; \cdot \; \dim V$$

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \times \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \; = \; \left[\begin{array}{c} u_1 \\ u_2 \\ u_3 \\ \hline v_1 \\ v_2 \end{array}\right], \qquad \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \otimes \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \; = \; \begin{bmatrix} u_1 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \\ u_2 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \\ u_3 \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \end{bmatrix}$$

Przestrzeń stanów dwóch qubitów

Niech $\mathcal{H}_1$ oznacza przestrzeń stanów pojedynczego qubitu, czyli 2-wymianową przestrzeń zespoloną z bazą $\left\{ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \;\; |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$.

Zapis skrótowy: $|a\rangle \otimes |b\rangle = |ab\rangle$. Baza $\mathcal{H}_2 = \mathcal{H}_1 \otimes \mathcal{H}_1$:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \qquad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \qquad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

Zauważmy, że niektóre superprozycje stanów takiego układu można rozłożyć na iloczyn tensorowy stanów pojedynczych qubitów, a innych nie. Np.

$$\frac{1}{\sqrt{2}}(\, |00\rangle \; + \; |01\rangle \,) = \; |0\rangle \; \otimes \frac{|0\rangle \; + \; |1\rangle}{\sqrt{2}} \, ,$$

ale nie można tego zrobić dla stanu $\frac{1}{\sqrt{2}}(\, |00\rangle \; + \; |11\rangle \,)$ (trochę analogicznie do $a^2 + ab = a(a+b)$, ale już nie dla $a^2 + b^2$).

Oznaczenia: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ – identyczność, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ – macierz NOT.

Macierz CNOT

$$\left[\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right] \; = \; \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

Macierz CCNOT (Toffoli)

$$\left[\begin{array}{c|c|c} \begin{array}{c|c} I & 0 \\ \hline 0 & I \end{array} & \multicolumn{2}{c}{0} \\ \hline \multicolumn{2}{c|}{0} & \begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array} \end{array}\right] = \left[\begin{array}{cccccc} 1 & 0 & & & & \\ 0 & 1 & 0 & & & \\ & 0 & \ddots & 0 & & \\ & & 0 & 1 & 0 & \\ & & & 0 & 0 & 1 \\ & & & & 1 & 0 \end{array}\right]$$

ZADANIE: *Zapisz macierz dla bramki Fredkina.*

Wszystkie te macierze są unitarne.

Jak działają te bramki na kwantowych stanach qubitów?

Bramka CNOT z drugim bitem ustawionym na 0 klonuje klasyczne stany $a \in \{\,|0\rangle\,,\,|1\rangle\,\}$ pierwszego bitu: $|a0\rangle \;\rightarrow\; |aa\rangle$. Ale nie jest to już prawdą, gdy pierwszy bit ma wartość $a = \alpha\,|0\rangle + \beta\,|1\rangle$. Wtedy

$$|a0\rangle = \begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix} = \alpha\,|00\rangle + \beta\,|11\rangle \quad \neq \quad |aa\rangle$$

No-cloning Theorem

Nie istnieje proces kwantowy, który powielałby nieznany stan qubitu.

Dowód. Załóżmy nie wprost, że taka operacja U istnieje, tj. dla dowolnych dwóch stanów $|\psi\rangle\,,\;|\phi\rangle$ mamy

$$\begin{aligned} U(\,|\psi\rangle \otimes |s\rangle\,) &= |\psi\rangle \otimes |\psi\rangle \\ U(\,|\phi\rangle \otimes |s\rangle\,) &= |\phi\rangle \otimes |\phi\rangle \end{aligned}$$

Obliczając stronami iloczyny skalarne

$$(\,\langle\phi| \otimes \langle s|\,)U^*U(\,|\psi\rangle \otimes |s\rangle\,) \;=\; \langle\phi|\psi\rangle\;\langle s|s\rangle \;=\; (\,\langle\phi|\psi\rangle\,)^2\,,$$

czyli $z = z^2$, a to ma tylko dwa rozwiązania: $z = 0$ lub $z = 1$. W pierwszym wypadku mamy $|\phi\rangle \perp |\psi\rangle$, a w drugim $|\phi\rangle = |\psi\rangle$. Widać więc, że klonowanie nie może działać uniwersalnie. Jeśli daje się (przypadkiem) sklonować jakiś stan, to można tą samą operacją sklonować co najwyżej stany do niego ortogonalne.

