Wstęp do informatyki kwantowej

Marek Góźdź

wersja z dnia: 22 stycznia 2025

Główne zagadnienia:

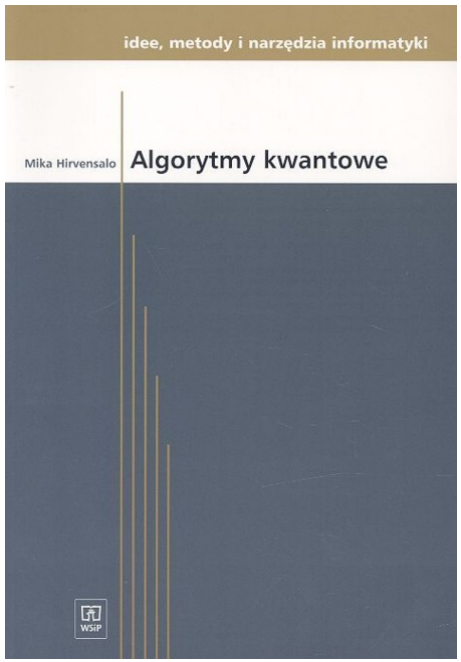
- Macierze i wektory, przestrzeń liniowa.
- Wprowadzenie do mechaniki kwantowej – stan, pomiar, splątanie.
- Informatyka kwantowa – pojęcie kubitu.
- Podstawowe bramki kwantowe.
- Podstawowe algorytmy kwantowe.
- Bezpieczeństwo układów kwantowych – zakaz klonowania, szyfrowanie kwantowe, możliwe ataki.
- Algorytmy korekcji błędów.
- Symulacje układów kwantowych, „komputery kwantowe”.

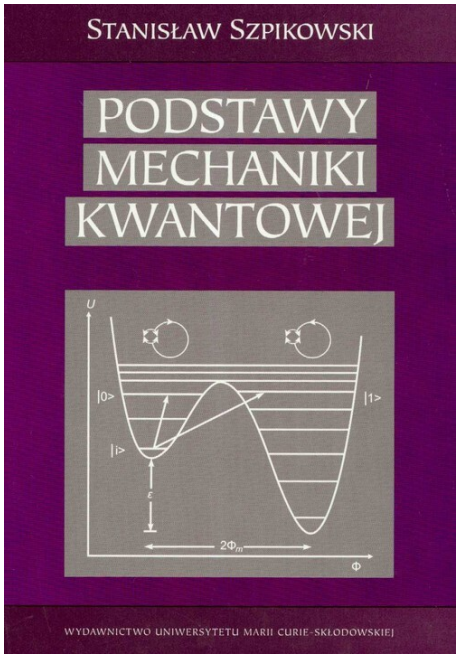
Podręczniki:

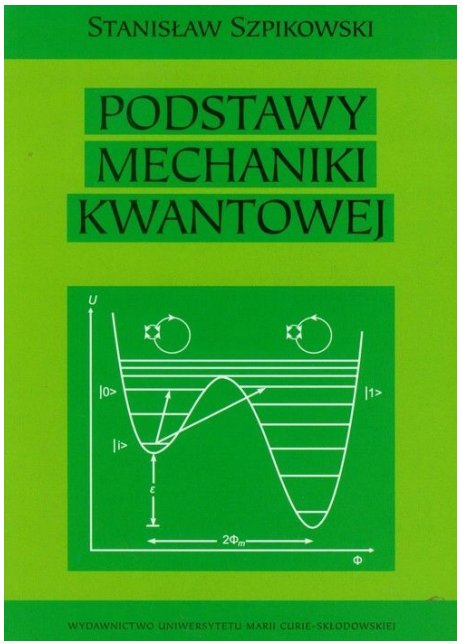
- M.Le Bellac, Wstęp do informatyki kwantowej, PWN, Warszawa 2011.
- M.Hirvensalo, Algorytmy kwantowe, WSiP, Warszawa 2004.
- J.Preskill, skypt do wykładu *Quantum Computation*, Caltech `http://theory.caltech.edu/~preskill/ph229/`

Dodatkowo:

- S.Szpikowski, Podstawy mechaniki kwantowej, UMCS, Lublin 2011.







Informatyka klasyczna jest wprowadzana poprzez **algebrę Boole'a**:

- zbiór dwuelementowy, np. $\{0, 1\}$, $\{t, f\}$, $\{\uparrow, \downarrow\}$ lub inne
- działanie unarne NOT
- działania binarne AND i OR

x	y	$\bar{y}$	$x \cdot y$	$x + y$
0	0	1	0	0
0	1	0	0	1
1	0		0	1
1	1		1	1

Co można chcieć poprawić w systemach klasycznych?

	Mamy:	Chcielibyśmy mieć:
Sprzęt	elektronikę cyfrową	układy dwustanowe
Błędy	ciepło	brak strat energii
Wydajność	pracę bit po bicie	szybszą pracę
Bezpieczeństwo	kopiowanie, podsłuch	zabezpieczone dane

Brak strat energii oznacza brak utraty informacji, a w konsekwencji odwracalność używanych operacji i brak błędów.

Mikroświat jest kwantowy

Wielkość skwantowana może przyjmować tylko ściśle określone wartości.

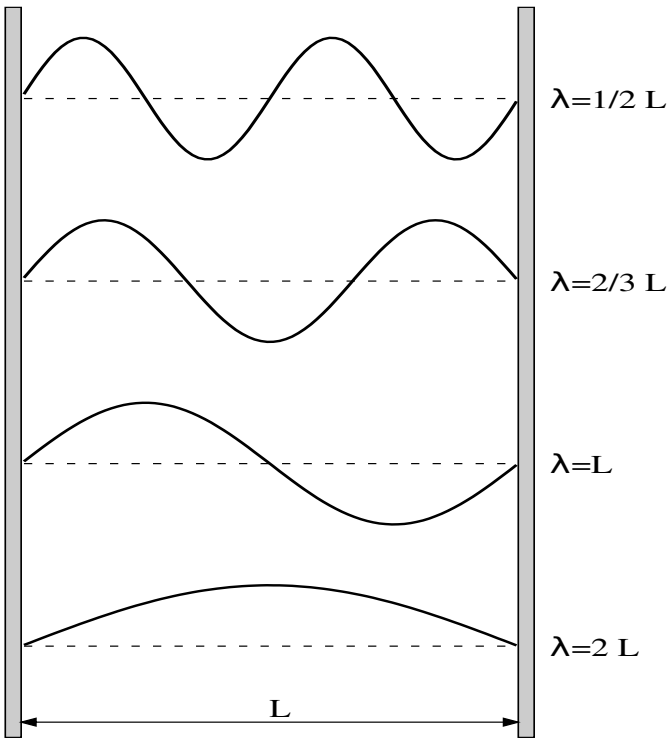
- W świecie makroskopowym kwantowania nie widać i wiele wielkości wydaje się ciągłe: czas, położenie, pęd, moment pędu, energia...
- W świecie mikroskopowym niemal każda cecha jest lub może podlegać kwantowaniu. Są one wtedy funkcjami pewnych parametrów, zwanych **liczbami kwantowymi**.

Przykład: promień orbity i energia elektronu w atomie wodoru mają w modelu Bohra postać (dla $n = 1, 2, 3, \dots$)

$$R_n = \frac{4\pi\epsilon_0\hbar^2}{me^2}n^2 \qquad E_n = -\frac{me^4}{32\pi^2\epsilon_0^2\hbar^2}\frac{1}{n^2}$$

Przykład: czy cząstka zamknięta pomiędzy dwiema ścianami może mieć dowolną energię?

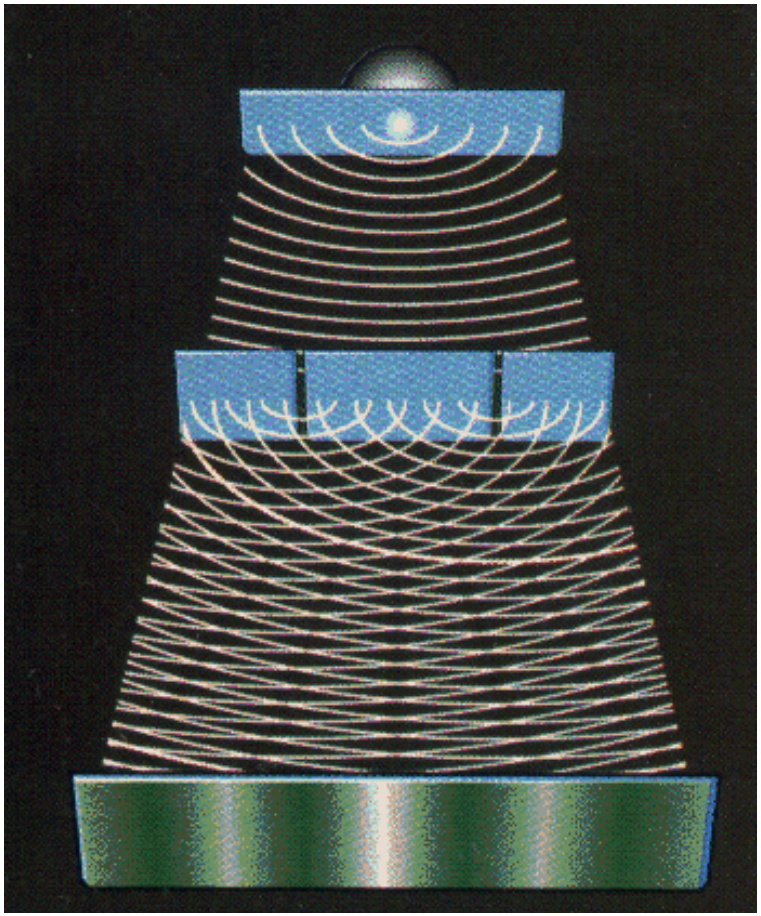
- Prawidłowy opis takiej cząstki uwzględnia, że cząstka zachowuje się jak fala (dualizm korpuskularno-falowy).
- Fala na ścianach musi mieć węzły, bo zakładamy, że cząstka w ścianę nie wnika.

