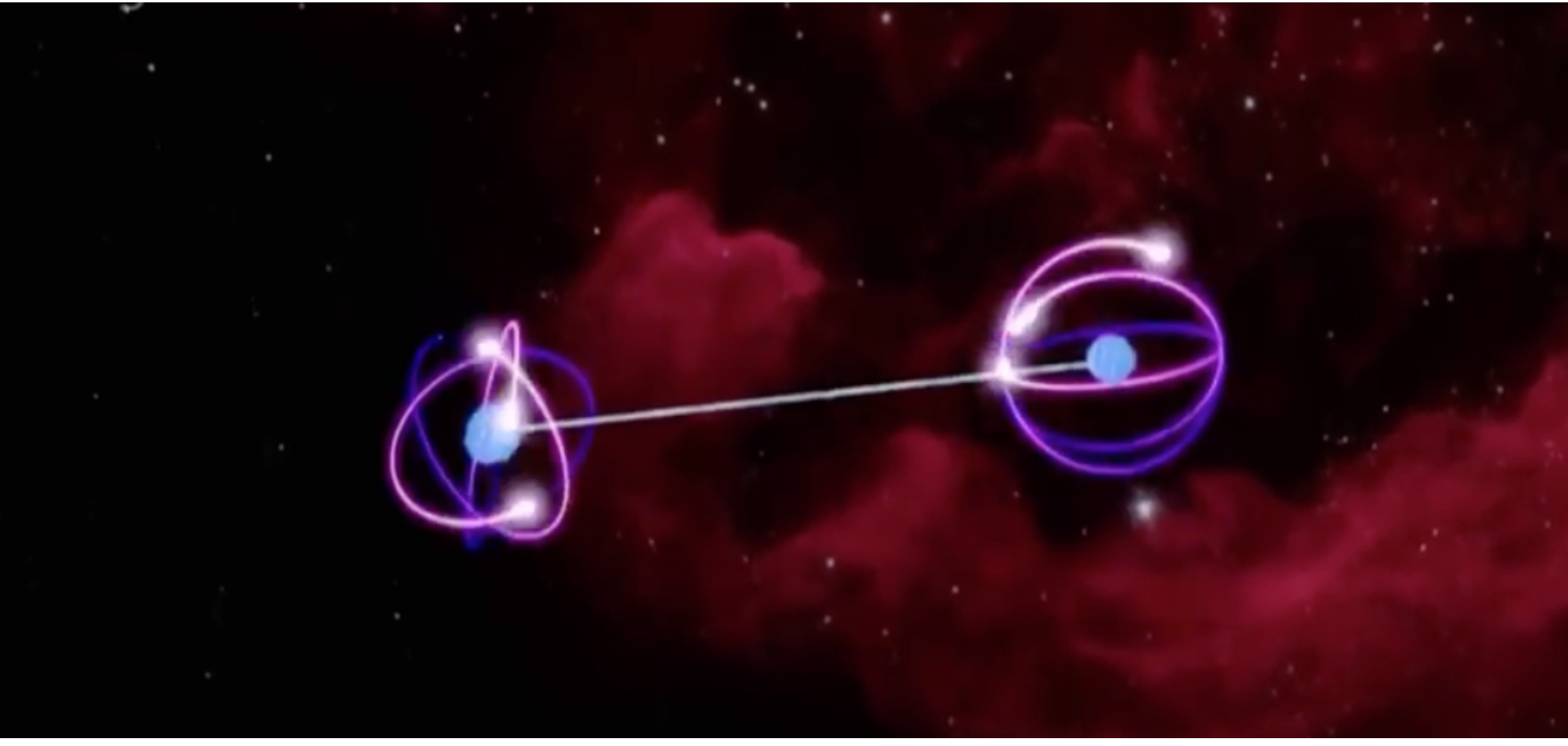
bity kwantowe

zastosowania stanów splątanych

Jacek Matulewski Karolina Słowik Jarosław Zaremba Jacek Jurkowski



Bit jest jednostką informacji

tzn. jest "najmniejszą możliwą porcją informacji": 0 lub 1

Bit jest jednostką informacji

tzn. jest "najmniejszą możliwą porcją informacji": 0 lub 1

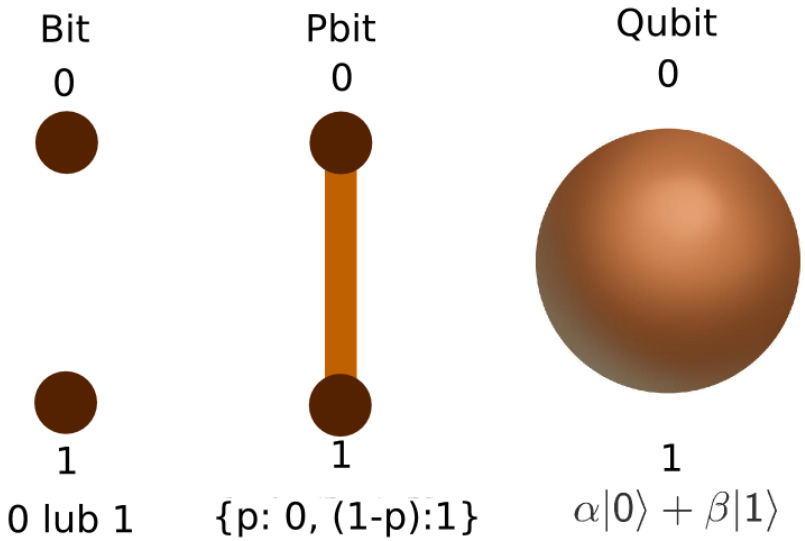
Ile bitów potrzeba żeby podać współrzędne geologiczne?

Bit kwantowy zawiera więcej informacji niż bit klasyczny

- bit klasyczny: 0 lub 1
- bit prawdopodobieństwa:
  0 z prawdop. $p \in [0, 1]$
  1 z prawdop. $1 - p$
- bit kwantowy:

$$\alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

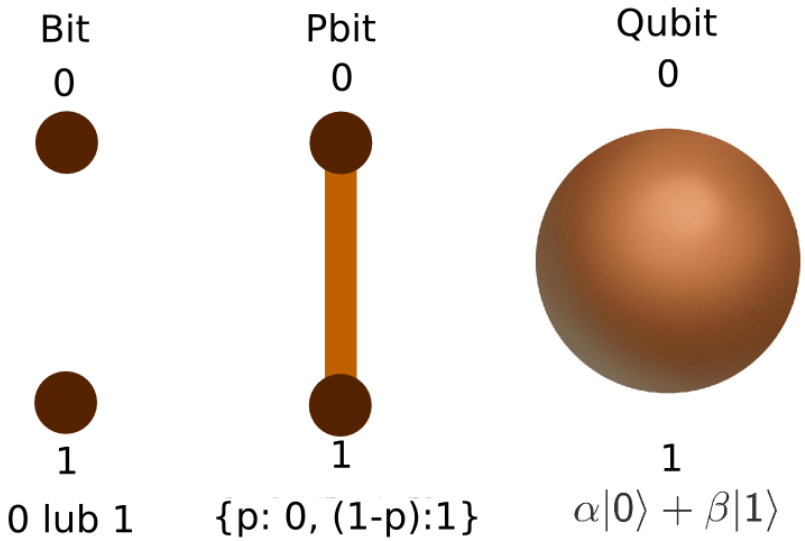


Bit kwantowy zawiera więcej informacji niż bit klasyczny

- bit klasyczny: 0 lub 1
- bit prawdopodobieństwa:
  0 z prawdop. $p \in [0, 1]$
  1 z prawdop. $1 - p$
- bit kwantowy:

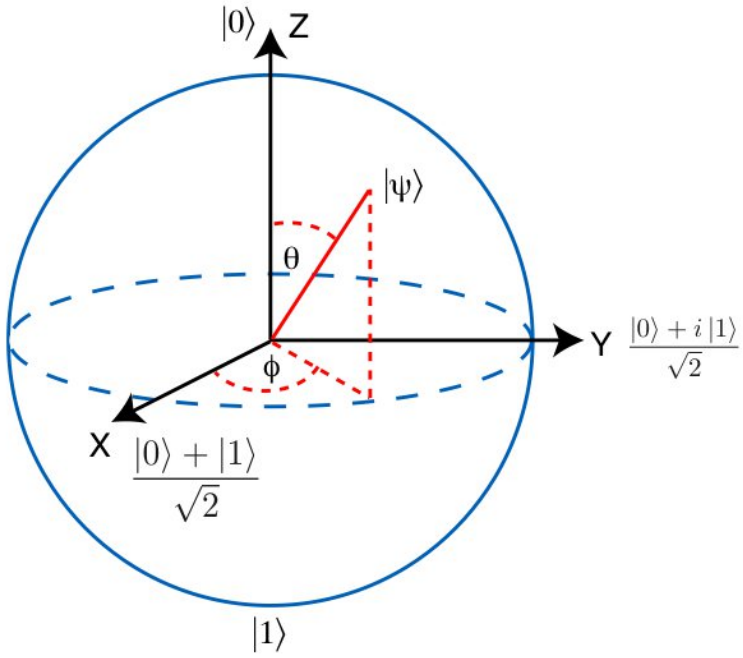
$$\alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$



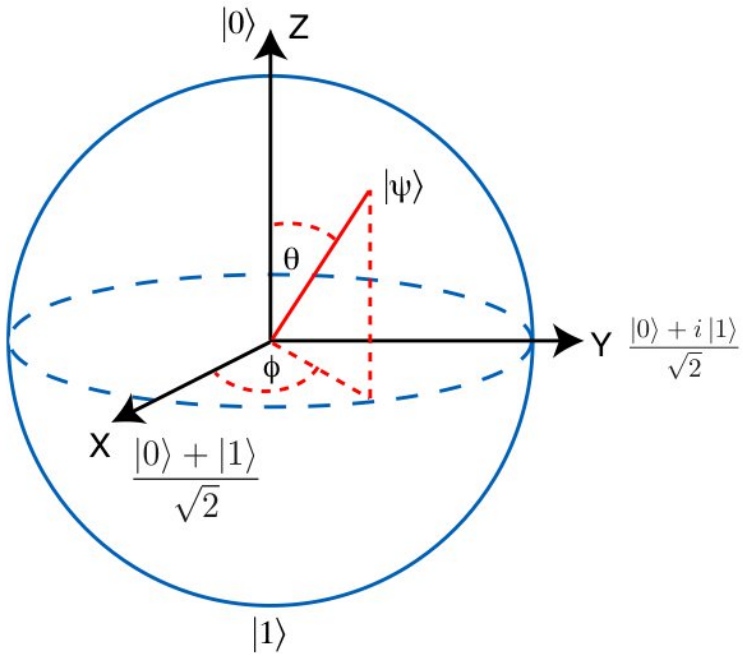
bit kwantowy = kubit (ang. *q-bit*, *quantum bit*)

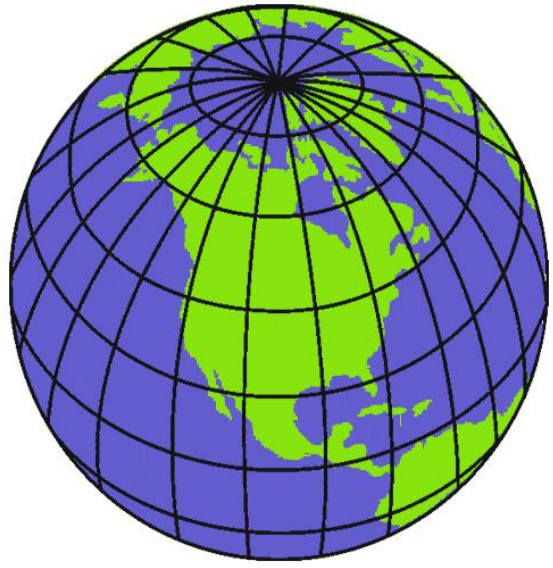
Stan kubitu dany przez parę liczb rzeczywistych



$$\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$$

Stan kubitu dany przez parę liczb rzeczywistych





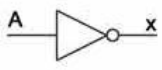
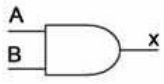
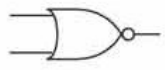
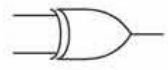
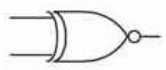
... zupełnie jak współrzędne na powierzchni Ziemi

Dowolny układ dwustanowy może kodować kubit

- polaryzacja fotonu $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$
- foton poruszający się jedną z dwóch dróg $\alpha|\text{droga } 1\rangle + \beta|\text{droga } 2\rangle$
- dwa wybrane poziomy w atomie $\alpha|\text{podstawowy}\rangle + \beta|\text{wzbudzony}\rangle$
- azot po lewej lub prawej stronie względem płaszczyzny wodorów w amoniaku $\alpha|\text{lewa}\rangle + \beta|\text{prawa}\rangle$
- rotacja cząstki w lewo lub w prawo $\alpha|\circlearrowleft\rangle + \beta|\circlearrowright\rangle$
- prąd nadprzewodnictwa płynący w lewo lub w prawo $\alpha|\leftarrow\rangle + \beta|\rightarrow\rangle$
- ...

W ogólności zapisujemy $\alpha|0\rangle + \beta|1\rangle$.

Klasyczne bramki logiczne

Name	NOT	AND	NAND	OR	NOR	XOR	XNOR
Alg. Expr.	$\overline{A}$	AB	$\overline{AB}$	$A+B$	$\overline{A+B}$	$A \oplus B$	$\overline{A \oplus B}$
Symbol							
Truth Table	A | X 0 | 1 1 | 0	B A | X 0 0 | 0 0 1 | 0 1 0 | 0 1 1 | 1	B A | X 0 0 | 1 0 1 | 1 1 0 | 1 1 1 | 0	B A | X 0 0 | 0 0 1 | 1 1 0 | 1 1 1 | 1	B A | X 0 0 | 1 0 1 | 0 1 0 | 0 1 1 | 0	B A | X 0 0 | 0 0 1 | 1 1 0 | 1 1 1 | 0	B A | X 0 0 | 1 0 1 | 0 1 0 | 0 1 1 | 1

Kwantowe bramki logiczne działają zarówno na stany bazowe, jak i na ich superpozycje