Bramki kwantowe

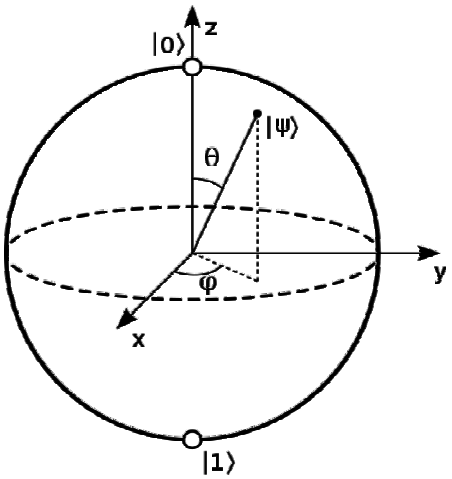
Uniwersalność: chodzi o utworzenie minimalnego zbioru prostych bramek, z którego dałoby się zbudować dowolną operację unitarną na układzie n qubitów, $\mathcal{H}_n = \mathbb{C}^{2^n}$. (Podobnie jak NOT i AND albo NAND tworzą klasy zupełne w klasycznej logice). Oprócz poznanych bramek X, CNOT i CCNOT, zwykle korzysta się z kilku innych:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Są to tzw. *macierze Pauliego* tworzące wygodną bazę popdprzestrzeni macierzy Hermitowskich w $\mathbb{M}_{2\times 2}(\mathbb{C})$. Dodatkowo używa się bramek Hadamarda $H = \frac{1}{\sqrt{2}}(X+Z)$ oraz tzw. bramek "fazowych" S i T, powiązanych relacjami $S^2 = Z$, $T^2 = S$:

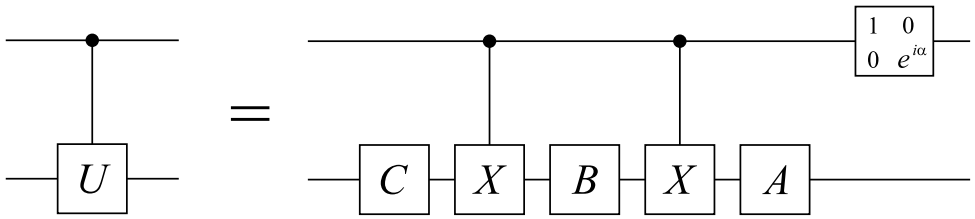
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \qquad T = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix},$$

X, Y, Z generują obroty wokół osi $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ sfery Blocha



Każda operacja unitarna na pojedynczym qubicie może być przedstawiona jako złożenie 3 obrotów wokół 2 nierównoległych osi. Można to zrealizować kombinacją operatorów X, Y, Z, H i T.

Podobnie jak CNOT, ważne są operacje "sterowane" drugim qubitem:

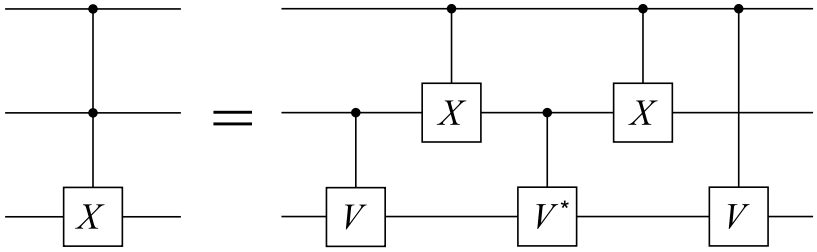


Gdy pierwszy qubit $b = 0$, bramka nie robi nic ($= I$), a gdy $b = 1$, U działa na drugi qubit. Czasem w uproszczeniu zapisuje się to jako U^b. Konstrukcja bramki "sterowane U" korzysta z twierdzenia o rozkładzie operatorów unitarnych 2×2

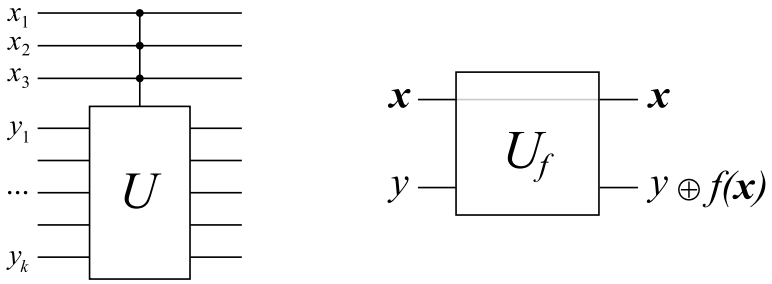
$$U \;=\; e^{i\alpha} AXBXC\,, \qquad \text{przy czym} \quad ABC = I\,,$$

gdzie A, B, C można poskładać z prostych obrotów wokół osi $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$.

