Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

http://zon8.physd.amu.edu.pl/~tanas

Wykład 13

Spis treści

19 Algorytmy kwantowe

19.1 Bit kwantowy — kubit (qubit)

- Klasyczny bit może przyjmować dwie wartości $\{0, 1\}$.
- Układ kwantowy, który ma dwa możliwe stany $\{|0\rangle, |1\rangle\}$ może się znajdować w każdym z nich, ale także w stanie będącym syperpozycją stanów bazowych

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

  i taki stan nazywamy kubitem.
- Oznacza to, że z prawdopodobieństwem $p_0 = |a|^2$ układ znajduje się w stanie $|0\rangle$ i z prawdopodobieństwem $p_1 = |b|^2$ w stanie $|1\rangle$, oczywiście $p_0 + p_1 = 1$. Stan układu kwantowego możemy przedstawić jako wektor na sferze Blocha

19 Algorytmy kwantowe

19.1 Bit kwantowy — kubit (qubit)

- Klasyczny bit może przyjmować dwie wartości $\{0, 1\}$.
- Układ kwantowy, który ma dwa możliwe stany $\{|0\rangle, |1\rangle\}$ może się znajdować w każdym z nich, ale także w stanie będącym syperpozycją stanów bazowych

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

  i taki stan nazywamy kubitem.
- Oznacza to, że z prawdopodobieństwem $p_0 = |a|^2$ układ znajduje się w stanie $|0\rangle$ i z prawdopodobieństwem $p_1 = |b|^2$ w stanie $|1\rangle$, oczywiście $p_0 + p_1 = 1$. Stan układu kwantowego możemy przedstawić jako wektor na sferze Blocha

19 Algorytmy kwantowe

19.1 Bit kwantowy — kubit (qubit)

- Klasyczny bit może przyjmować dwie wartości $\{0, 1\}$.
- Układ kwantowy, który ma dwa możliwe stany $\{|0\rangle, |1\rangle\}$ może się znajdować w każdym z nich, ale także w stanie będącym syperpozycją stanów bazowych

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

  i taki stan nazywamy kubitem.

- Oznacza to, że z prawdopodobieństwem $p_0 = |a|^2$ układ znajduje się w stanie $|0\rangle$ i z prawdopodobieństwem $p_1 = |b|^2$ w stanie $|1\rangle$, oczywiście $p_0 + p_1 = 1$. Stan układu kwantowego możemy przedstawić jako wektor na sferze Blocha

19 Algorytmy kwantowe

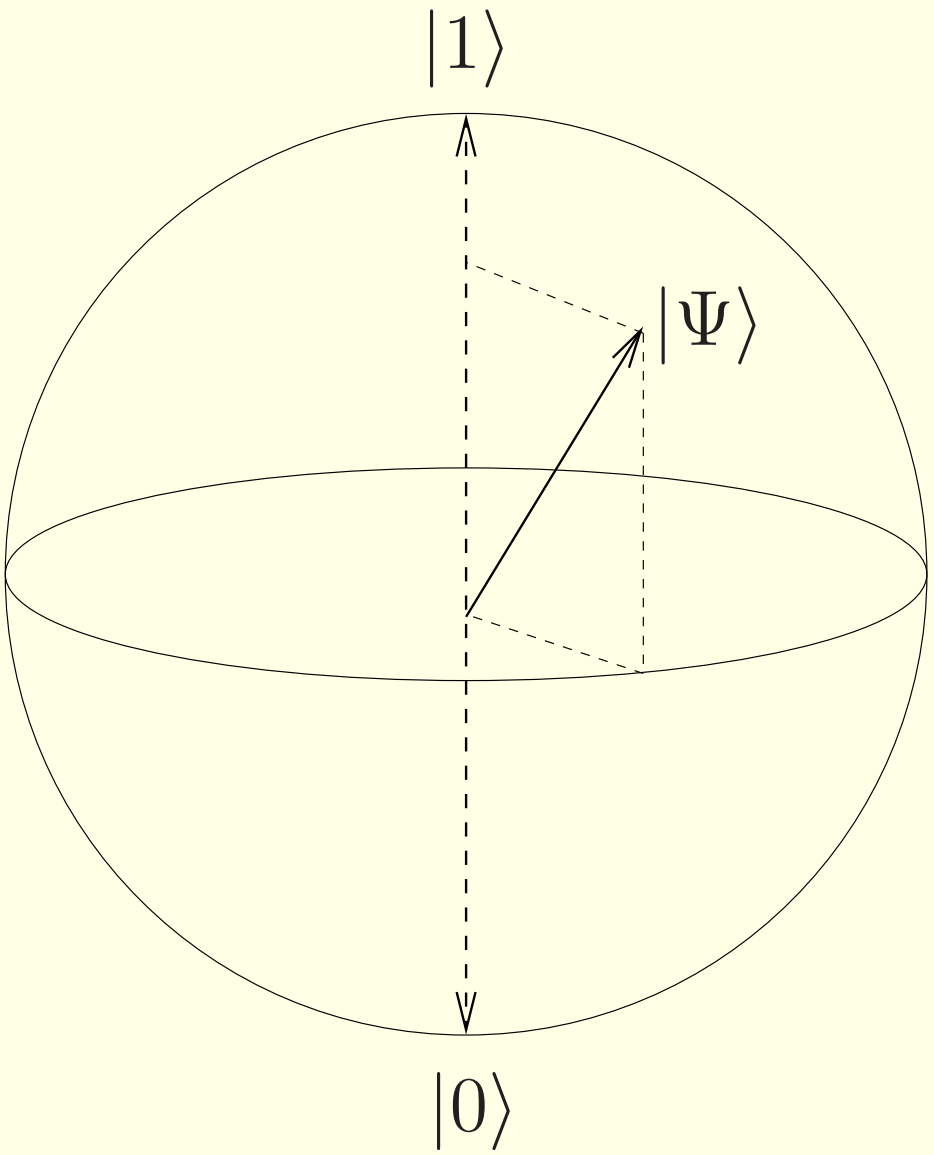
19.1 Bit kwantowy — kubit (qubit)