Klasyczna bramka zaprzeczenia:

$$\mathrm{NOT}(0) = 1,\ \mathrm{NOT}(1) = 0$$

Kwantowa bramka zaprzeczenia:

$$\mathrm{NOT}|0\rangle = |1\rangle,\ \mathrm{NOT}|1\rangle = |0\rangle$$

ale również:

$$\mathrm{NOT}\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha\mathrm{NOT}|0\rangle + \beta\mathrm{NOT}|1\rangle = \alpha|1\rangle + \beta|0\rangle$$

Kwantowe bramki logiczne

- Bramka NOT działa na pojedynczy kubit.
- Inne bramki jednokubitowe:
  bramka fazowa zmienia znak superpozycji

$$\mathrm{PHASE}|0\rangle = |0\rangle,\ \mathrm{PHASE}|1\rangle = -|1\rangle$$
$$\mathrm{PHASE}\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle - \beta|1\rangle$$

  bramka Hadamarda tworzy superpozycje

$$\mathrm{H}|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}},\ \mathrm{H}|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Zadanie domowe:
znajdź działanie bramki Hadamarda na stany $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ i $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

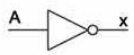
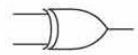
Jednokubitowe kwantowe bramki logiczne

$$
\begin{aligned}
\mathrm{NOT}\,(\alpha|0\rangle + \beta|1\rangle) &= \alpha|1\rangle + \beta|0\rangle \\
\mathrm{PHASE}\,(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle - \beta|1\rangle \\
\mathrm{H}\,(\alpha|0\rangle + \beta|1\rangle) &= \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}
$$

Operacje kwantowe są **odwracalne**

tzn. znając wyjście potrafimy odtworzyć wejście.

- dwubitowe bramki klasyczne nie są odwracalne

Name	NOT	AND	NAND	OR	NOR	XOR	XNOR
Alg. Expr.	$\overline{A}$	AB	$\overline{AB}$	$A+B$	$\overline{A+B}$	$A \oplus B$	$\overline{A \oplus B}$
Symbol							
Truth Table	A X: 0 1; 1 0	B A X: 0 0 0; 0 1 0; 1 0 0; 1 1 1	B A X: 0 0 1; 0 1 1; 1 0 1; 1 1 0	B A X: 0 0 0; 0 1 1; 1 0 1; 1 1 1	B A X: 0 0 1; 0 1 0; 1 0 0; 1 1 0	B A X: 0 0 0; 0 1 1; 1 0 1; 1 1 0	B A X: 0 0 1; 0 1 0; 1 0 0; 1 1 1

- warunek konieczny odwracalności:
  ta sama liczba kubitów na wejściu i na wyjściu

Przykłady bramek dwukubitowych (tzw. bramki sterowane)

sterowane zaprzeczenie CNOT

$$|00\rangle \to |00\rangle$$

$$|01\rangle \to |01\rangle$$

$$|10\rangle \to |11\rangle$$

$$|11\rangle \to |10\rangle$$

Przykłady bramek dwukubitowych (tzw. bramki sterowane)

sterowana zmiana fazy CPHASE

$$|00\rangle \to |00\rangle$$

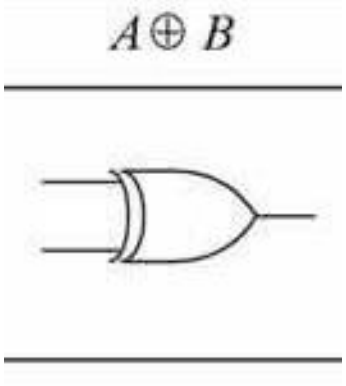
$$|01\rangle \to |01\rangle$$

$$|10\rangle \to |10\rangle$$

$$|11\rangle \to -|11\rangle$$

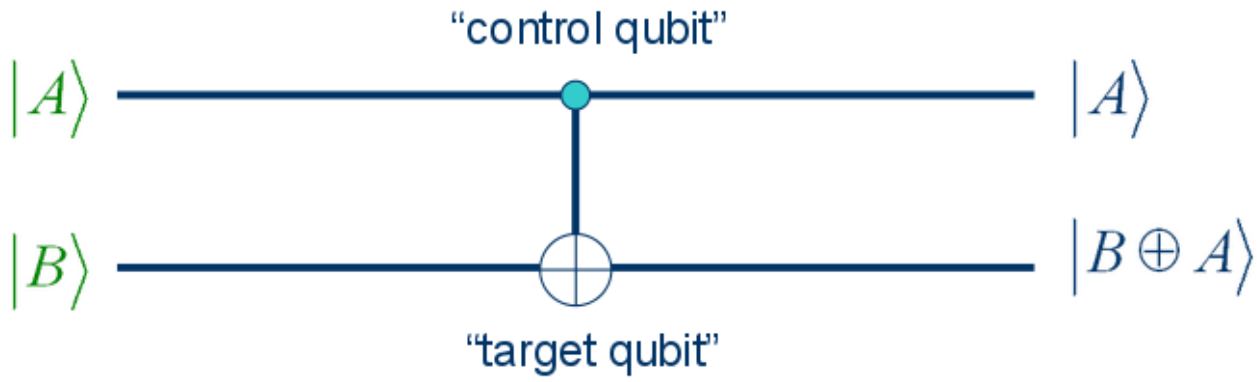
Klasyczny XOR a kwantowy CNOT

XOR



$00 \to 0$
$01 \to 1$
$10 \to 1$
$11 \to 0$

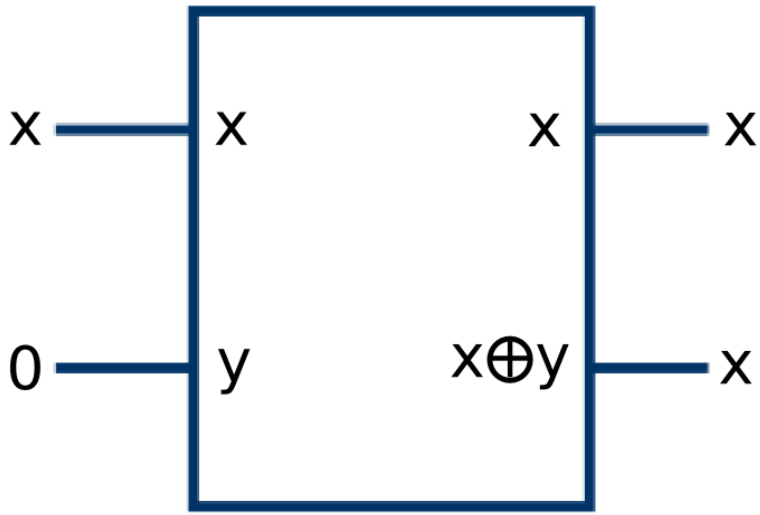
CNOT



$|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$
$|10\rangle \to |11\rangle$
$|11\rangle \to |10\rangle$

Powielanie bitu

Klasyczna bramka XOR pozwala powielić bit:

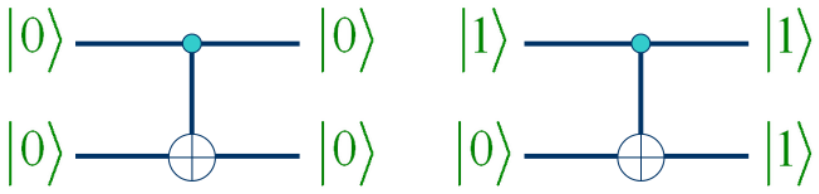


Czy na to samo pozwala bramka CNOT:

$$|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle?$$

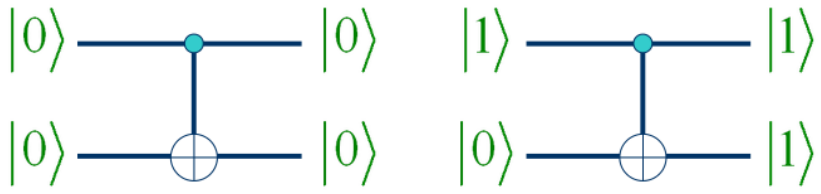
Powielanie bitu

Działanie na stanach bazowych: OK

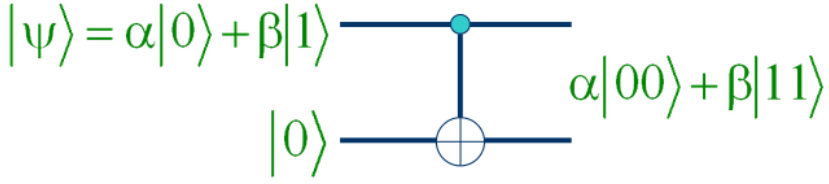


Powielanie bitu

Działanie na stanach bazowych: OK



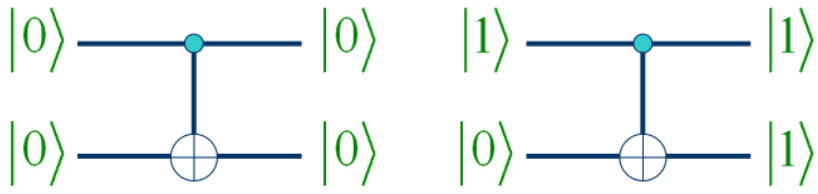
Działanie na superpozycjach: produkcja splątania



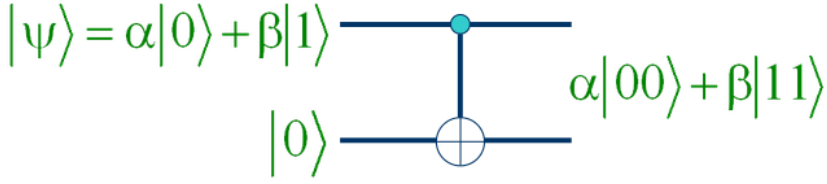
Niemożliwe klonowanie nieznanego stanu kwantowego.

Powielanie bitu

Działanie na stanach bazowych: OK



Działanie na superpozycjach: produkcja splątania



Niemożliwe klonowanie nieznanego stanu kwantowego.

$$|\psi\rangle|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$
$$= \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle \neq \alpha|00\rangle + \beta|11\rangle$$

Uniwersalny zestaw kwantowych bramek logicznych

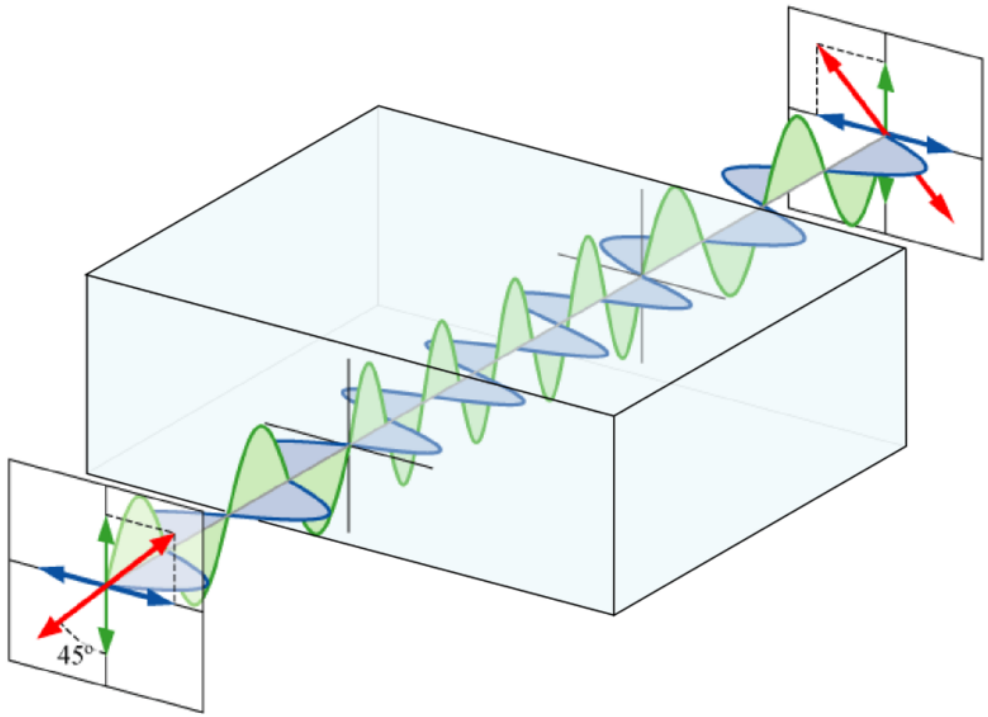
Twierdzenie:
Do zrealizowania dowolnego algorytmu kwantowego wystarczy zestaw bramek jednokubitowych (np. H i PHASE) oraz jedna bramka dwukubitowa (np. CNOT).

Zadanie domowe: Sprawdzić że $\mathrm{CNOT} = \mathrm{H}_2 \cdot \mathrm{CPHASE} \cdot \mathrm{H}_2$,
gdzie indeks 2 oznacza że bramka działa na drugi z kubitów.

Fizyczne realizacje kwantowych bramek logicznych

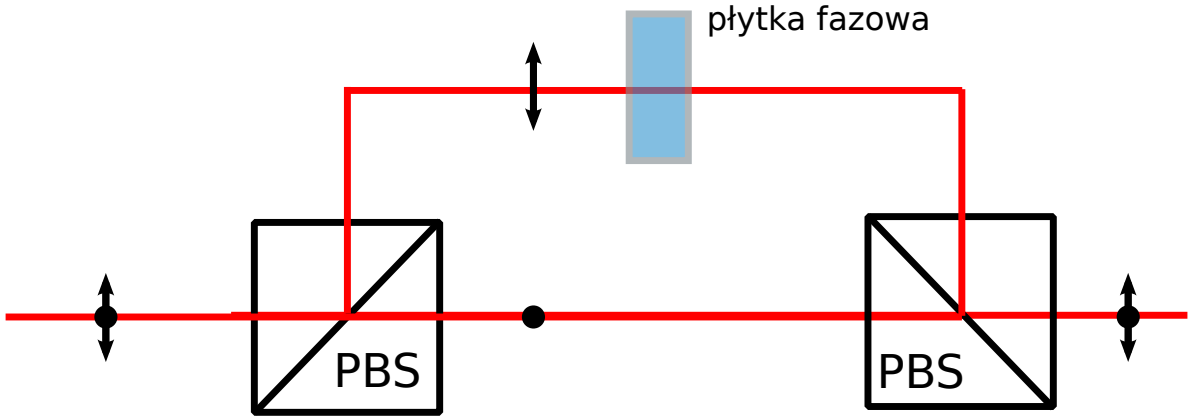
Dla kubitów zakodowanych w polaryzacji fotonu:

- bramka NOT: obrót polaryzacji o 90^o - półfalówka
  różne współczynniki załamania dla poziomej i pionowej polaryzacji



- podobnie bramka H: obrót o 45^o

Fizyczne realizacje kwantowych bramek logicznych



Dla kubitów zakodowanych w polaryzacji fotonu:

- zmiana fazy PHASE:
  polaryzacyjny dzielnik wiązki PBS rozdziela/łączy bazowe pol.
  płytka fazowa φ opóźnia fazę wiązki: zmiana znaku $+$ na $-$
  kombinacja $\mathrm{PBS} + \varphi + \mathrm{PBS}$ realizuje bramkę

Fizyczne realizacje kwantowych bramek logicznych

Dla kubitów zakodowanych w polaryzacji fotonu:

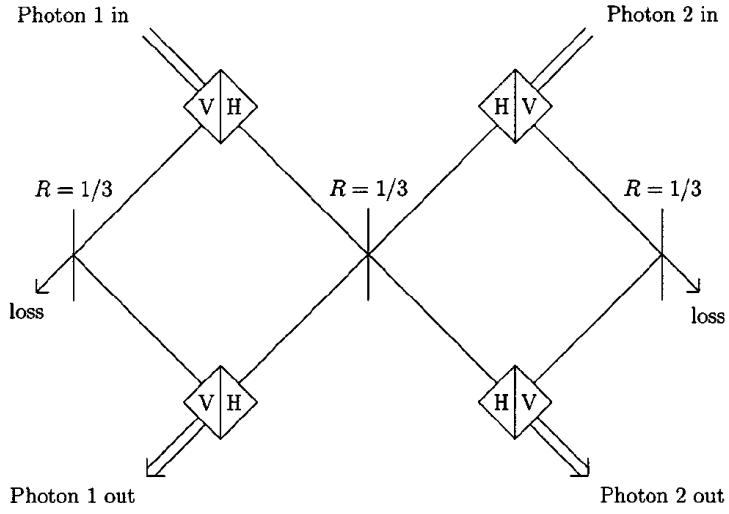
- deterministyczna bramka CPHASE np. w oparciu o nieliniowy ośrodek

Fizyczne realizacje kwantowych bramek logicznych

Dla kubitów zakodowanych w polaryzacji fotonu:

- deterministyczna bramka CPHASE np. w oparciu o nieliniowy ośrodek

- probabilistyczne bramki sterowane CPHASE lub CNOT mogą być realizowane w oparciu o użycie dodatkowych fotonów i pomiary - działają w ułamku przypadków (wiadomo kiedy), ale nie wymagają nieliniowych ośrodków



Proces SPDC generuje splątane pary fotonów

Spontaniczne Parametryczne Dzielenie Częstości

- podział fotonu o energii $h\nu$ (częstotliwości ν) na parę fotonów o energii $h\frac{\nu}{2}$ (częstotliwości $\frac{\nu}{2}$)
- stan pary jest splatany

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle\right)$$

Proces SPDC generuje splątane pary fotonów

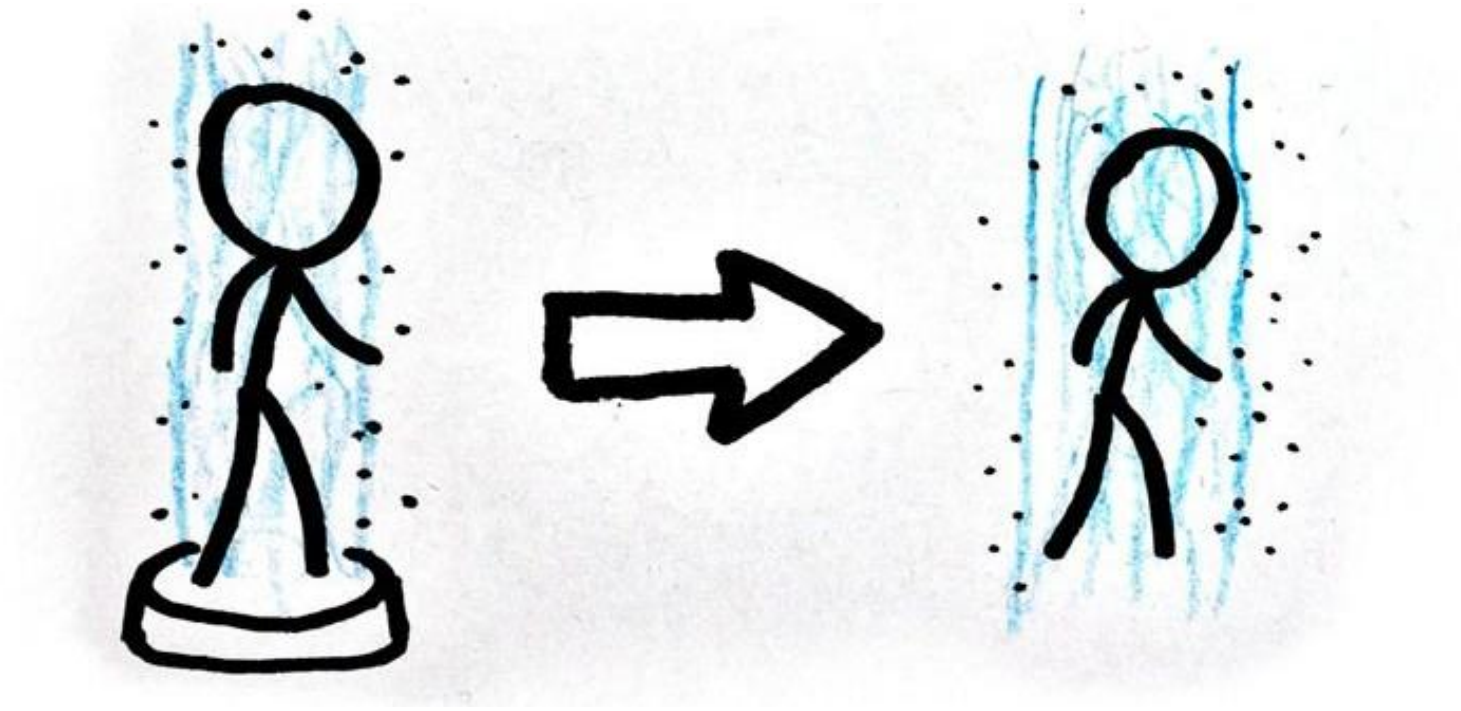
Testy Bella

- istnieją **nielokalne** (= na dystanse $> ct$) **korelacje kwantowe** (= splątanie)
- pomiar polaryzacji jednego z fotonów powoduje kolaps funkcji falowej obu, np.

$$|\psi\rangle \rightarrow |\,\updownarrow\updownarrow\rangle$$

- zgodne z teorią względności: przekaz informacji tą drogą niemożliwy

Teleportacja kwantowa



Teleportacja kwantowa

Alicja i Bob spotkali się dawno temu. Wygenerowali wówczas splątaną parę cząstek i podzielili się nią. Teraz Bob ukrywa się w nieznanym miejscu. Misją Alicji jest przesłać mu wiadomość, której nawet ona sama nie zna. Wiadomość zakodowana jest w postaci kubitu, ale Alicja ma jedynie możliwość klasycznej komunikacji (np. przez telefon). Niestety, opis stanu kubitu wymaga nieskończonej ilości klasycznej informacji!