CNOT służy także do konstrukcji bramek wielo-qubitowych, np. CCNOT



gdzie $V = \sqrt{X} = \frac{1-i}{2}(I + iX)$. Układy bramek pozwalają w szczególności tworzyć wielopoziomowe, wielokrotnie sterowane operacje



w skrócie: $U^{x_1 x_2 x_3} \, |y_1 \ldots y_k\rangle$. Drugi rysunek pokazuje schemat jak w sposób odwracalny można obliczać dowolną funnkcję logiczną $f : \{0,1\}^n \to \{0,1\}$.

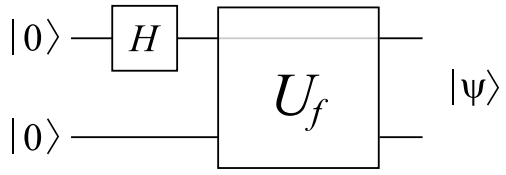
Algorytm Deutscha-Jozsy

f jest nieznaną funkcją logiczną na pojedynczego bitu. Są 4 takie funkcje: $\mathbf{0}$, $\mathbf{1}$, I oraz X. Ile "pytań" typu $f(0) = ...$ trzeba zadać, aby sprawdzić czy f jest stała? Klasycznie muszą być zadane 2 pytania $f(0)$ i $f(1)$. Kwantowo można jednoznacznie rozpoznać typ f za pomocą ... *jednego* pytania.

Algorytm, tak jak na obrazku wyżej, oblicza $|x,\, y\rangle \;\to\; |x,\, y \oplus f(x)\rangle$. Można sprawdzić, wypisując pary tych wektorów dla czterech różnych funkcji f, że U_f jest dane kolejno dla $\mathbf{0}$, $\mathbf{1}$, I, X następującymi macierzami

$$\left[\begin{array}{cc|cc} 1 & & & \\ & 1 & & \\ \hline & & 1 & \\ & & & 1 \end{array}\right] \quad \left[\begin{array}{cc|cc} 0 & 1 & & \\ 1 & 0 & & \\ \hline & & 0 & 1 \\ & & 1 & 0 \end{array}\right] \quad \left[\begin{array}{cc|cc} 1 & & & \\ & 1 & & \\ \hline & & 0 & 1 \\ & & 1 & 0 \end{array}\right] \quad \left[\begin{array}{cc|cc} 0 & 1 & & \\ 1 & 0 & & \\ \hline & & 1 & \\ & & & 1 \end{array}\right]$$

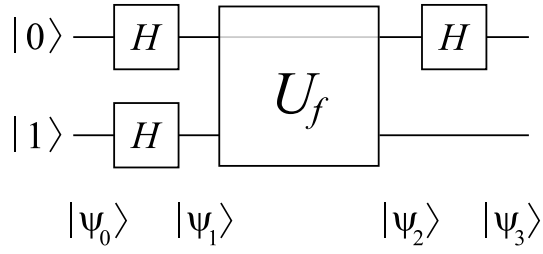
Zadanie polega więc na tym, żeby najmniejszą liczbą testów dowiedzieć się czy U_f ma postać 1 lub 2, czy też 3 lub 4. Jeśli utworzymy układ bramek



$$|0\rangle\ |0\rangle \quad \to \quad \frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)\,|0\rangle \quad \to \quad \frac{1}{\sqrt{2}}(\,|0, f(0)\rangle + |1, f(1)\rangle\,)\,,$$

w wyniku $|\psi\rangle$ mieści się *pełna informacja* o f.

Weźmy teraz układ



Kolejno mamy $|\psi_0\rangle = |0, 1\rangle \quad \to \quad |\psi_1\rangle = \frac{1}{2}(\,|0\rangle + |1\rangle\,) \otimes (\,|0\rangle - |1\rangle\,)$.