- Klasyczny bit może przyjmować dwie wartości $\{0, 1\}$.
- Układ kwantowy, który ma dwa możliwe stany $\{|0\rangle, |1\rangle\}$ może się znajdować w każdym z nich, ale także w stanie będącym syperpozycją stanów bazowych

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

  i taki stan nazywamy kubitem.

- Oznacza to, że z prawdopodobieństwem $p_0 = |a|^2$ układ znajduje się w stanie $|0\rangle$ i z prawdopodobieństwem $p_1 = |b|^2$ w stanie $|1\rangle$, oczywiście $p_0 + p_1 = 1$. Stan układu kwantowego możemy przedstawić jako wektor na sferze Blocha



Kubit na sferze Blocha

19.2 Twierdzenie o nieklonowaniu

- Nie istnieje transformacja unitarna U taka, że

$$U|\Psi\rangle|0\rangle \quad = \quad |\Psi\rangle|\Psi\rangle$$

dla dowolnego $|\Psi\rangle$.

- Dowód:
Przypuśćmy, że istnieje U takie, że

$$\begin{aligned} U|\Psi\rangle|0\rangle &= |\Psi\rangle|\Psi\rangle \\ U|\Phi\rangle|0\rangle &= |\Phi\rangle|\Phi\rangle \end{aligned}$$

dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$.

- Transformacja U reprezentowała by maszynę klonującą, gdyby taka istniała.

19.2 Twierdzenie o nieklonowaniu

- Nie istnieje transformacja unitarna U taka, że

$$U|\Psi\rangle|0\rangle \quad = \quad |\Psi\rangle|\Psi\rangle$$

dla dowolnego $|\Psi\rangle$.

- Dowód:
Przypuśćmy, że istnieje U takie, że

$$\begin{aligned} U|\Psi\rangle|0\rangle &= |\Psi\rangle|\Psi\rangle \\ U|\Phi\rangle|0\rangle &= |\Phi\rangle|\Phi\rangle \end{aligned}$$

dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$.

- Transformacja U reprezentowała by maszynę klonującą, gdyby taka istniała.

19.2 Twierdzenie o nieklonowaniu

- Nie istnieje transformacja unitarna U taka, że

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$

dla dowolnego $|\Psi\rangle$.

- Dowód:
Przypuśćmy, że istnieje U takie, że

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$
$$U|\Phi\rangle|0\rangle = |\Phi\rangle|\Phi\rangle$$

dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$.

- Transformacja U reprezentowała by maszynę klonującą, gdyby taka istniała.

19.2 Twierdzenie o nieklonowaniu

- Nie istnieje transformacja unitarna U taka, że

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$

dla dowolnego $|\Psi\rangle$.

- Dowód:
Przypuśćmy, że istnieje U takie, że

$$\begin{aligned} U|\Psi\rangle|0\rangle &= |\Psi\rangle|\Psi\rangle \\ U|\Phi\rangle|0\rangle &= |\Phi\rangle|\Phi\rangle \end{aligned}$$

dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$.

- Transformacja U reprezentowała by maszynę klonującą, gdyby taka istniała.

- Z unitarności U wynika jednak, że

$$\begin{aligned} \langle\Psi|\langle 0|U^\dagger U|\Phi\rangle|0\rangle &= \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle \\ \langle\Psi|\Phi\rangle\langle 0|0\rangle &= \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle \end{aligned}$$

  co nie jest prawdziwe dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$, natomiast może zachodzić dla stanów ortogonalnych $\langle\Psi|\Phi\rangle = \{0, 1\}$.

- Stany ortogonalne (klasyczne bity) mogą być kopiowane, natomiast dowolne stany kwantowe nie.