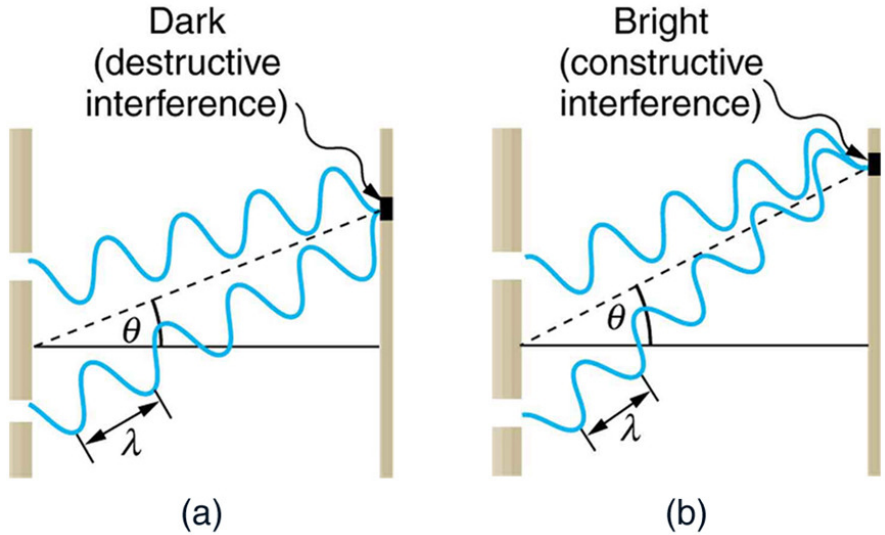


Energia w normalnych warunkach nie jest skwantowana.

Obecność ścian narzuca ograniczenie na możliwe długości fali. Ponieważ $E = hc/\lambda$, energia zaczyna przybierać tylko ściśle określone wartości.

Przykład: Doświadczenie dwuszczelinowe Younga i jego rozwinięcia.



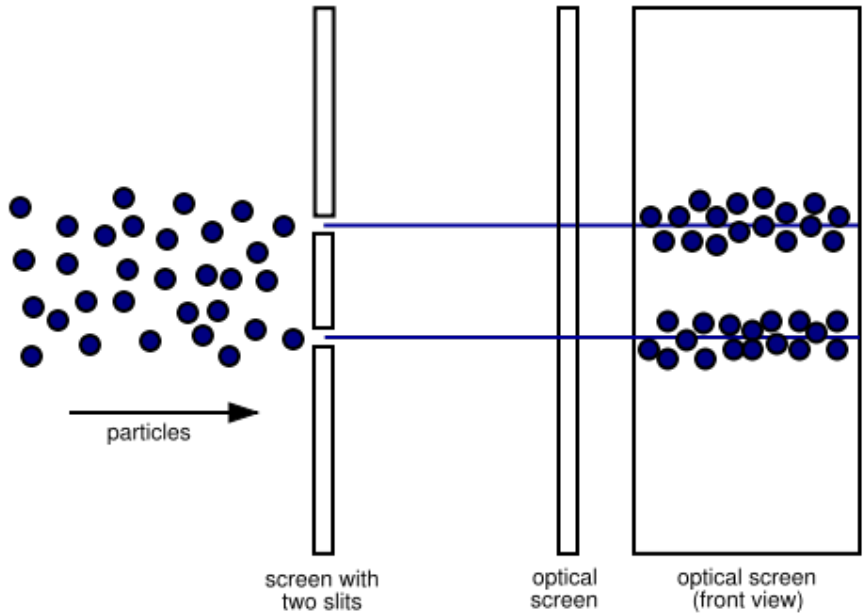


Fale podlegają

- interferencji konstruktywnej (wzmocnieniu) jeśli zgodne fazy
- interferencji destruktywnej (osłabieniu) jeśli fazy przeciwne

Obserwacja: światło ma naturę falową, więc tworzy obraz interferencyjny, podobnie jak fale na wodzie.

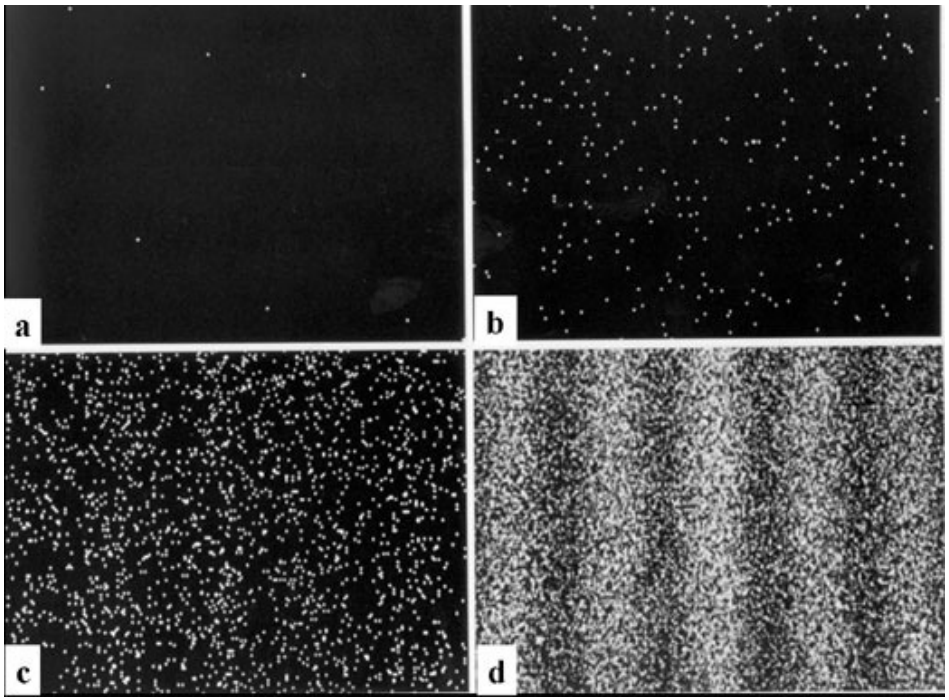
Obraz klasyczny: cząstki puszczone przez dwie szczeliny interferować nie mogą, dając obraz dwóch szczelin i nic więcej



Wydawało się więc, że

- elektrony powinny dawać obraz dwóch szczelin,
- fotony puszczane pojedynczo, a nie strumieniem, też powinny dawać obraz dwóch szczelin.

Naświetlając ekran poprzez dwie szczeliny pojedynczymi elektronami ekran wyglądał wraz z upływem czasu tak:



Trudne pytanie: z czym interferują pojedyncze cząstki?
Odpowiedź wymaga teorii kwantowej, klasycznie jest to niemożliwe.

Przykład: informatyka klasyczna opiera się na wielkościach „skwantowanych”:

- bit ma dwie wartości,
- podstawowe operacje arytmetyczne i logiczne dają przy ustalonym wejściu za każdym razem ten sam wynik,
- i tak dalej.

Problem polega na tym, że sprzęt realizujący te operacje jedynie symuluje dwustanowość (gdyż prąd elektryczny nie jest wielkością kwantową w takich układach), przez co pojawiają się błędy, straty energii itd.

Interludium: trochę matematyki...

Rząd tensora odpowiada liczbie jego wskaźników:

α	skalar	tensor rzędu 0
x_i	wektor	tensor rzędu 1
x_{ij}	macierz	tensor rzędu 2
x_{ijk}		tensor rzędu 3

Skalar można utożsamić z polem skalarnym, liczbą rzeczywistą lub macierzą 1×1.
Wektor poziomy o długości n jest macierzą $1 \times n$.
Wektor kolumnowy to macierz $n \times 1$.