Dalej jeśli oznaczymy pierwszy qubit przez $|x\rangle$ (tj. $x = 0$ lub $x = 1$) obliczymy dla składników $|\psi_1\rangle$

$$\begin{aligned}
\frac{1}{2}\,|x\rangle\,(\,|0\rangle\,-\,|1\rangle\,) \quad &\rightarrow \quad \frac{1}{2}\,|x\rangle\,(\,|f(x)\rangle\,-\,\left|\overline{f(x)}\right\rangle\,) \\
&= \quad \begin{cases} \frac{1}{2}\,|x\rangle\,(\,|0\rangle\,-\,|1\rangle\,) & \text{gdy } f(x)=0 \\ \frac{1}{2}\,|x\rangle\,(\,|1\rangle\,-\,|0\rangle\,) & \text{gdy } f(x)=1 \end{cases} \\
&= \quad \frac{(-1)^{f(x)}}{2}\,|x\rangle\,(\,|0\rangle\,-\,|1\rangle\,)
\end{aligned}$$

Łącząc teraz wszystkie wyniki, zapiszemy $|\psi_2\rangle = U_f\,|\psi_1\rangle$ jako

$$\begin{aligned}
|\psi_2\rangle \;&=\; \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}\,|0\rangle\,+(-1)^{f(1)}\,|1\rangle\Big)\otimes\frac{1}{\sqrt{2}}\,(\,|0\rangle\,-\,|1\rangle\,) \\
&= \begin{cases} \pm\frac{1}{\sqrt{2}}(\,|0\rangle\,+\,|1\rangle\,)\otimes\frac{1}{\sqrt{2}}(\,|0\rangle\,-\,|1\rangle\,) & \text{gdy } f(0)=f(1) \\ \pm\frac{1}{\sqrt{2}}(\,|0\rangle\,-\,|1\rangle\,)\otimes\frac{1}{\sqrt{2}}(\,|0\rangle\,-\,|1\rangle\,) & \text{gdy } f(0)\neq f(1) \end{cases}
\end{aligned}$$

Bramka H działając na pierwszy qubit $|\psi_2\rangle$ robi z tego

$$|\psi_3\rangle \;=\; \begin{cases} \pm\,|0\rangle\,\otimes\frac{1}{\sqrt{2}}(\,|0\rangle\,-\,|1\rangle\,) & \text{gdy } f(0)=f(1) \\ \pm\,|1\rangle\,\otimes\frac{1}{\sqrt{2}}(\,|0\rangle\,-\,|1\rangle\,) & \text{gdy } f(0)\neq f(1) \end{cases}$$

Pomiar pierwszego qubitu ujawnia czy $f(0) = f(1)$ czy też nie.

Podobne zadanie, ale znacznie trudniejsze: $f : \{0,1\}^n \rightarrow \{0,1\}$ nieznana funkcja. Co najmniej ile pytań $f(x_1, x_2, \ldots, x_n) = \ldots$ trzeba zadać, by upewnić się czy f jest stała, czy też zbalansowana (przyjmuje 2^{n-1} razy wartość 0 i tyle samo razy wartość 1).

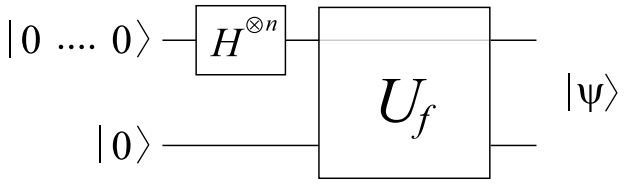
Liczba pytań w deterministycznym badaniu to maksymalnie $2^{n-1}+1$ dla różnych $\boldsymbol{x} = (x_1, \ldots, x_n)$. Można jednak prościej rozwiązać zadanie stosując rachunek prawdopodobieństwa: jeśli funkcja jest zbalansowana, dla losowo wybranego $\boldsymbol{x}$ prawdopodobieństwo obliczenia $f(\boldsymbol{x}) = 0$ wynosi $\frac{1}{2}$. W tym wypadku jeśli powtórzymy pytanie k razy dla różnych $\boldsymbol{x}$, prawdopodobieństwo tego, że kolejne wyniki będą takie same maleje tak jak $\frac{1}{2^k}$. Jeśli f jest zbalansowana, szybko się o tym przekonamy. Jeśli wychodzą stale takie same wartości, z dużym prawdopodobieństwem funkcja jest stała.

Wielowymiarowa wersja algorytmu Deutscha wymaga na końcu pomiaru stanu n qubitów.

Wykorzystywana sztuczka:

$$\begin{aligned} H^{\otimes n}\,|00\ldots0\rangle &= H\,|0\rangle \otimes H\,|0\rangle \otimes \cdots \otimes H\,|0\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned}$$

gdzie przez $|x\rangle$ oznaczamy n cyfrowe binarne rozwinięcie liczby x (np. $|21\rangle = |00010101\rangle$ gdy $n = 8$)



$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x,\, f(x)\rangle \ ,$$

a więc stan ten jest superpozycją wszystkich wyników obliczania $f(x)$ dla kolejnych x od $0 = |00\ldots0\rangle$ do $2^n - 1 = |11\ldots1\rangle$.