- Z unitarności U wynika jednak, że

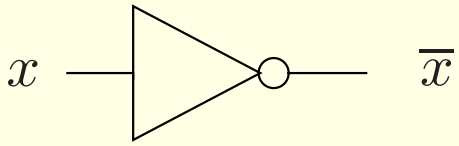
$$\begin{aligned} \langle\Psi|\langle 0|U^\dagger U|\Phi\rangle|0\rangle &= \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle \\ \langle\Psi|\Phi\rangle\langle 0|0\rangle &= \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle \end{aligned}$$

  co nie jest prawdziwe dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$, natomiast może zachodzić dla stanów ortogonalnych $\langle\Psi|\Phi\rangle = \{0, 1\}$.

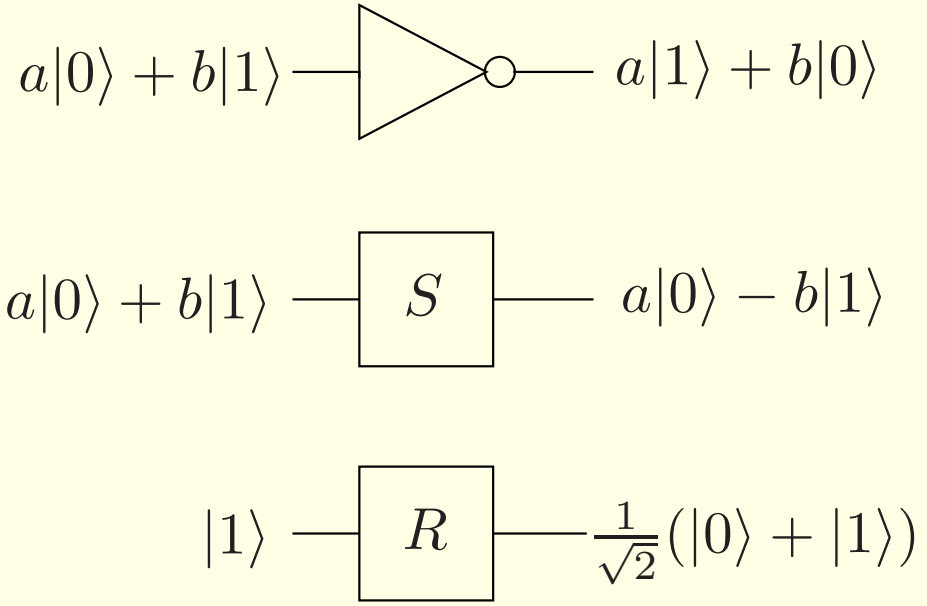
- Stany ortogonalne (klasyczne bity) mogą być kopiowane, natomiast dowolne stany kwantowe nie.