Przykład: całkowicie antysymetryczna gęstość tensorowa Leviego-Civity ϵ_{ijk} jest zdefiniowana dla $i, j, k = 1, 2, 3$

$$\epsilon_{ijk} = \begin{cases} 1 & \text{dla } ijk \text{ będącej parzystą permutacją } 123 \\ \text{-1} & \text{dla } ijk \text{ będącej nieparzystą permutacją } 123 \\ 0 & \text{w pozostałych przypadkach} \end{cases}$$

Iloczyn wektorowy można zapisać wtedy jako

$$(\vec{x} \times \vec{y})_i = \sum_{jk} \epsilon_{ijk}\ x_j\ y_k$$

co daje

$$(\vec{x} \times \vec{y})_1 = x_2 y_3 - x_3 y_2$$
$$(\vec{x} \times \vec{y})_2 = x_3 y_1 - x_1 y_3$$
$$(\vec{x} \times \vec{y})_3 = x_1 y_2 - x_2 y_1$$

Dodawanie wektorów i macierzy

$$\begin{pmatrix} a & b & c \end{pmatrix} + \begin{pmatrix} x & y & z \end{pmatrix} = \begin{pmatrix} a+x & b+y & c+z \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a+w & b+x \\ c+y & d+z \end{pmatrix}$$

Mnożenie przez skalar

$$\alpha \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} = \begin{pmatrix} \alpha x_1 & \alpha x_2 & \alpha x_3 \end{pmatrix}$$

$$\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}$$

Mnożenie wektorów

Iloczyn skalarny:

$$\begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = ax + by + cz$$

Iloczyn diadyczny:

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{pmatrix} x & y & z \end{pmatrix} = \begin{pmatrix} a\ (x\ y\ z) \\ b\ (x\ y\ z) \\ c\ (x\ y\ z) \end{pmatrix} = \begin{pmatrix} ax & ay & az \\ bx & by & bz \\ cx & cy & cz \end{pmatrix}$$

Mnożenie macierzy

Mnożymy „wiersz przez kolumnę”, dodając wyniki:

$$w_{ij} = \sum_k x_{ik}\ y_{kj}$$

Mnożenie macierzy i wektorów nie jest w ogólności przemienne, $AB \neq BA$.

Przykład:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+2c & b+2d \\ 3a+4c & 3b+4d \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} a+3b & 2a+4b \\ c+3d & 2c+4d \end{pmatrix}$$

Sprzężenie zespolone

Zmiana znaku części urojonej liczby: $(a+bi)^* = a - bi$, gdzie $i^2 = -1$.

Sprzężenie zespolone wektora lub macierzy to sprzężenie każdego ich elementu:

$$w = \begin{pmatrix} a & b & c & d \end{pmatrix} \qquad w^* = \begin{pmatrix} a^* & b^* & c^* & d^* \end{pmatrix}$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad A^* = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$$

Transpozycja

Transpozycja oznacza zamianę wskaźników miejscami.
Skalar jest niezmienniczy względem transpozycji: $\alpha^T = \alpha$.
Wektor transponowany staje się wektorem kolumnowym:

$$x = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} \qquad x^T = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$$

Transpozycja macierzy: $(x^T)_{ij} = x_{ji}$

$$x = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix} \qquad x^T = \begin{pmatrix} x_{11} & x_{21} & \dots & x_{m1} \\ x_{12} & x_{22} & \dots & x_{m2} \\ \dots & \dots & \dots & \dots \\ x_{1n} & x_{2n} & \dots & x_{mn} \end{pmatrix}$$

Podwójna transpozycja jest operacją tożsamościową:

$$(x^T)^T = x$$

Zadanie: Pokaż, że dla dowolnych macierzy A i B zachodzi

$$(AB)^T = B^T A^T$$

Wersja prostsza: pokazać to samo jawnie dla dowolnych macierzy 2×2 i 3×3.

Wektory i wartości własne

Równanie własne (r-nie wiekowe) macierzy kwadratowej

$$Aw = \lambda w$$

wyznacza jej wektory własne w i wartości własne λ. Macierz $n \times n$ posiada n wektorów i n wartości własnych. Niektóre mogą być wielokrotne.
Po pełnej diagonalizacji macierz A ma postać

$$A = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ & \dots & & \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Przykład: aby znaleźć wektory i wartości własne macierzy

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

należy rozwiązać równanie $Aw = \lambda w$

$$(A - \lambda 1)w = 0$$
$$\begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = 0$$
$$\det \begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix} = 0$$
$$(a-\lambda)(d-\lambda) - bc = 0$$

Z równania kwadratowego otrzymujemy dwie λ, dla których znajdowane są wektory w.

Np. dla $A = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}$ wartości własne wyznaczamy następująco:

$$\det \begin{pmatrix} 3-\lambda & 2 \\ 4 & 1-\lambda \end{pmatrix} = 0 \quad \Rightarrow \quad \lambda^2 - 4\lambda - 5 = 0 \quad \Rightarrow \quad \lambda = 5, -1$$

Wektor własny dla $\lambda = 5$

$$\begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} 5w_1 \\ 5w_2 \end{pmatrix} \quad \Rightarrow \quad \begin{cases} 3w_1 + 2w_2 = 5w_1 \\ 4w_1 + w_2 = 5w_2 \end{cases} \quad \Rightarrow \quad w_1 = w_2$$

czyli przykładowym wektorem jest $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Dla $\lambda = -1$ podobny rachunek prowadzi do warunku $w_2 = -2w_1$; przykładowy wektor własny odpowiadający tej wartości własnej to $\begin{pmatrix} 1 \\ -2 \end{pmatrix}$.

Sprzężenie hermitowskie

Sprzężenie po hermitowsku to transpozycja i sprzężenie zespolone:

$$(A)_{ij} = a_{ij} \Rightarrow (A^\dagger)_{ij} = (A^{*T})_{ij} = a^*_{ji}$$

Macierz nazywana jest **hermitowską** jeśli sprzężenie jej nie zmienia, czyli $A^\dagger = A$. Oznacza to, że:

- elementy diagonalne muszą być rzeczywiste,
- górny i dolny trójkąt pozadiagonalny są względem siebie odwrócone i sprzężone zespolenie, $a_{ij} = a^*_{ji}$.

Każda symetryczna macierz rzeczywista jest hermitowska.

Właściwość

Wartości własne macierzy hermitowskiej są rzeczywiste.

Dowód: Niech $A^\dagger = A$. Równanie własne i równanie do niego sprzężone:

$$\begin{cases} Aw = \lambda w \\ w^\dagger A = \lambda^* w^\dagger \end{cases}$$

Pierwsze domnażam z lewej przez $w^\dagger$, drugie z prawej przez w,

$$\begin{cases} w^\dagger A w = \lambda w^\dagger w \\ w^\dagger A w = \lambda^* w^\dagger w \end{cases}$$

Wynika stąd, że $\lambda = \lambda^*$.

Macierz unitarna to taka, dla której

$$U^\dagger U = U U^\dagger = 1,$$

albo inaczej: $U^\dagger = U^{-1}$. Uwaga: nie każda macierz jest odwracalna, np. ponieważ det $U^{-1} = 1/\det U$, nieodwracalne są macierze o zerowym wyznaczniku.

Długość wektora
Jeśli $w = (w_1, \ldots, w_n)$, to

$$|w| = \sqrt{w \cdot w} = \sqrt{w_1^2 + \cdots + w_n^2}$$

Jest to więc pierwiastek z iloczynu skalarnego $w \cdot w$.

Wektor unormowany ma długość równą 1.

Każdy niezerowy wektor można unormować: $w \to w/|w|$.

Kombinacja liniowa wektorów $x_1, x_2, \ldots, x_n$ ma postać

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$$

gdzie α_i to skalary.
Wektory z pewnego zbioru są **liniowo niezależne** jeśli nie dają się przedstawić jako skończona kombinacja liniowa innych wektorów z tego zbioru.

Baza to zbiór liniowo niezależnych wektorów, których kombinacje liniowe pozwalają na zapisanie wszystkich wektorów z danej przestrzeni.

Wektory **bazy ortonormalnej** są:

- ortogonalne, $x \cdot y = 0$,
- unormowane, $|x| = 1$.

Bazami w odpowiednich przestrzeniach są znane układy współrzędnych. Przykłady:

- na okręgu: pojedyncza współrzędna, np. ϕ
- w płaskiej przestrzeni 2D: układ kartezjański (x, y), układ biegunowy (r, ϕ)
- w zakrzywionej przestrzeni 2D: patrz np. siatki kartograficzne
- w płaskiej przestrzeni 3D: układ kartezjański (x, y, z), układ walcowy (cylindryczny) (r, ϕ, z), układ sferyczny (r, θ, ϕ)

Trzeba tylko zwrócić uwagę na jednoznaczność współrzędnych każdego punktu. Np. w układzie biegunowym, punkt w środku układu ma nieskończenie wiele możliwych współrzędnych: $r = 0$, ϕ dowolne.

Uwagi:

- w każdej przestrzeni można zbudować wiele baz,
- baza w przestrzeni nieskończeniewymiarowej ma nieskończenie wiele wektorów,
- wektory bazowe nie są uporządkowane, ale dla wygody często się wprowadza umowny porządek, ponieważ...
- ... reprezentację macierzową operatora zapisujemy w danej bazie przy określonej kolejności wektorów bazowych; w innej bazie macierz będzie miała inną postać,
- odpowiedni wybór bazy może znacznie ułatwić rachunki.

Opis bitu kwantowego buduje się na przestrzeni dwuwymiarowej, więc wybór bazy jest w prostych sytuacjach niezbyt skomplikowany. Przestrzenie potrzebne do realizacji algorytmów są bardziej złożone.