Pomiar kwantowy

Najprostszy schemat — pomiar w bazie obliczeniowej. Operatory W_i mają postać

$$W_0 \;=\; |0\rangle\langle 0| \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad W_1 \;=\; |1\rangle\langle 1| \;=\; \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Jeśli pomiar dotyczy stanu $|\psi\rangle \;= \alpha\,|0\rangle \,+\, \beta\,|1\rangle$, prawdopodobieństwa otrzymania wyniku 0 i 1 wynoszą

$$\begin{aligned} p_0 \;=\; \langle\psi|0\rangle\langle 0|\psi\rangle \;&=\; \overline{\alpha}\,\langle 0|0\rangle\,\alpha\,\langle 0|0\rangle \;+\; \overline{\alpha}\,\langle 0|0\rangle\,\beta\,\langle 0|1\rangle \\ &\qquad + \overline{\beta}\,\langle 1|0\rangle\,\alpha\,\langle 0|0\rangle \;+\; \overline{\beta}\,\langle 1|0\rangle\,\beta\,\langle 0|1\rangle \\ &=\; |\alpha|^2 \end{aligned}$$

i podobnie $p_1 = |\beta|^2$. Po pomiarze $|\psi\rangle$ przechodzi, zależnie od wyniku, w jeden ze stanów

$$\frac{1}{|\alpha|}\,|0\rangle\langle 0|\,\psi\rangle \;=\; \frac{\alpha}{|\alpha|}\,|0\rangle \qquad \text{lub} \qquad \frac{1}{|\beta|}\,|1\rangle\langle 1|\,\psi\rangle \;=\; \frac{\beta}{|\beta|}\,|1\rangle$$

Jeśli $\psi = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ oba wyniki są jednakowo prawdopodobne $p_i = \frac{1}{2}$.

Jeśli pomiar byłby wykonywany w bazie "diagonalnej"[1]

$$|\nearrow\rangle \;= \frac{|0\rangle \,+\, |1\rangle}{\sqrt{2}}, \qquad |\searrow\rangle\; \frac{|0\rangle \,-\, |1\rangle}{\sqrt{2}}$$

operatory W_i miałyby postać

$$W_{\nearrow} \;=\; \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad \text{i} \qquad W_{\searrow} \;=\; \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

Pomiar stanu $|\psi\rangle \;=\; |0\rangle$ w tej bazie zwraca jako wynik orientację $|\nearrow\rangle$ lub $|\searrow\rangle$, każdą z prawdopodobieństwem $\frac{1}{2}$, ponieważ

$$|0\rangle \;=\; \frac{|\nearrow\rangle \,+\, |\searrow\rangle}{\sqrt{2}}.$$

Podobnie ponieważ

$$|1\rangle \;=\; \frac{|\nearrow\rangle \,-\, |\searrow\rangle}{\sqrt{2}},$$

pomiar $|\psi\rangle \;=\; |1\rangle$ w diagonalnej bazie daje taki sam wynik jak wyżej.

[1] Stany $|0\rangle$ i $|1\rangle$ mogą być reprezentowane odpowiednio przez fotony o polaryzacji pionowej $|\uparrow\rangle$ i poziomej $|\rightarrow\rangle$, wtedy polaryzacja diagonalna odpowiada stanom $|\nearrow\rangle$ i $|\searrow\rangle$.

Kwantowy protokół uzgodnienia klucza szyfrującego

Klucz szyfrujący — bezpiecznie uzgodniony przez Alicję i Boba ciąg bitów

$$K = (k_1, k_2, \ldots, k_N)$$

Wiadomość od Alicji do Boba $\quad A = (a_1, a_2, \ldots, a_N)$
Szyfrogram $\quad S = (s_1, s_2, \ldots, s_N), \quad s_i = a_i \oplus k_i, \quad i = 1, 2, \ldots N\,.$
Deszyfrowanie $\quad A = S \oplus K, \quad a_i = s_i \oplus k_i\,.$

Problem redukuje się do opracowania metody bezpiecznego uzgodnienia klucza, który można wymieniać po jednorazowym użyciu.