19.3 Bramki logiczne

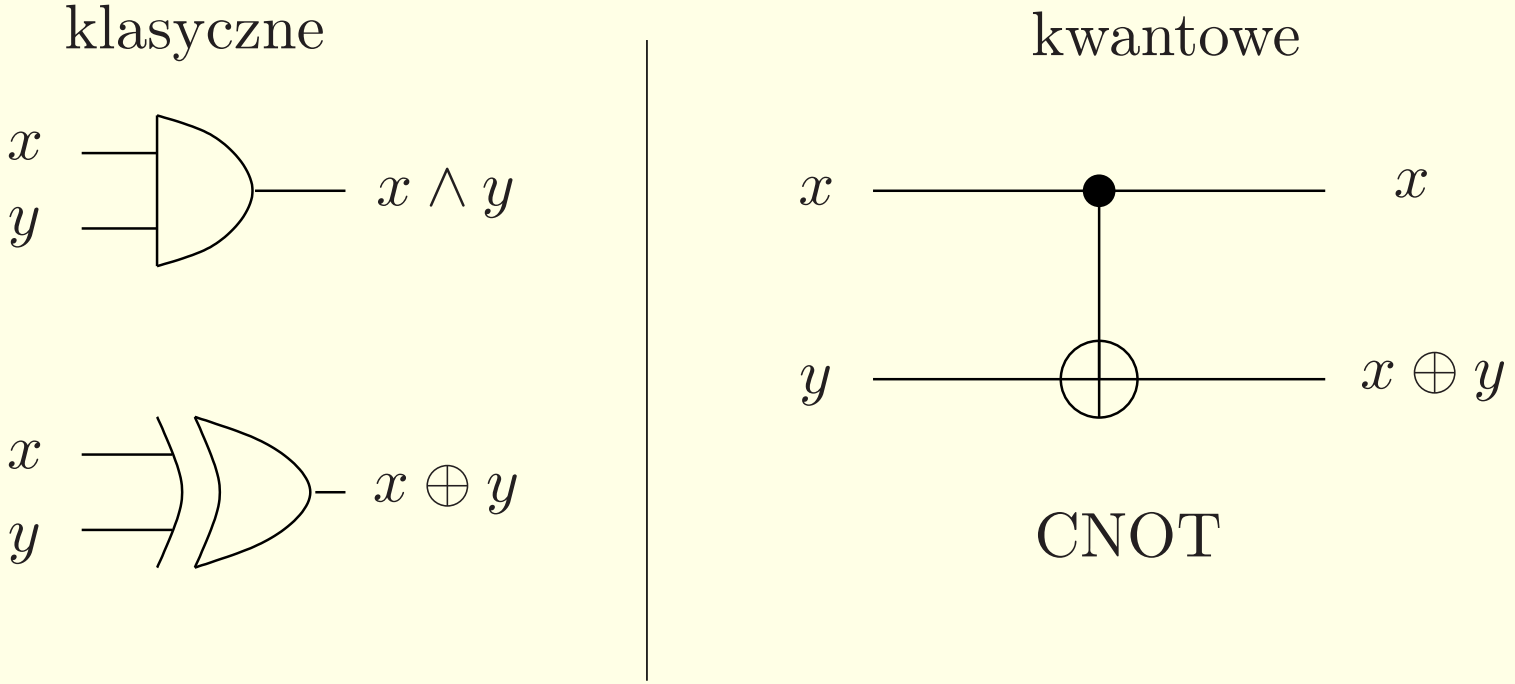
klasyczne



kwantowe



Jednobitowe bramki logiczne



Dwubitowe bramki logiczne

- W bazie stanów $\{|0\rangle, |1\rangle\}$, mamy

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Wtedy operacje na stanach kwantowych mają reprezentację macierzową, i tak na przykład

$$U_{\mathrm{NOT}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$U_{\mathrm{NOT}}|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

- W bazie stanów $\{|0\rangle, |1\rangle\}$, mamy

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Wtedy operacje na stanach kwantowych mają reprezentację macierzową, i tak na przykład

$$U_{\mathrm{NOT}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$U_{\mathrm{NOT}}|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

- Operacja przesunięcia fazy, która nie zmienia stanu $|0\rangle$ zaś stan $|1\rangle$ zmienia na $-|1\rangle$, ma postać

$$U_S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Operacja Hadamarda, czasem nazywana pierwiastkiem kwadratowym z NOT ($\sqrt{\text{NOT}}$), ma postać

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

- Operacja przesunięcia fazy, która nie zmienia stanu $|0\rangle$ zaś stan $|1\rangle$ zmienia na $-|1\rangle$, ma postać

$$U_S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Operacja Hadamarda, czasem nazywana pierwiastkiem kwadratowym z NOT ($\sqrt{\mathrm{NOT}}$), ma postać

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

- Istnieje nieskończenie wiele bramek kwantowych generowanych przez rotacje o kąt θ

$$U_R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

- oraz przesunięcia faz

$$U_P(\varphi_1, \varphi_2) = \begin{bmatrix} e^{i\varphi_1} & 0 \\ 0 & e^{i\varphi_2} \end{bmatrix}$$

- Istnieje nieskończenie wiele bramek kwantowych generowanych przez rotacje o kąt θ

$$U_R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

- oraz przesunięcia faz

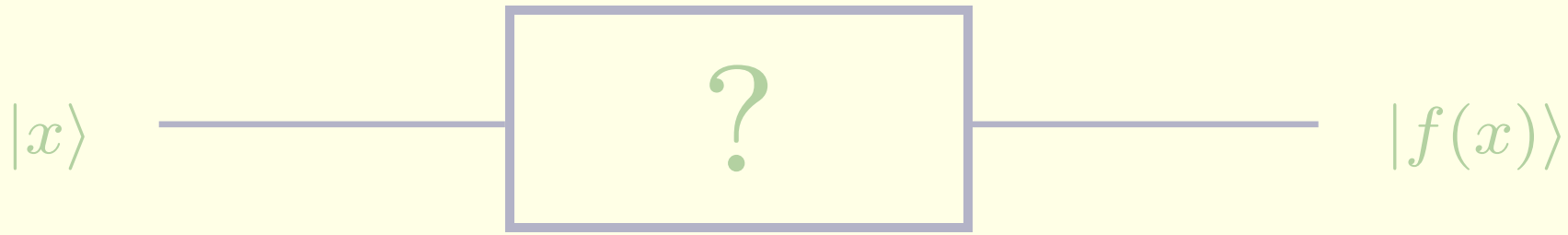
$$U_P(\varphi_1, \varphi_2) = \begin{bmatrix} e^{i\varphi_1} & 0 \\ 0 & e^{i\varphi_2} \end{bmatrix}$$

- Operacja CNOT (kontrolowane NOT) na dwóch kubitach ma postać

$$U_{\mathrm{CN}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

19.4 Problem Deutscha

- Przypuśćmy, że mamy kwantową czarną skrzynkę obliczającą funkcję $f(x)$, tzn. wykonującą transformację unitarną na dwóch kubitach przedstawioną poniżej