Przestrzeń Hilberta jest wektorową przestrzenią liniową, w której dla dowolnych wektorów x, y, z i dowolnych skalarów α, β zachodzi:

skalowanie wektorów	$(\alpha+\beta)x = \alpha x + \beta x$
	$\alpha(x+y) = \alpha x + \alpha y$
	$(\alpha\beta)x = \alpha(\beta x)$
dodawanie wektorów	$(x+y)+z = x+(y+z)$
mnożenie przez jeden	$\exists 1: \quad 1 \cdot x = x$
wektor zerowy	$\exists 0: \quad 0+x = x+0 = x$
wektor przeciwny	$\forall x \;\; \exists \xi: \quad x+\xi = 0$

Iloczyn skalarny zdefiniowany jest przez:

$$x \cdot y = (y \cdot x)^*$$
$$x \cdot (\alpha y) = \alpha(x \cdot y)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$
$$x \cdot x \geq 0$$

Dodatkowo w przestrzeni Hilberta każdy zbieżny ciąg wektorów dąży do jakiegoś wektora z tej przestrzeni.

Wektory opisane w pewnej przestrzeni Hilberta, wraz z operacjami iloczynu skalarnego i skalowania, są podstawą opisu mechaniki kwantowej.

Mechanikę kwantową można również zbudować na innej podstawie matematycznej, jednak opis wektorowy jest najpopularniejszy.

Podstawy mechaniki kwantowej

W skrócie:

- Wektory przestrzeni Hilberta opisują fizyczny **stan** układu.
- Wielkości fizyczne są reprezentowane przez **operatory** z tej przestrzeni. Operatory, po wybraniu bazy przestrzeni, można przedstawić jako odpowiednie macierze. Działanie macierzą na wektor daje w wyniku inny wektor.
- Na układzie można wykonać **pomiar** jakiejś wielkości fizycznej. Zazwyczaj pomiar zmienia stan układu na inny.

Zapis braket Diraca

Dla ułatwienia będę wektory zapisywał jako ket $|b\rangle$. Wektory sprzężone działają jak operatory i są reprezentowane przez bra $\langle a|$, gdzie $\langle a|^* = |a\rangle$. Działanie operatora na stan ma postać iloczynu skalarnego:

$$\langle a|b\rangle = \int a^*(x)b(x)dx.$$

Właściwości iloczynu skalarnego w zapisie Diraca:

$$\langle a|b\rangle^* = \langle b|a\rangle$$
$$\langle a|\alpha x + \beta y\rangle = \alpha\langle a|x\rangle + \beta\langle a|y\rangle$$
$$\langle \alpha a|b\rangle = \alpha^*\langle a|b\rangle$$
$$\langle a|a\rangle \geq 0$$
$$\langle a|Tb\rangle = \langle T^\dagger a|b\rangle$$

UWAGA: W fizyce przyjmuje się liniowość iloczynu skalarnego względem drugiego argumentu. W matematyce często przyjmuje się liniowość względem pierwszego argumentu, ale ja przyjmuję definicję z fizyki, bo jest ona spójna z interpretacją drugiego argumentu (ket) jako stanu układu.

Zagadka: jaką interpretację ma operator $|x\rangle\langle x|$?

Mechanika kwantowa w ujęciu przestrzeni Hilberta oparta jest na kilku podstawowych postulatach.

Postulat 0

Stan układu kwantowego opisywany jest przez unormowany wektor z ośrodkowej (o przeliczalnej bazie wektorów), zespolonej przestrzeni Hilberta.

Postulat 1

Każdej mierzalnej wielkości fizycznej przypisany jest operator hermitowski.

Postulat 2

Jedyne możliwe wartości pomiarów wielkości fizycznej dane są przez wartości własne operatora ją reprezentującego.

Już trzy podstawowe postulaty mają ciekawe konsekwencje.
Po pierwsze, wektory można dodawać do siebie, co oznacza, że np.

- cząstka może być w dwóch (i więcej) miejscach jednocześnie,
- cząstka może się „poruszać" we wszystkie strony na raz.

Po drugie, trzeba uważać na przemienność.

Komutatorem dwóch wielkości nazywamy

$$[x, y] = xy - yx.$$

Jeśli x i y są przemienne, to ich komutator się zeruje.

Skoro operatory można reprezentować jako macierze, niektóre pary operatorów nie będą komutować. Oznacza to, że podziałanie nimi na stan w różnej kolejności da różne wyniki.

Wielkości kanonicznie sprzężone to takie, których komutator wynosi $i\hbar$.

Przykład: operator pędu w kierunku x i operator położenia w kierunku x są kanonicznie sprzężone. Definicje tych operatorów to:

$$p_x = -i\hbar\frac{\partial}{\partial x}, \qquad\qquad x = x.$$

Ich komutator jest równy $i\hbar$, ponieważ

$$\begin{aligned}
[x, p_x]\psi &= \left(x(-i\hbar)\frac{\partial}{\partial x} - (-i\hbar)\frac{\partial}{\partial x}x\right)\psi = \\
&= (-i\hbar)\left(x\frac{\partial\psi}{\partial x} - \frac{\partial}{\partial x}(x\psi)\right) = \\
&= (-i\hbar)\left(x\frac{\partial\psi}{\partial x} - \psi - x\frac{\partial\psi}{\partial x}\right) = i\hbar\psi
\end{aligned}$$

Jeśli operatory nie komutują, opisują one wielkości, które są ze sobą w jakiś sposób powiązane. Zwróć uwagę, że $[x, p_y] = 0$.

Wielkości kanonicznie sprzężonych **nie można jednocześnie zmierzyć z dowolną precyzją**. Podlegają one zasadzie nieoznaczoności.

Zasada nieoznaczoności Heisenberga

Niepewności jednoczesnego pomiaru położenia Δx i pędu w tym samym kierunku Δp_x są związane zależnością:

$$(\Delta x)(\Delta p_x) \geq \frac{1}{2}\hbar$$

Następstwa zasady nieoznaczoności:

- jeśli dokładnie zmierzę pęd cząstki, może ona być dosłownie wszędzie,
- jeśli dokładnie zlokalizuję cząstkę, nie mam pojęcia o jej pędzie, czyli nie potrafię powiedzieć, gdzie ona będzie chwilę później.

Drugą parą wielkości kanonicznie sprzężonych jest czas i energia. Umożliwia to m.in. spontaniczne tworzenie w próżni par cząstek.

Postulat 3

Oczekiwana wartość średnia w stanie ψ wielkości reprezentowanej przez operator A dana jest przez

$$\langle A \rangle = \langle \psi | A | \psi \rangle = \int \psi^* A \psi \ \ dx$$

Jeśli A reprezentuje wielkość, której możliwe wartości są ciągłe, wartość średnia jest najbardziej prawdopodobnym wynikiem pomiaru. Nie jest to prawdą dla wartości dyskretnych, gdyż $\langle A \rangle$ może nie być dopuszczoną wartością A.

W mechanice kwantowej wyniki pomiarów posiadają pewien rozkład statystyczny, ciągły lub dyskretny, wokół wartości średniej.

Przykład: Niech funkcja falowa ma postać

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_2\rangle),$$

przy czym ψ_1 i ψ_2 są ortonormalne. Niech operator T działa następująco:

$$T|\psi_1\rangle = 1|\psi_1\rangle, \qquad T|\psi_2\rangle = 2|\psi_2\rangle.$$

Wartość średnia operatora T w stanie $|\psi\rangle$ wynosi:

$$\begin{aligned}\langle\psi|T|\psi\rangle &= \left(\frac{1}{\sqrt{2}}\right)^2 [\langle\psi_1|T|\psi_1\rangle + \langle\psi_1|T|\psi_2\rangle + \langle\psi_2|T|\psi_1\rangle + \langle\psi_2|T|\psi_2\rangle] = \\ &= \frac{1}{2}(1+0+0+2) = \frac{3}{2}.\end{aligned}$$

Jak widać, oczekiwana wartość średnia T nie jest wartością możliwą do zmierzenia w pomiarze.

Zadanie: Operator pędu w kierunku x ma postać

$$p_x = -i\hbar\frac{\partial}{\partial x}.$$

Znajdź wartość średnią pędu cząstki znajdującej się pomiędzy dwiema nieprzepuszczalnymi ścianami odległymi o L. Przyjmij, że funkcja falowa cząstki $\psi_k(x) = \sin(\alpha k x)$ zeruje się dla $x = 0$ i $x = L$. Ustal parametr α i oblicz $\langle\psi_k(x)|p_x|\psi_k(x)\rangle$.

Szkic rozwiązania: Funkcja falowa cząstki ma się zerować na ścianach, które umieszczamy w $x = 0$ i $x = L$. Mamy więc

$$\psi_k(x) = \sin\left(\frac{k\pi}{L}x\right), \qquad k = 1, 2, 3, \ldots.$$

Wartość średnia operatora pędu to

$$\langle\psi_k(x)|p_x|\psi_k(x)\rangle = \int_0^L dx \sin\left(\frac{k\pi}{L}x\right)(-i\hbar)\frac{\partial}{\partial x}\sin\left(\frac{k\pi}{L}x\right).$$

Wykorzystując wzór $\sin(2x) = 2\sin(x)\cos(x)$ i wykonując całkowanie otrzymujemy wynik

$$\langle\psi_k(x)|p_x|\psi_k(x)\rangle = 0.$$

Uzupełnij obliczenia. Co oznacza ten wynik? Dlaczego pominąłem $k = 0$?