BB84 QUANTUM KEY DISTRIBUTION (Bennet & Brassard, 1984)

Bob losowo decyduje o wyborze bazy zwykłej (+) lub diagonalnej (×), oraz losowo wybiera klasyczny bit 0 lub 1. Dla każdej z 4 możliwości wysyła do Alicji foton w odp. stanie kwantowym

wybrana baza	+	+	×	×
wybrany bit	0	1	0	1
wysłany kubit	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$

Alicja odbiera foton Boba i dokonuje pomiaru w losowo wybranej bazie + lub ×. Dla bazy + ustawia detektor na wykrywanie polaryzacji $|\uparrow\rangle$, a dla bazy × odpowiednio $|\searrow\rangle$. Zapisuje wynik 1, jeśli detektor zarejestrował foton lub 0 w przeciwnym razie. Wszystkie możliwe przypadki to

wybrana baza Boba	+	+	×	×	+	+	×	×
wybrany bit Boba	0	1	0	1	0	1	0	1
wysłany kubit	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$
wybrana baza Alicji	+	+	+	+	×	×	×	×
wynik Alicji	0	1	$*$	$*$	$*$	$*$	0	1

Wynik "$*$" to 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$.

Bob i Alicja powtarzają tą procedurę $4N$ razy, po czym komunikują sobie nawzajem ciągi wybranych baz. Każde z nich może wówczas stwierdzić dla których fotonów wybrane bazy były identycznie. Są wtedy pewni, które z wyników zapisanych przez Alicję powinny być identyczne z wartościami bitów wybranych przez Boba. Średnio mają więc $2N$ zgodnych bitów i znają ich pozycje w ciągu.

W kolejnym kroku Alicja wybiera połowę z nich (N) i przesyła Bobowi ich pozycje i wartości, a Bob przesyła jej swoje wartości tych bitów. Wszystkie powinny być zgodne. W tym wypadku N pozostałych nieujawnionych bitów służy jako klucz szyfrujący.

Jeśli komunikacja byłaby przechwytywana przez podsłuchującą Ewę, chcąc się dowiedzieć o tym jakie kubity wysyła Bob, musiałaby wykonywać ich pomiary w przypadkowo wybranych bazach. Jeśli w danym momencie bazy Boba i Alicji byłyby zgodne, Ewa z prawdopodobieństwem $\frac{1}{2}$ mogłaby wybrać niewłaściwą bazę i wykonując pomiar zmienić stan fotonu. Np. gdy Bob i Alicja używają bazy $+$, a wysłany foton to $|\uparrow\rangle$, Ewa wykonując pomiar w źle wybranej bazie zarejestruje $|\nearrow\rangle$ lub $|\searrow\rangle$ z prawdopodobieństwem $\frac{1}{2}$. Do Alicji dotrze wówczas foton w jednym z tych stanów diagonalnych, więc jej pomiar w bazie $+$ zwróci $|\uparrow\rangle$ lub $|\rightarrow\rangle$ z prawdopodobienstwem $\frac{1}{2}$. Oznacza to, że w $\frac{1}{4}$ przypadków otrzyma ona foton $|\rightarrow\rangle$, którego nie zarejestruje jej detektor, mimo iż Bob nadał $|\uparrow\rangle$. Bity Boba i Alicji nie będą wtedy zgodne mimo wyboru tych samych baz. Jeśli więc zauważalna frakcja ujawnianych w trzecim kroku protokołu N bitów nie jest zgodna, zachodzi podejrzenie naruszenia tajności komunikacji. Bity są wymazywane i procedura rozpoczyna się od początku.

Kwantowy algorytm faktoryzacji Shora

Przypomnienie: $N = pq$, p i q to duże liczby pierwsze i chcemy je znaleźć.

Algorytm korzysta z prostego do udowodnienia faktu, że jeśli wybrana losowo liczba $x < N$ jest względnie pierwsza z N, to prawdopodobieństwo tego, że jej rząd r jest parzysty wynosi co najmniej $\frac{3}{4}$.