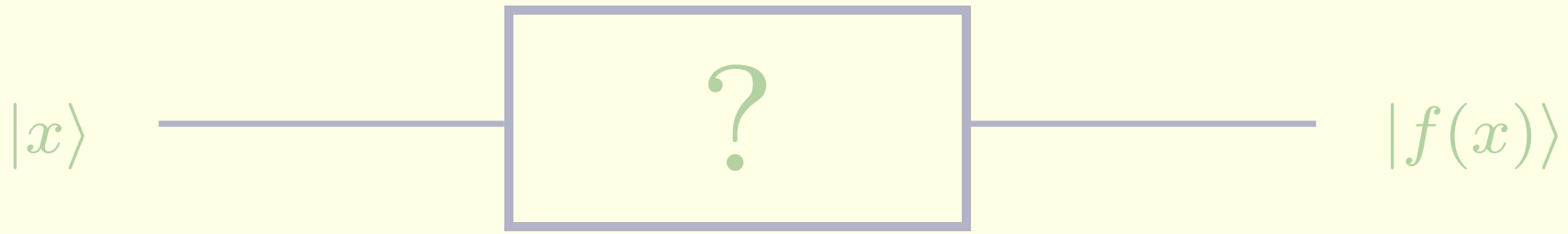
$$f : \{0,1\} \to \{0,1\}$$

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

- Pytanie: Czy po jednym przebiegu kwantowego komputera możemy stwierdzić, że $f(0) = f(1)$?

19.4 Problem Deutscha

- Przypuśćmy, że mamy kwantową czarną skrzynkę obliczającą funkcję $f(x)$, tzn. wykonującą transformację unitarną na dwóch kubitach przedstawioną poniżej



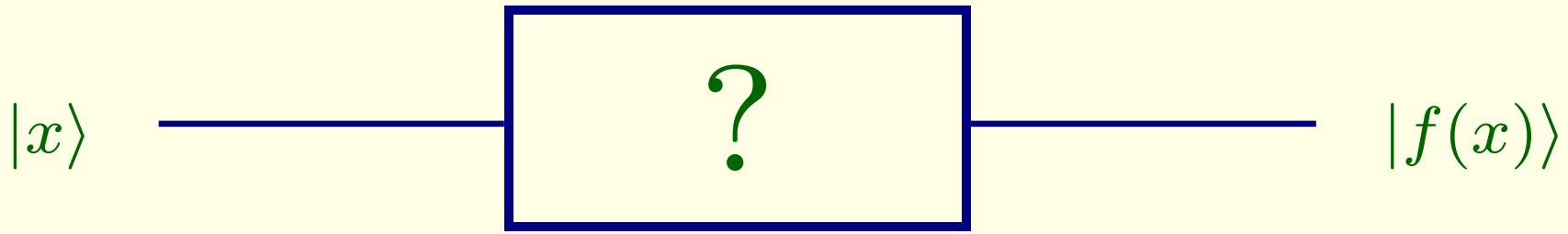
$$f : \{0,1\} \to \{0,1\}$$

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

- Pytanie: Czy po jednym przebiegu kwantowego komputera możemy stwierdzić, że $f(0) = f(1)$?

19.4 Problem Deutscha

- Przypuśćmy, że mamy kwantową czarną skrzynkę obliczającą funkcję $f(x)$, tzn. wykonującą transformację unitarną na dwóch kubitach przedstawioną poniżej



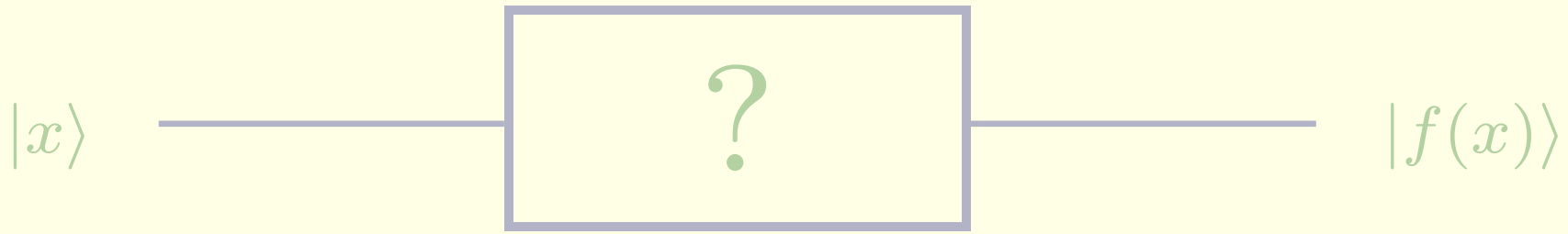
$$f : \{0,1\} \to \{0,1\}$$

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

- Pytanie: Czy po jednym przebiegu kwantowego komputera możemy stwierdzić, że $f(0) = f(1)$?