Protokół teleportacji

1. Alicja i Bob dzielą splątaną parę kubitów

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

Protokół teleportacji

1. Alicja i Bob dzielą splątaną parę kubitów

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

2. Alicja ma dodatkowo nieznany stan

$$|\psi\rangle = \alpha|0\rangle_X + \beta|1\rangle_X$$

Protokół teleportacji

1. Alicja i Bob dzielą splątaną parę kubitów

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

2. Alicja ma dodatkowo nieznany stan

$$|\psi\rangle = \alpha|0\rangle_X + \beta|1\rangle_X$$

3. Alicja przetwarza swoją parę cząstek AX, wykonuje na niej pomiar, i informuje Boba telefonicznie o wyniku pomiaru.

Protokół teleportacji

1. Alicja i Bob dzielą splątaną parę kubitów

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

2. Alicja ma dodatkowo nieznany stan

$$|\psi\rangle = \alpha|0\rangle_X + \beta|1\rangle_X$$

3. Alicja przetwarza swoją parę cząstek AX, wykonuje na niej pomiar, i informuje Boba telefonicznie o wyniku pomiaru.

4. W zależności od wyniku, Bob wykonuje określoną operację jednokubitową na swojej cząstce. Stan cząstki B Boba staje się identyczny z $|\psi\rangle$.

Protokół teleportacji

Stan początkowy:

$|\psi\rangle_X \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (\alpha|0\rangle_X + \beta|1\rangle_X) \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)]$

Protokół teleportacji

Stan początkowy:

$|\psi\rangle_X \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (\alpha|0\rangle_X + \beta|1\rangle_X) \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)]$

Operacja CNOT na parze Alicji:

$\rightarrow \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

Protokół teleportacji

Stan początkowy:

$|\psi\rangle_X \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (\alpha|0\rangle_X + \beta|1\rangle_X) \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)]$

Operacja CNOT na parze Alicji:

$\rightarrow \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

Operacja H na kubicie X:

$\rightarrow \frac{1}{2} [\alpha (|0\rangle_X + |1\rangle_X) (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta (|0\rangle_X - |1\rangle_X) (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

$= \frac{1}{2} [|0\rangle_X|0\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) + |0\rangle_X|1\rangle_A (\alpha|1\rangle_B + \beta|0\rangle_B)$

$+ |1\rangle_X|0\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) + |1\rangle_X|1\rangle_A (\alpha|1\rangle_B - \beta|0\rangle_B)]$

Protokół teleportacji

Stan początkowy:

$|\psi\rangle_X \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (\alpha|0\rangle_X + \beta|1\rangle_X) \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)]$

Operacja CNOT na parze Alicji:

$\rightarrow \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

Operacja H na kubicie X:

$\rightarrow \frac{1}{2} [\alpha (|0\rangle_X + |1\rangle_X) (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta (|0\rangle_X - |1\rangle_X) (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

$= \frac{1}{2} [|0\rangle_X|0\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) + |0\rangle_X|1\rangle_A (\alpha|1\rangle_B + \beta|0\rangle_B)$

$+ |1\rangle_X|0\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) + |1\rangle_X|1\rangle_A (\alpha|1\rangle_B - \beta|0\rangle_B)]$

Pomiar pary kubitów Alicji daje jeden z czterech wyników, kolapsując stan kubitu Boba:

$$
\begin{aligned}
|0\rangle_X|0\rangle_A &\rightarrow \alpha|0\rangle_B + \beta|1\rangle_B \\
|0\rangle_X|1\rangle_A &\rightarrow \alpha|1\rangle_B + \beta|0\rangle_B \\
|1\rangle_X|0\rangle_A &\rightarrow \alpha|0\rangle_B - \beta|1\rangle_B \\
|1\rangle_X|1\rangle_A &\rightarrow \alpha|1\rangle_B - \beta|0\rangle_B
\end{aligned}
$$

Protokół teleportacji

Stan początkowy:

$|\psi\rangle_X \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = (\alpha|0\rangle_X + \beta|1\rangle_X) \frac{1}{\sqrt{2}} (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)]$

Operacja CNOT na parze Alicji:

$\rightarrow \frac{1}{\sqrt{2}} [\alpha|0\rangle_X (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta|1\rangle_X (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

Operacja H na kubicie X:

$\rightarrow \frac{1}{2} [\alpha (|0\rangle_X + |1\rangle_X) (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) + \beta (|0\rangle_X - |1\rangle_X) (|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)]$

$= \frac{1}{2} [|0\rangle_X|0\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) + |0\rangle_X|1\rangle_A (\alpha|1\rangle_B + \beta|0\rangle_B)$

$+ |1\rangle_X|0\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) + |1\rangle_X|1\rangle_A (\alpha|1\rangle_B - \beta|0\rangle_B)]$

Pomiar pary kubitów Alicji daje jeden z czterech wyników, kolapsując stan kubitu Boba:
Następnie, Alicja dzwoni do Boba i podaje mu 2 bity informacji (wynik pomiaru).
Bob wykonuje odpowiednią operację na swoim kubicie:

$$
\begin{aligned}
|0\rangle_X|0\rangle_A &\rightarrow \alpha|0\rangle_B + \beta|1\rangle_B \rightarrow \mathrm{nic} \\
|0\rangle_X|1\rangle_A &\rightarrow \alpha|1\rangle_B + \beta|0\rangle_B \rightarrow \mathrm{NOT} \\
|1\rangle_X|0\rangle_A &\rightarrow \alpha|0\rangle_B - \beta|1\rangle_B \rightarrow \mathrm{PHASE} \\
|1\rangle_X|1\rangle_A &\rightarrow \alpha|1\rangle_B - \beta|0\rangle_B \rightarrow \mathrm{NOT} \cdot \mathrm{PHASE}
\end{aligned}
$$

Podsumowanie: teleportacja

- Teleportacja dotyczy stanu kwantowego kubitu.
- Protokół teleportacji wymaga następujących zasobów:
  - para splątana
  - klasyczna komunikacja (np. telefon)
- Na końcu stan cząstki w lab. B jest identyczny z początkowym stane cząstki w lab. A.
- Nie ma klonowania: stan cząstki w A zniszczony.

Dystrybucja klucza kryptograficznego

Dystrybucja klucza kryptograficznego

- Mamy wiadomość W daną w postaci szeregu bitów.
- Żeby zaszyfrować wiadomość W, należy dodać do niej szereg K losowych bitów.
- Do odczytania zaszyfrowanej wiadomości niezbędna jest znajomość szeregu K.
- Zaszyfrowana komunikacja między Alicją i Bobem możliwa, gdy oboje są w posiadaniu tego samego klucza kryptograficznego.
- W praktyce, największą słabością kryptografii jest trudność dystrybucji klucza.
- Wykorzystanie fizyki kwantowej daje możliwość bezpiecznej generacji klucza z użyciem publicznych kanałów komunikacji.

Protokół BB84

- Alicja generuje ciąg losowych bitów (0 lub 1).