Na podstawie tw. Eulera $x^{\varphi(N)} = 1 \pmod N$, czyli x ma rząd $r \leq \varphi(N)$. Przy tym r jest podzielnikiem $\varphi(N)$. Tak więc łatwo jest wylosować x o parzystym rzędzie $r = 2s$, a więc $(x^s)^2 = 1 \pmod N$. Stąd

$$(x^s)^2 - 1 = 0 \pmod N \quad \Rightarrow \quad (x^s + 1)(x^s - 1) = kN = kpq$$

Zatem jedna z liczb $x^s + 1$ lub $x^s - 1$ ma podzielnik p lub q. Wyjątek stanowi przypadek, gdy $x^s = \pm 1 \pmod N$. Nie może to być $x^s = 1$ bo $2s$ jest rzędem x, a więc $x^s = -1 = N - 1 \pmod N$. Wtedy $k = 0$ i metoda nie działa. Na szczęście to też jest sytucja rzadka. Algorytm faktroryzacji z wykorzystaniem rzędu elementu x jest następujący:

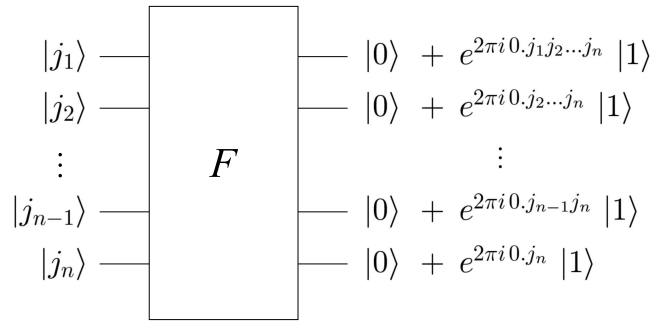
1. Wylosuj $x < N$ i sprawdź czy $\mathrm{NWP}(x, N) = 1$ (algorytm Euklidesa).
2. Oblicz rząd elementu x, czyli min r takie, że $x^r = 1 \pmod N$.
3. Jeśli r jest nieparzyste lub gdy $x^{r/2} = N - 1 \pmod N$ wróć do 1.
4. Oblicz p lub q jako $\mathrm{NWP}(x^s + 1, N)$ lub $\mathrm{NWP}(x^s - 1, N)$ (znowu algorytm Euklidesa).

Problemem jest p. 2: nie umiemy klasycznie obliczać szybko rzędu elementu. Algorytm Shora pokazuje jak zrobić to na kwantowym komputerze. Wykorzystuje w tym celu 2 moduły: kwantową transformatę Fouriera i estymator fazy. Dla każdego z nich podany jest szczegółowy opis w postaci odp. układu elementarnych bramek kwantowych.

Transformata Fouriera

$$|j\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i\, jk/N}\ |k\rangle \ , \qquad j = 0, 1, \ldots N-1 \, ,$$

gdzie $|j\rangle = |j_1 j_2 \ldots j_n\rangle$ rozwinięcie binarne. Więc $N = 2^n$ jest na ogół za duże do efektywnych obliczeń klasycznych.

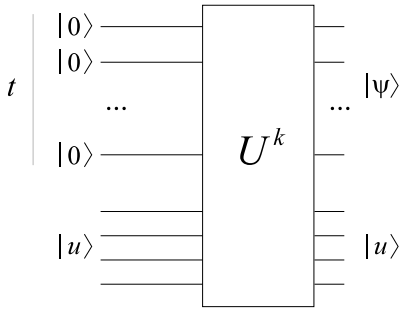


$0.j_1 j_2 \ldots j_n$ oznacza binarny ułamek o cyfrach j_i. Liczba elementarnych bramek w F jest rzędu n^2.

Drugi układ to tzw. estymator fazy

$$U\ |u\rangle\ =\ e^{2\pi i\,\phi}\ |u\rangle$$

Należy znaleźć dostatecznie dobre przybliżenie ułamka ϕ.



$|\psi\rangle$ ma postać iloczynu tensorowego czynników

$$\frac{1}{\sqrt{2}}\left(\,|0\rangle\ +\ e^{2\pi i\, 2^m \phi}\ |1\rangle\,\right)$$

gdzie $m = 0, 1, ..., t-1$. W tych czynnikach, tak jak w wyniku tranformaty Fouriera mamy poprzesuwane binarne t-cyfrowe przybliżenie ułamka ϕ. Odwrotna transformata Fouriera robi z tego wektor

$$|\phi_0 \phi_1 \ldots \phi_{t-1}\rangle$$

Mierząc qubity otrzymujemy binarny ułamek $0.\phi_0 \phi_1 \ldots \phi_{t-1}$.