19.4 Problem Deutscha

- Przypuśćmy, że mamy kwantową czarną skrzynkę obliczającą funkcję $f(x)$, tzn. wykonującą transformację unitarną na dwóch kubitach przedstawioną poniżej

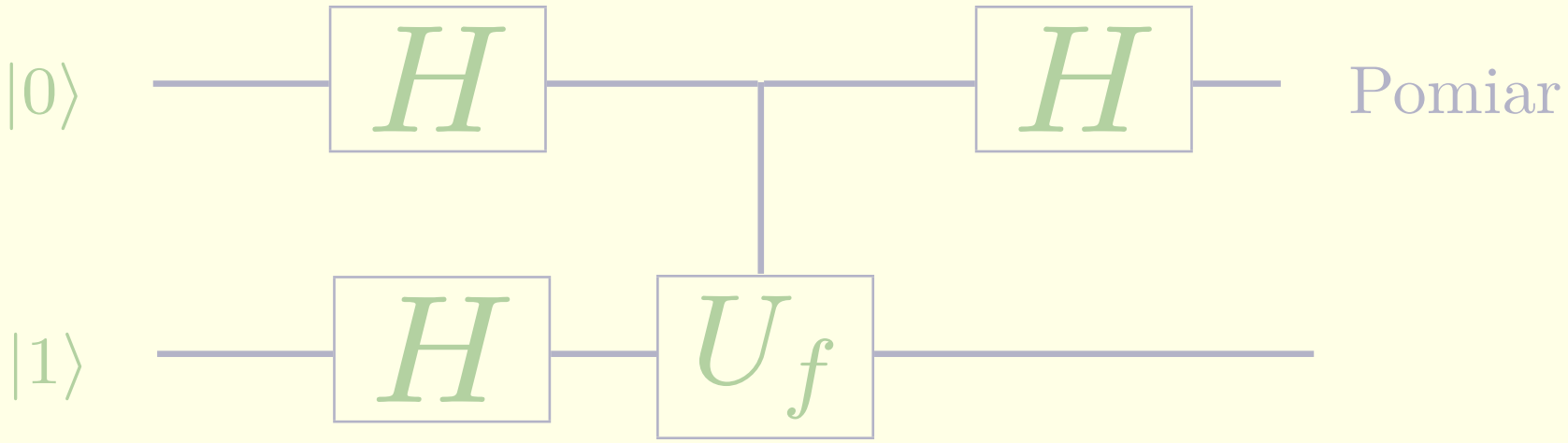


$$f : \{0,1\} \to \{0,1\}$$

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

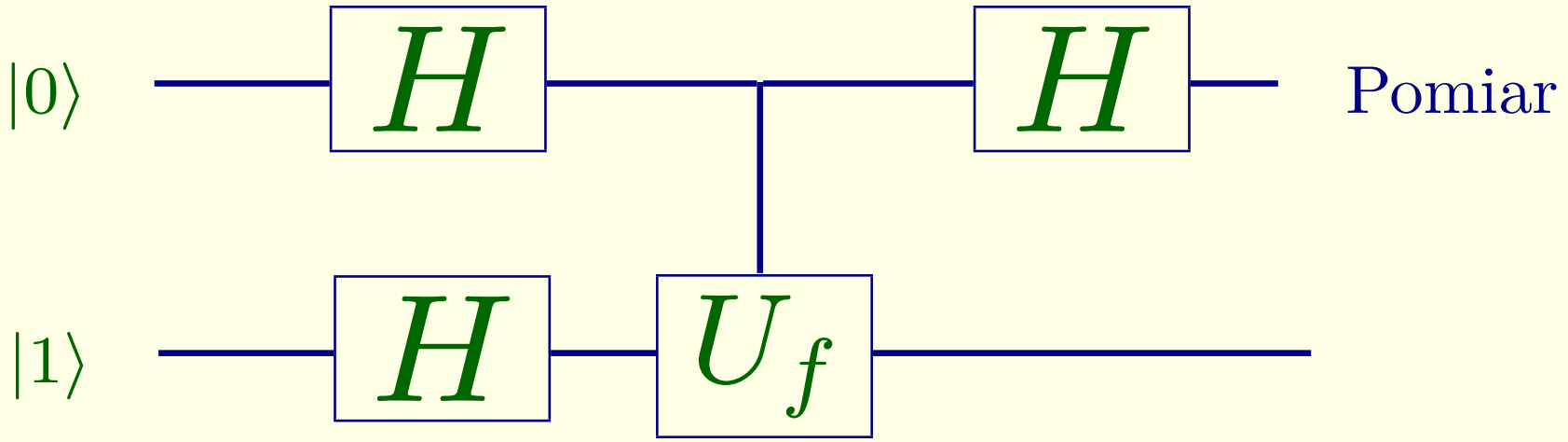
- Pytanie: Czy po jednym przebiegu kwantowego komputera możemy stwierdzić, że $f(0) = f(1)$?

- Weźmy następujący obwód kwantowy



gdzie H jest kwantową bramką Hadamarda.

- Weźmy następujący obwód kwantowy



gdzie $\boxed{H}$ jest kwantową bramką Hadamarda.