Protokół BB84

- Alicja generuje ciąg losowych bitów (0 lub 1).
- Alicja koduje bity w polaryzacji fotonów losowo w bazach + lub x, wg zasady

	0	1
+	|	-
x	/	\

i wysyła je do Boba

Protokół BB84

- Alicja generuje ciąg losowych bitów (0 lub 1).
- Alicja koduje bity w polaryzacji fotonów losowo w bazach + lub x, wg zasady

	0	1
+	|	-
x	/	\

  i wysyła je do Boba
- Bob mierzy polaryzacje w losowych bazach (wybór baz niezależny od wyboru Alicji).
  Jeśli bazy A i B zgadzają się, B ma prawidłową inform. o bicie klucza.
  Jeśli bazy A i B nie zgadzają się, B ma losową inform. o bicie klucza.

Protokół BB84

- Alicja generuje ciąg losowych bitów (0 lub 1).
- Alicja koduje bity w polaryzacji fotonów losowo w bazach + lub x, wg zasady

	0	1
+	|	-
x	/	\

  i wysyła je do Boba
- Bob mierzy polaryzacje w losowych bazach (wybór baz niezależny od wyboru Alicji).
  Jeśli bazy A i B zgadzają się, B ma prawidłową inform. o bicie klucza.
  Jeśli bazy A i B nie zgadzają się, B ma losową inform. o bicie klucza.
- Alicja publicznie ogłasza swój ciąg baz.
  Jako klucz kryptograficzny wykorzystane zostają tylko bity kodowane w zgodnych bazach, tj. około połowy początkowo wygenerowanych bitów.

Test umożliwia wykrycie podsłuchu

- A i B generują klucz kryptograficzny.
- Ewa (*evesdropper*) usiłuje przechwycić klucz.
  Strategia: E mierzy każdy z bitów wysyłanych przez A
  w losowej bazie. Następnie, wysyła foton do B spolaryzowany
  zgodnie z wynikiem swojego pomiaru.
  Gdy E prawidłowo odgadnie bazę, jest nie do wykrycia,
  a uzyskuje dostęp do bitu klucza.
  Gdy E nie zgadnie bazy, wprowadza zaburzenia.
- B mierzy fotony jak wcześniej. Zaburzenia pojawiają się,
  gdy E nie zgadnie bazy, a B zgadnie: w 25% przypadków.
  A ogłasza swoje bazy - powstaje klucz.
- Celem wykrycia podsłuchu, A i B porównują część bitów
  klucza. Więcej niż 25% błędów jest sygnałem o podsłuchu.
- Dla dobrej wiarygodności, test wykonywany jest
  na około połowie bitów klucza.

Podsumowanie: kodowanie

- Prawa fizyki kwantowej umożliwiają bezpieczną wymianę klucza kryptograficznego z użyciem publicznych kanałów komunikacji.
- Obecność podsłuchu wprowadza zaburzenia demaskujące podsłuchiwacza.

Komputery kwantowe

- kwantowe superkomputery: uczenie maszynowe, medycyna, chemia, inżynieria materiałów, symulacje procesów biologicznych
- komunikacja kwantowa
- szyfrowanie

Klasyczny superkomputer Tianhe-2, Guangzhou, Chiny $<$ 50 kubitów

Wyścig o *supremację kwantową*:
Google, IBM, Rigetti Computing, D-Wave Systems, ...

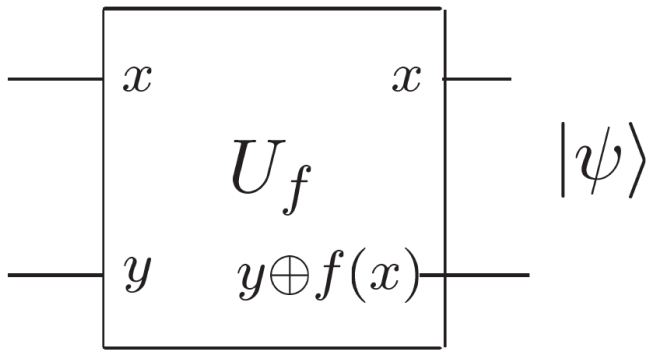
Algorytmy kwantowe bazują na równoległych obliczeniach dla wszystkich możliwych bitów wejściowych

Przykład: obliczenie wartości funkcji $f(x)$ dla różnych wartości argumentu x jednocześnie.

- Niech funkcja $f(x) : \{0, 1\} \to \{0, 1\}$.
- Mamy algorytm, który dla wartości wejściowych $|x, y\rangle$ (gdzie $x, y \in \{0, 1\}$) zwraca $|x, y + f(x)\rangle$

$$|0, 0\rangle \to |0, f(0)\rangle$$

$$|1, 0\rangle \to |1, f(1)\rangle$$



Algorytmy kwantowe bazują na równoległych obliczeniach dla wszystkich możliwych bitów wejściowych

Przykład: obliczenie wartości funkcji $f(x)$ dla różnych wartości argumentu x jednocześnie.

- Niech funkcja $f(x) : \{0, 1\} \to \{0, 1\}$.
- Mamy algorytm, który dla wartości wejściowych $|x, y\rangle$ (gdzie $x, y \in \{0, 1\}$) zwraca $|x, y + f(x)\rangle$

$$|0, 0\rangle \to |0, f(0)\rangle$$

$$|1, 0\rangle \to |1, f(1)\rangle$$

- Użycie superpozycji jako kubitu wejściowego x, daje:

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

Algorytm oblicza wszystkie wartości funkcji za jednym zamachem.

Algorytmy kwantowe bazują na równoległych obliczeniach dla wszystkich możliwych bitów wejściowych

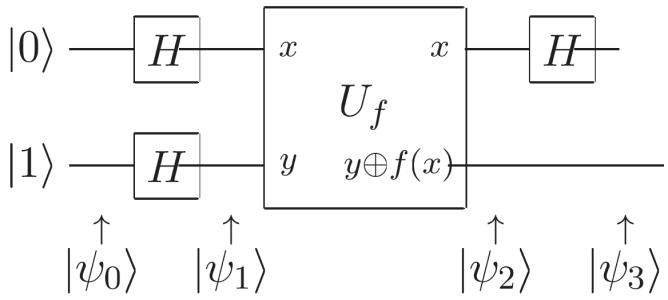
- Bardziej skomplikowane algorytmy bazują na superpozycji w wielu kubitach wejściowych:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, 0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$$

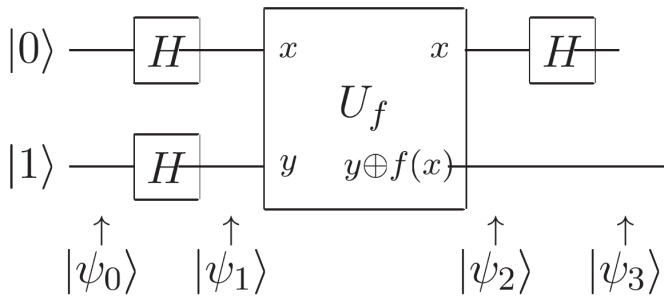
  gdzie $\sum$ oznacza superpozycję wszystkich możliwych stanów.
- Aby poznać wyniki, należy dokonać pomiaru obu kubitów wyjściowych. Istota algorytmów kwantowych polega na obróbce stanu wyjściowego tak, by zwiększyć prawdopodobieństwa uzyskania intresującej wartości x.