Interpretacja statystyczna funkcji falowej

- Stan ma często postać **superpozycji**, tj. kombinacji liniowej

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + \dots$$

przy czym, aby stan był unormowany $\langle\psi|\psi\rangle = \big||\psi\rangle\big|^2 = 1$, funkcje ψ_i muszą być ortogonalne względem siebie oraz dodatkowo

$$|c_1|^2 + |c_2|^2 + \cdots = 1.$$

- Współczynniki $|c_i|^2 = c_i^* c_i$ reprezentują **prawdopodobieństwo** (przypadek dyskretny) lub **gęstość prawdopodobieństwa** (przypadek ciągły), że układ w stanie $|\psi\rangle$ po pomiarze znajdzie się w stanie $|\psi_i\rangle$

Przykład: stan układu dany przez $(|a\rangle + |b\rangle)/\sqrt{2}$ oznacza, że układ z równym prawdopodobieństwem znajduje się zarówno w stanie $|a\rangle$, jak i w stanie $|b\rangle$.

Wnioski:

- Funkcja falowa zawiera w sobie informację o wszystkich potencjalnych stanach układu.
- Istnienie układu w którymś konkretnym stanie można zweryfikować wykonując pomiar. Wynik pomiaru otrzymamy zgodnie z rozkładem statystycznym zakodowanym w funkcji falowej.
- Do chwili pomiaru układ znajduje się w każdym z możliwych stanów jednocześnie.

Często różne stany wzajemnie się wykluczają, więc w języku przestrzeni Hilberta rozpinają ortogonalne do siebie podprzestrzenie. Do tych podprzestrzeni „dostać się” można poprzez rzutowanie.

Rzutowanie

W mechanice kwantowej taką operację opisują operatory rzutowe. Operator $|\psi\rangle\langle\psi|$ działa jak operator rzutujący na stan ψ,

$$(|\psi\rangle\langle\psi|)\,|\phi\rangle = |\psi\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle|\psi\rangle,$$

gdzie $\langle\psi|\phi\rangle$ określa „długość rzutu", czyli stopień przekrycia stanów ψ i ϕ, zaś $|\psi\rangle$ to „kierunek", na który następuje rzutowanie. Skalar i stan można zapisać w dowolnej kolejności.

Ciekawostka: (M. Le Bellac, rozdz.2) Jeśli $|m\rangle$ jest bazą w przestrzeni Hilberta, to elementy macierzowe operatora A w tej bazie otrzymuje się licząc

$$A_{mn} = \langle m|A|n\rangle.$$

Baza opisuje całą przestrzeń, a rzutowanie na całą przestrzeń jest operatorem tożsamościowym (jedynką), czyli

$$\sum_k |k\rangle\langle k| = 1.$$

Wobec tego dla złożenia operatorów otrzymujemy

$$(AB)_{mn} = \langle m|AB|n\rangle = \langle m|A1B|n\rangle = \sum_k \langle m|A|k\rangle\langle k|B|n\rangle = \sum_k A_{mk}B_{kn},$$

co jest regułą mnożenia macierzy.

Postulat 4

Stan kwantowy zmienia się w czasie zgodnie z zależnością

$$\psi(x,t) = \psi(x,0)e^{\frac{-i}{\hbar}Ht}.$$

- Tak więc, aby opisać przyszłość układu, musimy znać operator jego całkowitej energii H (hamiltonian).
- W większości przypadków taki operator można zdefiniować. Dla bardziej skomplikowanych układów (np. otwartych lub podlegających przejściom fazowym) zbudowanie hamiltonianu jest niemożliwe, gdyż sens ma jedynie średnia energia układu, a nie jego energia chwilowa.
- Postulat 4 odnosi się więc tylko do najprostszych, dobrze kontrolowanych przypadków.

Dygresja: symetrie a prawa zachowania.
Podejrzewamy (i jest to zgodne póki co z każdą naszą obserwacją), że

(1) *prawa fizyczne nie zmieniają się w czasie*,

(2) *prawa fizyczne w każdym punkcie są takie same*,

(3) *prawa fizyczne są takie same po obrocie układu współrzędnych*.

Te symetrie pozwalają wyprowadzić zasady zachowania!

Symetria	Operator	Zasada zachowania
(1) translacja w czasie	hamiltonian H	energii
(2) translacja w przestrzeni	pęd p	pędu
(3) obrót w przestrzeni	moment pędu L	momentu pędu

Dla zainteresowanych: patrz twierdzenie Emmy Noether.

Główne różnice między fizyką klasyczną a kwantową.

- Równania ruchu
  - klasycznie: określają dokładnie przyszłość i przeszłość obiektu,
  - kwantowo: zawierają wszystkie możliwe przyszłości obiektu.
- Opis układu
  - klasycznie: przez jego cechy (położenie, pęd, masa...),
  - kwantowo: przez stan (funkcję falową).
- Charakter układu
  - klasycznie: cząstka lub fala,
  - kwantowo: cząstka i fala.
- Chronologia
  - klasycznie: ścisłe następstwo zdarzeń, przyczynowość,
  - kwantowo: nie wiadomo.
- Świat
  - klasycznie: deterministyczny,
  - kwantowo: probabilistyczny.

Kwestia granicy między zachowaniem klasycznym a kwantowym jest dość skomplikowana. Należy uwzględnić:

- rozmiar układu,
- izolację układu od wpływu środowiska (eliminacja dekoherencji),
- brak pomiarów,
- styk pomiędzy częścią klasyczną a kwantową aparatury.

Układy dwustanowe

Przestrzeń dwustanową zbudować można w sposób zupełnie abstrakcyjny jako konstrukcję matematyczną.

Realizacja fizyczna wykorzystuje najczęściej elektrony i fotony.

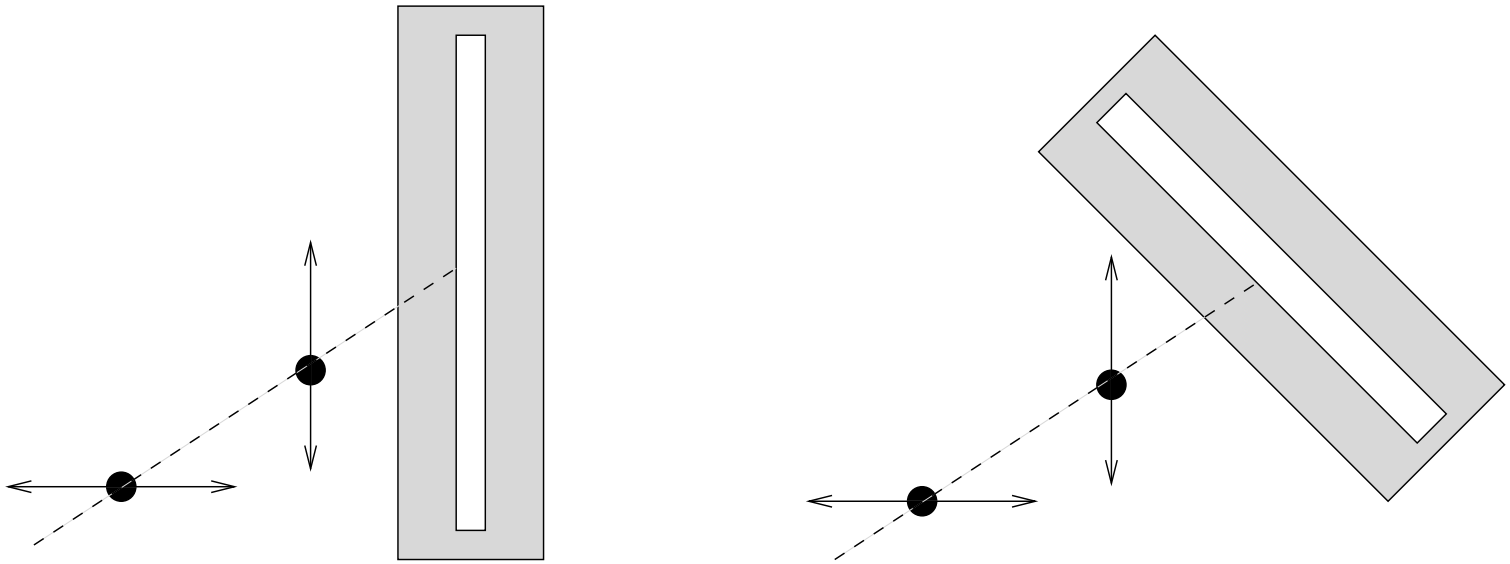
Spin elektronu

- Spin to „wewnętrzny" moment pędu cząstki.
- Spin fermionu wynosi $\frac{1}{2}\hbar$ i ma rzut na określony kierunek równy $\pm\frac{1}{2}\hbar$.