19.4.1 Działanie obwodu

$$H : |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

19.4.1 Działanie obwodu

$$H : |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0\rangle|1\rangle \rightarrow \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

19.4.1 Działanie obwodu

$$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0\rangle|1\rangle \to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$\to \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)(|0\rangle - |1\rangle)$$

19.4.1 Działanie obwodu

$$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\begin{aligned}
|0\rangle|1\rangle &\to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\Bigg[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle \\
&\qquad + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\Bigg]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

19.4.1 Działanie obwodu

$$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\begin{aligned}
|0\rangle|1\rangle &\to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\Bigg[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle \\
&\quad + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\Bigg]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

$$|m\rangle = \begin{cases} \pm|0\rangle & \text{dla} \quad f(0) = f(1) \\ \pm|1\rangle & \text{dla} \quad f(0) \neq f(1) \end{cases}$$

19.5 Kwantowy paralelizm

- Przypuśćmy, że mamy funkcję działającą na N bitów o 2^N możliwych wartościach. Aby obliczyć tablicę funkcji $f(x)$ musielibyśmy policzyć wartość funkcji 2^N razy (dla $N = 100$ $\sim 10^{30}$)!
- Na komputerze kwantowym działającym zgodnie z

$$U_f : |x\rangle|0\rangle \quad \rightarrow \quad |x\rangle|f(x)\rangle$$

możemy wybrać stan początkowy (kwantowy rejestr) w postaci

$$|\psi_0\rangle \quad = \quad \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle$$

19.5 Kwantowy paralelizm

- Przypuśćmy, że mamy funkcję działającą na N bitów o 2^N możliwych wartościach. Aby obliczyć tablicę funkcji $f(x)$ musielibyśmy policzyć wartość funkcji 2^N razy (dla $N = 100$ $\sim 10^{30}$)!
- Na komputerze kwantowym działającym zgodnie z

$$U_f : |x\rangle|0\rangle \quad \rightarrow \quad |x\rangle|f(x)\rangle$$

możemy wybrać stan początkowy (kwantowy rejestr) w postaci

$$|\psi_0\rangle \quad = \quad \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle$$

19.5 Kwantowy paralelizm

- Przypuśćmy, że mamy funkcję działającą na N bitów o 2^N możliwych wartościach. Aby obliczyć tablicę funkcji $f(x)$ musielibyśmy policzyć wartość funkcji 2^N razy (dla $N = 100$ $\sim 10^{30}$)!

- Na komputerze kwantowym działającym zgodnie z

$$U_f : |x\rangle|0\rangle \quad \rightarrow \quad |x\rangle|f(x)\rangle$$

możemy wybrać stan początkowy (kwantowy rejestr) w postaci

$$|\psi_0\rangle \quad = \quad \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle$$

i obliczając $f(x)$ tylko raz otrzymujemy stan

$$|\psi\rangle \quad = \quad \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle$$

- Stan ten jest superpozycją wartości funkcji dla wszystkich wartości jej argumentów. Mamy tu do czynienia z kwantowym paralelizmem.

i obliczając $f(x)$ tylko raz otrzymujemy stan

$$|\psi\rangle \quad = \quad \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle$$

- Stan ten jest superpozycją wartości funkcji dla wszystkich wartości jej argumentów. Mamy tu do czynienia z kwantowym paralelizmem.

- Na przykład, dla $N = 2$, stan początkowy może mieć postać

$$|\psi_0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$|00\rangle \to |0\rangle$$
$$|01\rangle \to |1\rangle$$
$$|10\rangle \to |2\rangle$$
$$|11\rangle \to |3\rangle$$

$$|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

- Otrzymujemy superpozycję czterech liczb, na których komputer kwantowy wykonuje operacje w jednym kroku!

- Na przykład, dla $N = 2$, stan początkowy może mieć postać

$$|\psi_0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$|00\rangle \to |0\rangle$$
$$|01\rangle \to |1\rangle$$
$$|10\rangle \to |2\rangle$$
$$|11\rangle \to |3\rangle$$

$$|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

- Otrzymujemy superpozycję czterech liczb, na których komputer kwantowy wykonuje operacje w jednym kroku!

19.6 Algorytm Shora

Rejestr A	Rejestr B
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0

Etap 1. Przygotowujemy rejestr A komputera kwantowego w superpozycji wszystkich możliwych stanów

19.6 Algorytm Shora

Rejestr A	Rejestr B
0	1
1	2
2	4
3	8
4	1
5	2
6	4
7	8
8	1
9	2
10	4
11	8
12	1
13	2
14	4
15	8

Etap 1. Przygotowujemy rejestr A komputera kwantowego w superpozycji wszystkich możliwych stanów

Etap 2. Liczba, którą chcemy sfaktoryzować jest N, $N = 15$. Wybieramy liczbę losową X, $1 < X < N - 1$, $X = 2$. Wykonujemy operację $B = X^A \pmod N$

np. dla $X = 2$ mamy wyniki przedstawione w tabelce

19.6 Algorytm Shora

Rejestr A	Rejestr B
0	1
1	2
2	4
3	8
4	1
5	2
6	4
7	8
8	1
9	2
10	4
11	8
12	1
13	2
14	4
15	8

Etap 1. Przygotowujemy rejestr A komputera kwantowego w superpozycji wszystkich możliwych stanów

Etap 2. Liczba, którą chcemy sfaktoryzować jest N, $N = 15$. Wybieramy liczbę losową X, $1 < X < N - 1$, $X = 2$. Wykonujemy operację $B = X^A \pmod N$
np. dla $X = 2$ mamy wyniki przedstawione w tabelce