Algorytm Deutscha: sprawdzenie czy funkcja jest stała

$$|\psi_0\rangle = |01\rangle$$

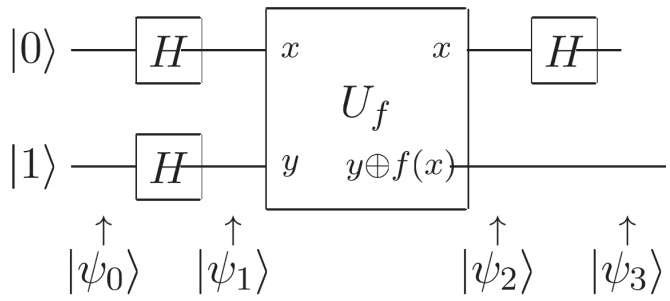


Algorytm Deutscha: sprawdzenie czy funkcja jest stała



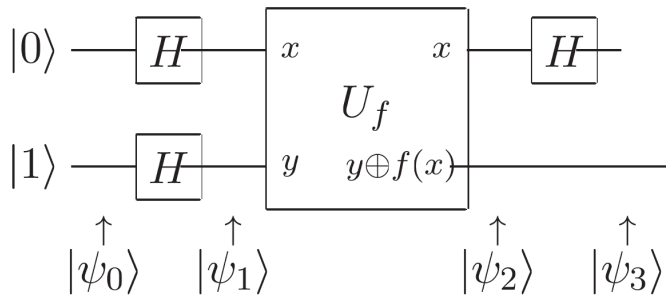
$$|\psi_0\rangle = |01\rangle$$
$$|\psi_1\rangle = \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

Algorytm Deutscha: sprawdzenie czy funkcja jest stała



$$|\psi_0\rangle = |01\rangle$$
$$|\psi_1\rangle = \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$
$$|\psi_2\rangle =$$
$$\begin{cases} \pm\tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm\tfrac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

Algorytm Deutscha: sprawdzenie czy funkcja jest stała



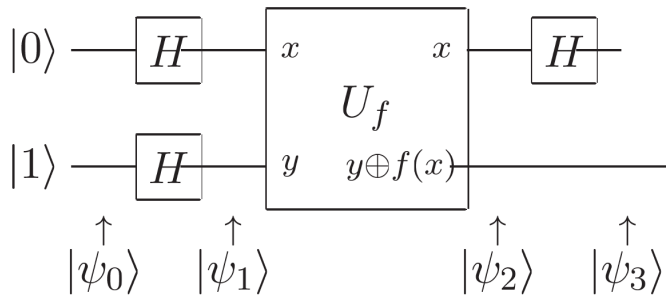
$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$$|\psi_2\rangle = \begin{cases} \pm\tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm\tfrac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm|1\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

Algorytm Deutscha: sprawdzenie czy funkcja jest stała



$$|\psi_0\rangle = |01\rangle$$

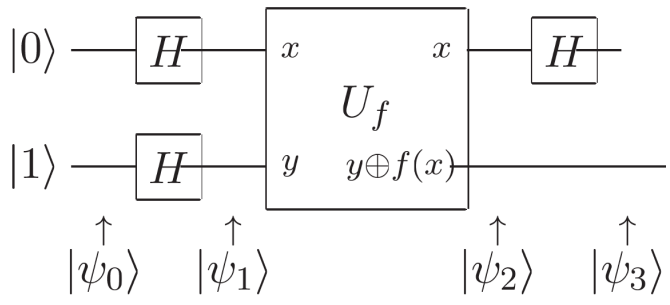
$$|\psi_1\rangle = \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$$|\psi_2\rangle = \begin{cases} \pm\tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm\tfrac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm|1\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

Pomiar pierwszego kubitu zdradza czy funkcja jest stała.

Algorytm Deutscha: sprawdzenie czy funkcja jest stała



$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

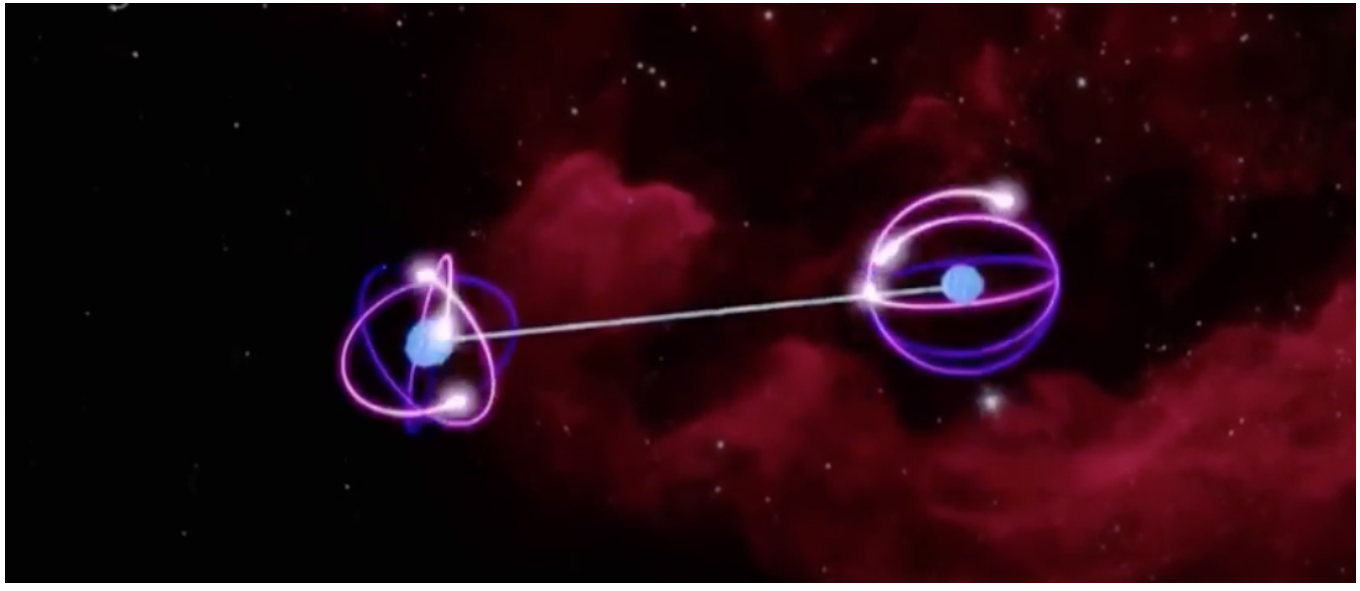
$$|\psi_2\rangle = \begin{cases} \pm\tfrac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm\tfrac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) = f(1) \\ \pm|1\rangle\left(|0\rangle - |1\rangle\right) & \text{gdy } f(0) \neq f(1) \end{cases}$$

Pomiar pierwszego kubitu zdradza czy funkcja jest stała.

Algorytm Deutscha-Jozsy to uogólnienie na większą liczbę bitów.

Algorytmy kwantowe: podsumowanie



- Komputery kwantowe to perspektywa bezprecedensowych mocy obliczeniowych.
- Algorytmy kwantowe bazują na jednoczesnym wykonaniu obliczeń dla wszystkich możliwych danych wejściowych. Stąd wynika szybkość kwantowych komputerów.