Polaryzacja fotonu

- Polaryzacja to kierunek drgań pola elektromagnetycznego.
- Polaryzacja liniowa pionowa i pozioma (względem umownego „poziomu") tworzą przestrzeń dwustanową.

Przykład: foton o polaryzacji liniowej natrafia na „przesłonę”.



Jak zachowa się układ?

- Klasycznie: przesłona zablokuje trzy cząstki, przepuści jedną.
- Kwantowo: przesłona zablokuje jedną cząstkę, przepuści trzy.

Podobnie zachowuje się spin, dlatego obie wielkości nadają się do zbudowania bazy w przestrzeni dwustanowej.

Wyjaśnienie na przykładzie spinu (dla polaryzacji jest analogicznie).

- W przypadku kwantowym przez przesłonę przejdzie cząstka, która ma niezerowy rzut spinu na kierunek przesłony.
- Cząstka ze spinem prostopadłym do przesłony ($\alpha = \pi/2$) ma rzut spinu równy

$$s\cos\alpha = \frac{\hbar}{2}\cos\left(\frac{\pi}{2}\right) = 0,$$

- cząstka ze spinem w kierunku 45° do przesłony ma rzut spinu równy

$$s\cos\alpha = \frac{\hbar}{2}\cos\left(\frac{\pi}{4}\right) = \frac{\hbar}{2}\frac{\sqrt{2}}{2} \neq 0.$$

Uwaga:

- Spin po przejściu przez przesłonę „odtwarza się”, czyli mierząc spin za przesłoną w dalszym ciągu otrzymamy $\hbar/2$. Dzieje się tak dlatego, że spin elektronu nie może mieć innej wartości!
- Wynika stąd, że możemy stosować całą serię rzutowań spinu na różne kierunki. Dopóki nie rzutujemy na kierunek prostopadły do spinu, spowodujemy jedynie jego obrót, bez zmiany wartości.

Uwaga: W przypadku fotonu, zablokowanie jednej składowej jego polaryzacji spowoduje utratę energii.

Pomiar

Funkcja falowa opisuje wszystkie możliwe do zmierzenia wartości parametrów danego obiektu.

- Pomiar to fizyczne oddziaływanie aparatury pomiarowej z badanym obiektem.
- Pomiar (również klasycznie) powoduje zaburzenie stanu układu.
- Istnieją obecnie tzw. pomiary słabe (niezaburzające, non-demolition measurements).

Co się dzieje w momencie pomiaru?

Następuje „kolaps funkcji falowej”, który matematycznie oznacza wyrzutowanie funkcji falowej na jedną z podprzestrzeni. Pomiar modyfikuje funkcję falową w zgodzie z wynikiem pomiaru. **Informacja zawarta w funkcji falowej przed pomiarem jest tracona.** Jest to operacja nieodwracalna.

Dodatkowo:

- Pomiar ustala wartość mierzonej wielkości. Jeśli funkcja falowa ma postać

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|\psi_1\rangle + |\psi_2\rangle + |\psi_3\rangle),$$

  to po pomiarze będzie zredukowana do $|\psi_1\rangle$, $|\psi_2\rangle$ lub $|\psi_3\rangle$.
- Pomiar niszczy kwantową superpozycję związaną z mierzoną wielkością, jest więc operacją nieodwracalną.
- Można jednak wykonać pomiar tak, aby utrzymać cechy kwantowe obiektu. Wiąże się to często z „nieodczytaniem" wyniku.
- Pomiary w obwodach kwantowych muszą być wykorzystywane bardzo ostrożnie. Pomiarem jest np. samoistne oddziaływanie obwodu ze środowiskiem oraz oddziaływanie elementów obwodu między sobą. Takie oddziaływanie prowadzi do **dekoherencji** czyli niekontrolowanego zaburzenia (zniszczenia) stanu kwantowego.

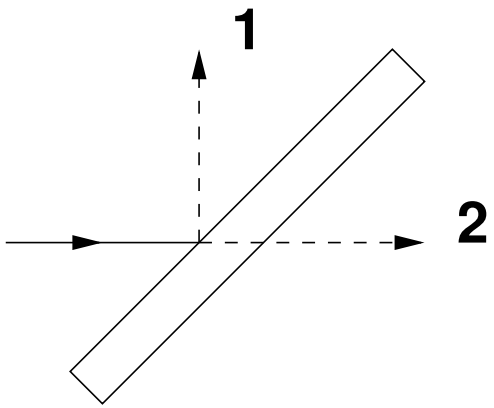
Przykład: foton pada na płytkę półprzepuszczalną (beamsplitter, BS).

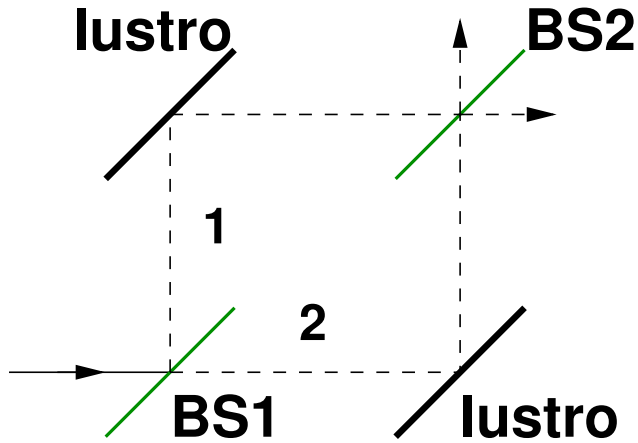
- Płytka półprzepuszczalna w 50% odbija światło, w 50% przepuszcza. Jest to proces losowy. (Istnieją też płytki z innym rozkładem, np. 30/70, ale musi to być jawnie podane.)
- Foton po natrafieniu na płytkę znajdzie się w stanie

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\text{odbity}\rangle + |\text{przepuszczony}\rangle),$$

  o ile żaden detektor nie ustali, co się z nim stało.
- Jeśli określimy w dowolny sposób, co płytka zrobiła z fotonem, jego stan będzie albo $|\text{odbity}\rangle$, albo $|\text{przepuszczony}\rangle$.

Sama płytka półprzepuszczalna (szczeliny w doświadczeniu Younga, przesłona z poprzedniego przykładu) nie wykonuje pomiaru, jeśli nie jest dodatkowo obserwowana.





Po przejściu przez BS1 foton będzie znajdował się na dwóch ścieżkach jednocześnie:

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

Jeśli drogi 1 i 2 spotkają się, np. w BS2, foton z jednej z nich będzie oddziaływał ze sobą z drugiej z nich. Tłumaczy to wersję doświadczenia dwuszczelinowego wykonywanego na pojedynczych cząstkach.

Podsumowując:

- każda operacja na stanie kwantowym jest oddziaływaniem,
- nie każde oddziaływanie jest pomiarem,
- „pomiar z odczytem wyniku" powoduje redukcję funkcji falowej i jest operacją nieodwracalną,
- „pomiar bez odczytu wyniku" modyfikuje stan, ale pozwala zachować cechy kwantowe.

Istnieją również tzw. **pomiary słabe**, które wytrącają układ ze swojego stanu na tyle delikatnie, że jest on w stanie samoistnie wrócić do stanu sprzed pomiaru.

S.Haroche, D.Wineland, nagroda Nobla 2012: *„for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems"*.

`www.nobelprize.org/prizes/physics/2012/summary/`

Cechy pomiaru a informatyka kwantowa

W sytuacji idealnej, całkowicie zgodnej z teorią, reguły działania naszego świata zabezpieczają dane w kanale kwantowym.

- Wszelkie próby przejęcia, podsłuchania, modyfikowania transmisji opartej na przesyle informacji kanałem kwantowym natychmiast niszczą strukturę przesyłanych danych (pomiar!).
- Podsłuchane kubity można odnaleźć, oznaczyć jako uszkodzone i ponowić dla nich transmisję.
- Charakter transmisji kwantowej do pełnego odczytania danych wymaga, oprócz podsłuchanych bitów, również pewnej dodatkowej informacji. Jeśli jest podejrzenie podsłuchu, te dodatkowe informacje dla uszkodzonych bitów nie są przesyłane.
- Teoretycznie kanał kwantowy jest w pełni bezpieczny, gdyż niemożliwy jest niezauważony podsłuch.

Więcej na ten temat w części wykładu poświęconej bezpieczeństwu.

Splątanie, pary EPR

Stan dwóch cząstek może mieć **postać iloczynową**, np.

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle|\uparrow\rangle + |\uparrow\rangle|\downarrow\rangle) = \frac{1}{\sqrt{2}}|\uparrow\rangle(|\uparrow\rangle + |\downarrow\rangle)$$

albo

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

Przestrzeń opisująca stan takiego układu ma strukturę iloczynu

$$\mathcal{H}_2 = \mathcal{H} \otimes \mathcal{H}.$$

Stan separowalny (iloczynowy) opisuje cząstki, które są od siebie niezależne. W ogólności dotyczy to dowolnej liczby obiektów.