Etap 3. Obliczamy $P = X^{f/2} - 1$; $f = 4$ i sprawdzamy czy P jest dzielnikiem N
w naszym przypadku
$P = 2^{4/2} - 1 = 3$,
$P = 2^{4/2} + 1 = 5$;

19.6 Algorytm Shora

Rejestr A	Rejestr B
0	1
1	2
2	4
3	8
4	1
5	2
6	4
7	8
8	1
9	2
10	4
11	8
12	1
13	2
14	4
15	8

Etap 1. Przygotowujemy rejestr A komputera kwantowego w superpozycji wszystkich możliwych stanów

Etap 2. Liczba, którą chcemy sfaktoryzować jest N, $N = 15$. Wybieramy liczbę losową X, $1 < X < N - 1$, $X = 2$. Wykonujemy operację $B = X^A \pmod N$

np. dla $X = 2$ mamy wyniki przedstawione w tabelce

Etap 3. Obliczamy $P = X^{f/2} - 1$; $f = 4$ i sprawdzamy czy P jest dzielnikiem N

w naszym przypadku

$P = 2^{4/2} - 1 = 3$,

$P = 2^{4/2} + 1 = 5$;

Hurra !!!

$15/3 = 5$

$15/5 = 3$

19.7 Kwantowa transformata Fouriera

$$QFT : |x\rangle \quad \rightarrow \quad \frac{1}{q} \sum_{y=0}^{q-1} \mathrm{e}^{2\pi i x y / q} |y\rangle$$

gdzie $q = 2^N$

19.7 Kwantowa transformata Fouriera

$$QFT : |x\rangle \quad \rightarrow \quad \frac{1}{q} \sum_{y=0}^{q-1} \mathrm{e}^{2\pi i x y/q} |y\rangle$$

gdzie $q = 2^N$

19.7.1 Okres funkcji

- Przygotowujemy stan

$$|\psi_0\rangle \quad = \quad \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |f(x)\rangle$$

- Mierzymy drugi rejestr dostając $|f(x_0)\rangle$, co powoduje, że pierwszy rejestr staje się superpozycją wszystkich stanów, które dają wartość $f(x_0)$
  (funkcja jest okresowa z okresem r)

$$\frac{1}{\sqrt{a}} \sum_{j=0}^{a-1} |x_0 + jr\rangle \,, \quad a - 1 < \frac{q}{r} < a + 1$$

19.7.1 Okres funkcji

- Przygotowujemy stan

$$|\psi_0\rangle \quad = \quad \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |f(x)\rangle$$

- Mierzymy drugi rejestr dostając $|f(x_0)\rangle$, co powoduje, że pierwszy rejestr staje się superpozycją wszystkich stanów, które dają wartość $f(x_0)$
  (funkcja jest okresowa z okresem r)

$$\frac{1}{\sqrt{a}} \sum_{j=0}^{a-1} |x_0 + jr\rangle \,, \quad a - 1 < \frac{q}{r} < a + 1$$

19.7.1 Okres funkcji

- Przygotowujemy stan

$$|\psi_0\rangle \quad = \quad \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |f(x)\rangle$$

- Mierzymy drugi rejestr dostając $|f(x_0)\rangle$, co powoduje, że pierwszy rejestr staje się superpozycją wszystkich stanów, które dają wartość $f(x_0)$
  (funkcja jest okresowa z okresem r)

$$\frac{1}{\sqrt{a}} \sum_{j=0}^{a-1} |x_0 + jr\rangle \,, \quad a - 1 < \frac{q}{r} < a + 1$$

- Stosujemy QTF

$$\frac{1}{\sqrt{qa}} \sum_{y=0}^{q-1} \mathrm{e}^{2\pi i x_0 y} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j r y/q} |y\rangle$$

$$\mathrm{Prob}(y) = \frac{a}{q} \left| \frac{1}{a} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j r y/q} \right|^2$$

- Jeśli q/r jest całkowite ($q/r = a$), to

$$\mathrm{Prob}(y) = \frac{1}{a} \left| \frac{1}{a} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j y/q} \right|^2 = \begin{cases} \frac{1}{r} & y = a * \text{integer} \\ 0 & \text{otherwise} \end{cases}$$

- Stosujemy QTF

$$\frac{1}{\sqrt{qa}} \sum_{y=0}^{q-1} \mathrm{e}^{2\pi i x_0 y} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j r y/q} |y\rangle$$

$$\mathrm{Prob}(y) = \frac{a}{q} \left| \frac{1}{a} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j r y/q} \right|^2$$

- Jeśli q/r jest całkowite ($q/r = a$), to

$$\mathrm{Prob}(y) = \frac{1}{a} \left| \frac{1}{a} \sum_{j=0}^{a-1} \mathrm{e}^{2\pi i j y/q} \right|^2 = \begin{cases} \frac{1}{r} & y = a * \text{integer} \\ 0 & \text{otherwise} \end{cases}$$