Operator U którego fazę zamierzamy estymować ma rozmiar $n \times n$, gdzie $n = \lceil \log_2 N \rceil$, i postać

$$U \ |y\rangle \ = \ |xy \ (\mathrm{mod}\ N)\rangle$$

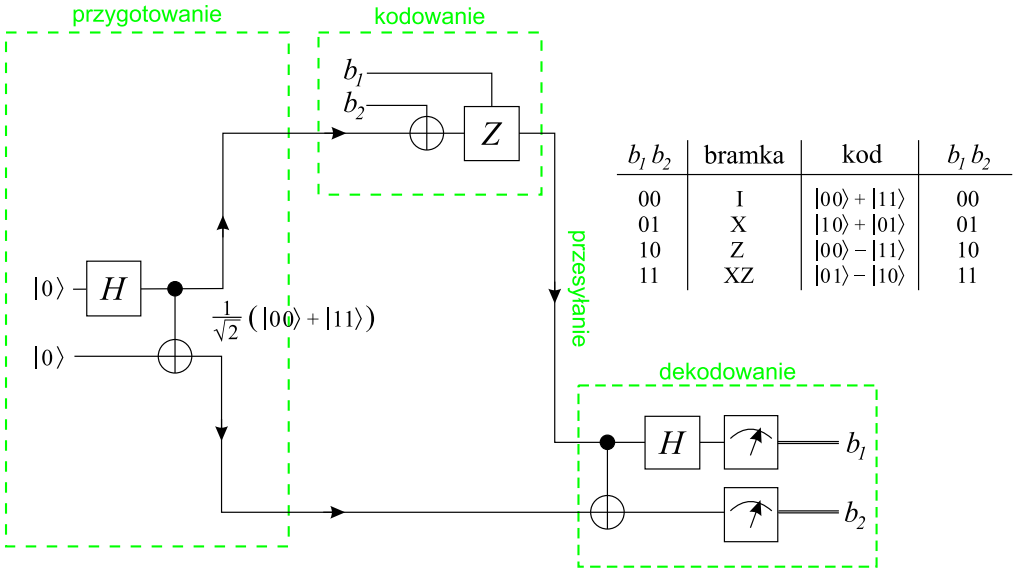
Jego wektory własne $|u_s\rangle$ mają fazy $\phi_s = \frac{s}{r}$ gdzie r jest rzędem liczby x mod N. Otrzymujemy więc z pomiarów binarne przybliżenia liczb $\frac{s}{r}$, z których już klasycznymi metodami można odczytać r.

Gęste kodowanie

Gęste kodowanie polega na transmisji 2 klasycznych bitów przy pomocy 1 qubitu. "Kanał" transmisyjny między Alicją i Bobem zawiera splątaną parę qubitów, jeden w posiadaniu Alicji, drugi — Boba (faza przygotowania),

$$\psi_{00} \;=\; \frac{1}{\sqrt{2}}\,(\,|0_A 0_B\rangle \;+\; |1_A 1_B\rangle\,)\;,$$

którą uzyskuje się działając kombinacją bramek H i $CNOT$ na parę $|00\rangle$.



$b_1\,b_2$	bramka	kod	$b_1\,b_2$
00	I	$\|00\rangle + \|11\rangle$	00
01	X	$\|10\rangle + \|01\rangle$	01
10	Z	$\|00\rangle - \|11\rangle$	10
11	XZ	$\|01\rangle - \|10\rangle$	11

- Kodowanie: Na swoim qubicie Alicja wykonuje jedną z operacji I, X, Z, XZ zależnie od wartości klasycznych bitów b_1 i b_2, które zamierza przesłać do Boba. Qubit Boba pozostaje niezmieniony, więc odpowiada to wykonianiu jednej z operacji na całym układzie $K_{b_1 b_2} = X^{b_2} Z^{b_1} \otimes I$, której wynikiem jest jeden ze stanów Bella

  $$K_{00}\psi_{00} = \psi_{00}, \quad K_{01}\psi_{00} = \psi_{01}, \quad K_{10}\psi_{00} = \psi_{10}, \quad K_{11}\psi_{00} = \psi_{11}\,,$$

  czyli odpowiednio

  $$\psi_{01} = \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \quad \psi_{10} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad \psi_{11} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}\,.$$

- Transmisja: Alicja przesyła swój qubit do Boba

- Dekodowanie: Bob wykonuje operację D odwrotną do generowania ψ_{00}

  $$D \;=\; (H \otimes I)CNOT)^{-1} \;=\; CNOT^{-1}(H \otimes I)^{-1} \;=\; CNOT(H \otimes I)\,,$$

  która produkuje $|00\rangle = D\psi_{00}$, $|01\rangle = D\psi_{01}$, $|10\rangle = D\psi_{10}$, $|11\rangle = D\psi_{11}$, odczytywane przez Boba w procesie pomiaru obydwu qubitów.