Stan splątany jest nieseparowalny, czyli nie da się rozważać stanu jednej cząstki z pominięciem drugiej. Przestrzeni nie da się rozłożyć na dwie osobne podprzestrzenie odpowiadające każdej z cząstek. Przykładowe stany splątane:

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle + |\downarrow\rangle|\uparrow\rangle)$$

albo

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

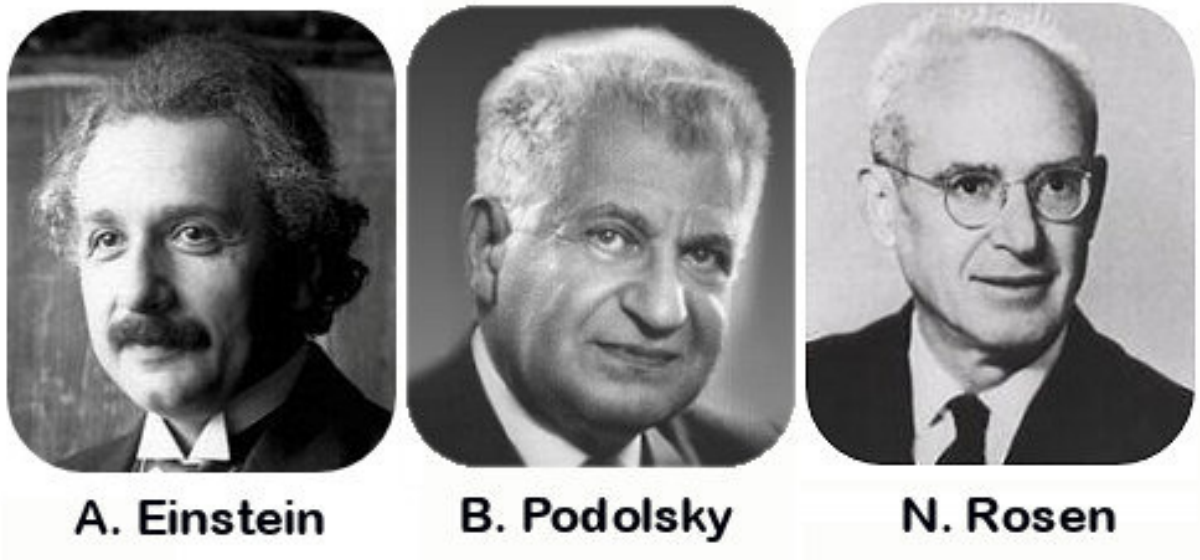
Takie pary muszą być opisywane jako całość.
Co łączy parę cząstek splątanych? Zasada zachowania. Na przykład dla pary opisanej pierwszym stanem powyżej spełniona jest zasada zachowania całkowitego spinu $s = 0$.

Uwagi:

- Cząstki splątane podali jako przykład dyskredytujący mechanikę kwantową Einstein, Podolski i Rosen, stąd nazwa **para EPR**.

  A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. 47 (1935) 777.

- Zjawisko splątania opisał dokładniej Schrödinger w liście do Einsteina twierdząc, że jest to świetny przykład, jak działa mechanika kwantowa. Teraz wiemy, że Schrödinger miał rację.



- Okazało się, że zachowanie cząstek EPR jest w doskonałej zgodności z fizyką, potwierdzając słuszność mechaniki kwantowej.
- Parę EPR można stworzyć i rozdzielić przestrzennie; manipulując jedną cząstką jednocześnie musi reagować druga cząstka – nie pozwala to jednak na nieskończenie szybkie przesyłanie informacji.
- Pary EPR są wykorzystywane w niektórych algorytmach kwantowych, m.in. teleportacji.

Podsumowując, układy kwantowe mają wiele cech potencjalnie przydatnych w informatyce. W idealnym przypadku:

- można pracować na fizycznych układach dwustanowych,
- superpozycja stanów pozwala na zrównoleglenie obliczeń,
- cechy pomiaru uniemożliwiają niezauważalny podsłuch,
- ewolucja czasowa stanu jest unitarna, czyli odwracalna, czyli pozbawiona strat energii, co wyklucza błędy,
- każdy wynik jest obarczony rozrzutem statystycznym, przez co obliczenia należy powtarzać.

Osobną kwestią jest rzeczywista realizacja układów kwantowych, której nie można wykonać w sposób idealny!

Pytanie: Dlaczego nie można zrealizować układu kwantowego w sposób idealny?

Podstawy informatyki kwantowej

Aby stworzyć informatykę w oparciu o układy kwantowe, należy zastanowić się nad kwantową wersją algebry Boole'a, której nie można przenieść bezpośrednio do mechaniki kwantowej:

- ze względu na unitarność ewolucji kwantowej, operacje kwantowe powinny być odwracalne,
- oznacza to m.in., że muszą one mieć tyle samo argumentów wejściowych, co wynikowych,
- warunku tego nie spełniają AND i OR.

Operacje AND i OR nie są odwracalne, nie posiadają więc swoich bezpośrednich wersji kwantowych. Można jednak zbudować ich kwantowe odpowiedniki korzystając z innych bramek.

Wprowadźmy przestrzeń Hilberta $\mathcal{H}$ o wymiarze dwa. Wtedy:

- elementy tej przestrzeni będą dwuwymiarowymi wektorami,
- wektory te można dodawać i skalować tworząc kombinacje liniowe z zespolonymi współczynnikami,
- każde dwa ortogonalne wektory będą tworzyły bazę w $\mathcal{H}$,
- wektory bazowe zawsze można unormować,
- baz w przestrzeni $\mathcal{H}$ jest nieskończenie wiele.

Można wyróżnić jedną z baz i interpretować jej wektory jako bity 0 i 1.

Przyjmijmy, że bity 0 i 1 reprezentowane są przez dwa stany $|0\rangle$ i $|1\rangle$. Niech te stany będą ortonormalne, czyli:

$$\text{unormowane: } \langle 0|0\rangle = \langle 1|1\rangle = 1,$$
$$\text{ortogonalne: } \langle 0|1\rangle = 0.$$

Wygodna jest reprezentacja w postaci wektorów kolumnowych:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Stany $\{|0\rangle, |1\rangle\}$ tworzą **bazę obliczeniową**. Te same rachunki można prowadzić dla różnych baz. Końcowy wynik nie powinien zależeć od wyboru bazy (fizyka jest niezależna od opisu matematycznego).

Sprawdzenie: można łatwo pokazać, że reprezentacja wektorowa jest unormowana i ortogonalna:

$$\langle 0|0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \cdot 1 + 0 \cdot 0 = 1,$$

$$\langle 1|1\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \cdot 0 + 1 \cdot 1 = 1,$$

$$\langle 0|1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1 \cdot 0 + 0 \cdot 1 = 0.$$

Kubit czyli bit kwantowy, to obiekt o strukturze

$$|q\rangle = c_0|0\rangle + c_1|1\rangle,$$

przy czym $|c_0|^2 + |c_1|^2 = 1$.

Zespolone współczynniki c_0 i c_1 mają interpretację **amplitud prawdopodobieństwa**. Prawdopodobieństwa znalezienia układu opisanego przez $|q\rangle$ w stanie $|0\rangle$ lub $|1\rangle$ to odpowiednio

$$p_0 = |c_0|^2 = c_0^* c_0 \qquad \text{i} \qquad p_1 = |c_1|^2 = c_1^* c_1,$$

gdzie, zgodnie z definicją,

$$p_0 + p_1 = |c_0|^2 + |c_1|^2 = 1.$$

Bit klasyczny to kubit, który jest cały czas podglądany.

Komputer klasyczny jest komputerem kwantowym, podglądanym na każdym etapie działania.

Charles H. Bennett

Insights from physics into information theory and vice versa

Lubelski Festiwal Nauki, 23.IX.2021

Kubit:

- jest kombinacją liniową stanów $|0\rangle$ i $|1\rangle$,
- operacje na kubitach mogą być wykonywane jednocześnie na $|0\rangle$ i $|1\rangle$,
- możliwa jest interferencja kubitów, prowadząca do wygaszenia lub wzmocnienia którejś z wartości,
- kubit można obrócić o pewien kąt („dopisać do niego globalną fazę") $e^{i\alpha}|q\rangle$, co nie zmieni prawdopodobieństw, ponieważ

$$|e^{i\alpha}c_0|^2 = |e^{i\alpha}|^2|c_0|^2 = e^{i\alpha}e^{-i\alpha}|c_0|^2 = |c_0|^2, \qquad |e^{i\alpha}c_1|^2 = |c_1|^2,$$

- względna faza między dwoma kubitami gra rolę, ponieważ zmieni wartość ich iloczynu skalarnego,

$$\langle\psi|e^{i\alpha}\phi\rangle = e^{i\alpha}\langle\psi|\phi\rangle \neq \langle\psi|\phi\rangle.$$

Konstrukcja kubitu jest podstawą **kwantowego zrównoleglenia**.

Często potrzebne są **stany wielokubitowe**. Jeśli pojedynczy kubit reprezentuje stan z przestrzeni Hilberta $\mathcal{H}$, to stan dwukubitowy będzie należał do iloczynu dwóch przestrzeni, $\mathcal{H}_2 = \mathcal{H} \otimes \mathcal{H}$.
Formalnie najpoprawniejszy zapis

$$|a\rangle \otimes |b\rangle$$

skracany jest zazwyczaj do

$$|a\rangle \otimes |b\rangle = |a\rangle|b\rangle = |ab\rangle.$$

Pamiętać tylko należy o kolejności: $|ab\rangle \neq |ba\rangle$.
Analogicznie tworzymy i opisujemy stany n–kubitowe z przestrzeni $\mathcal{H}_n = \mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}$ (n razy).

Przestrzeń $\mathcal{H}_2$ jest czterowymiarowa, dlatego też baza obliczeniowa w $\mathcal{H}_2$ składa się z czterech wektorów:

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle.$$

Ogólna postać kubitu z $\mathcal{H}_2$ to

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

przy czym oczywiście $|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$.
Jest to **rozwinięcie funkcji ψ w bazie** $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, ze współczynnikami rozwinięcia danymi przez c_{00}, c_{01}, c_{10}, c_{11}.

Każdą funkcję z danej przestrzeni można przedstawić w dowolnej bazie tej przestrzeni, dlatego operatory wystarczy zdefiniować poprzez ich działanie na stany bazowe jednej wybranej bazy.

Reprezentację wektorową bazy $\mathcal{H}_2$ tworzymy poprzez iloczyn diadyczny:

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

i podobnie:

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

Zadanie: Sprawdź trzy ostatnie wzory.

Bramki kwantowe

Rejestrem kwantowym o długości n nazywamy uporządkowany układ n kubitów. Jego przestrzenią stanów jest $\mathcal{H}_n = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$ (n razy). Stany bazowe dane są przez $\{|x\rangle : x \in \{0,1\}^n\}$. Jeśli utożsamimy rejestr kwantowy z zapisem binarnym liczb, odpowiada on liczbom $\{0, 1, \ldots, 2^n - 1\}$.

Bramką kwantową na n kubitach nazywamy odwzorowanie unitarne w przestrzeni $\mathcal{H}_n$, przekształcające rejestr kwantowy o długości n w rejestr kwantowy o długości n.

Obwodem kwantowym na n kubitach nazywamy odwzorowanie unitarne w przestrzeni $\mathcal{H}_n$, które można przedstawić w postaci złożenia skończonej liczby bramek kwantowych.

Teoria zazwyczaj opisuje sytuację wyidealizowaną. Konstruując obwody mające pracować w układach kwantowych należy pamiętać, że:

- każde przekształcenie unitarne jest odwracalne ($U^\dagger = U^{-1}$),
- fizyczne procesy mogą być odwracalne (ewolucja czasowa jest w teorii unitarna) lub nieodwracalne (pomiar),
- bramki nieodwracalne tracą część informacji (fizycznie odpowiada to dysypacji energii, najczęściej w postaci strat ciepła),
- pożądane jest, aby kwantowa bramka uniwersalna była odwracalna,
- żaden proces fizyczny nie jest dokładnie unitarny
  $\Rightarrow$ odtwarzanie zagubionej informacji,
  $\Rightarrow$ kwantowe algorytmy korekcji błędów (np. algorytm głosowania).

Bramki unarne (jednoargumentowe) ogólnie definiuje się przez ich działanie na stany bazowe $|0\rangle$ i $|1\rangle$:

$$U|0\rangle = a|0\rangle + b|1\rangle \qquad U|1\rangle = c|0\rangle + d|1\rangle$$

Cztery nieznane parametry a, b, c i d oznaczają, że U musi być czteroparametrowe. Ponieważ wektory bazowe są dwuwymiarowe, U będzie macierzą 2×2:

$$U\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}u_{11} & u_{12}\\ u_{21} & u_{22}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a & u_{12}\\ b & u_{22}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$$

$$U\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}u_{11} & u_{12}\\ u_{21} & u_{22}\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = c\begin{pmatrix}1\\0\end{pmatrix} + d\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}u_{11} & c\\ u_{21} & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$$

Mamy stąd:

$$U = \begin{pmatrix}a & c\\ b & d\end{pmatrix}$$

Negacja

Bramka negacji zdefiniowana jest przez macierz

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

Łatwo sprawdzić, że

$$|\bar{0}\rangle = \mathrm{NOT}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$|\bar{1}\rangle = \mathrm{NOT}|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Uwaga 1: Zaprzeczenie uzyskać też można poprzez XOR z jedynką: $|\bar{a}\rangle = |1 \oplus a\rangle$.

Uwaga 2: XOR w wersji kwantowej nazywa się CNOT.

Pierwiastek kwadratowy z negacji

Bramka „pierwiastek z negacji” zdefiniowana jest przez macierz

$$\sqrt{\mathrm{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

Dwukrotne użycie tej bramki prowadzi do zaprzeczenia:

$$\begin{aligned}
\sqrt{\mathrm{NOT}}^2 &= \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \\
&= \frac{1}{4}\begin{pmatrix} (1+i)^2+(1-i)^2 & 2(1+i)(1-i) \\ 2(1+i)(1-i) & (1+i)^2+(1-i)^2 \end{pmatrix} = \\
&= \frac{1}{4}\begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathrm{NOT}
\end{aligned}$$

Bramki binarne przyjmują dwa argumenty, a więc są odwzorowaniami typu $\mathcal{H}_2 \to \mathcal{H}_2$. Często wprowadza się bit kontrolny do bramek unarnych, który je „włącza" lub „wyłącza".

Dokładanie dodatkowych linii wejściowych związane jest z wymogiem równej liczby wejść i wyjść każdej bramki kwantowej. Linie kontrolne nie są zmieniane przez bramkę i ich wartości wejściowe są podawane na wyjścia. Zabieg ten pozwala na przeróbkę bramek klasycznych na ich odwracalne odpowiedniki kwantowe.

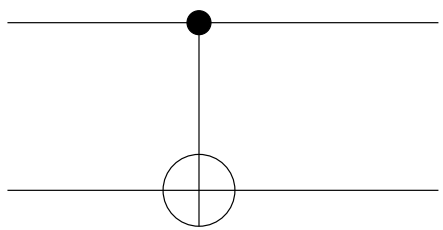
Kontrolowane NOT

Bramka CNOT (Controlled-NOT) zdefiniowana jest jako przekształcenie $\mathrm{CNOT} : \mathcal{H}_2 \to \mathcal{H}_2$ takie, że $\mathrm{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle$, czyli

$$\mathrm{CNOT}|0\rangle|x\rangle = |0\rangle|x\rangle,$$
$$\mathrm{CNOT}|1\rangle|x\rangle = |1\rangle|\bar{x}\rangle.$$

Reprezentacja macierzowa w bazie $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ to

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



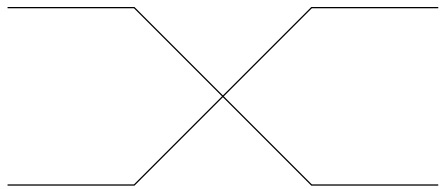
SWAP

Bramka SWAP zdefiniowana jest jako przekształcenie $\mathrm{SWAP} : \mathcal{H}_2 \to \mathcal{H}_2$ takie, że

$$\mathrm{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle.$$

Jej reprezentacja macierzowa i symbol

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Sama bramka SWAP jest rzadko wykorzystywana, ale jej kontrolowana wersja jest jedną z podstawowych kwantowych bramek uniwersalnych.

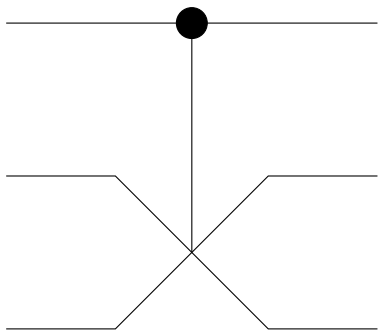
FREDKIN: kontrolowane SWAP

Bramka Fredkina (CSWAP) zdefiniowana jest jako przekształcenie $\mathrm{FREDKIN} : \mathcal{H}_3 \to \mathcal{H}_3$ takie, że

$$\mathrm{FREDKIN}|0\rangle|x\rangle|y\rangle = |0\rangle|x\rangle|y\rangle$$
$$\mathrm{FREDKIN}|1\rangle|x\rangle|y\rangle = |1\rangle|y\rangle|x\rangle$$

W bazie $\{000, 001, 010, 011, 100, 101, 110, 111\}$

$$\mathrm{FREDKIN} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$



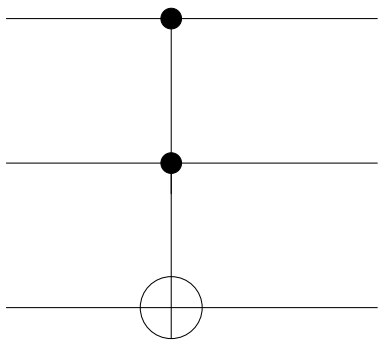
TOFFOLI: podwójnie kontrolowane NOT

Bramka Toffoliego (CCNOT) zdefiniowana jest jako przekształcenie $\mathrm{TOFFOLI} : \mathcal{H}_3 \to \mathcal{H}_3$ takie, że

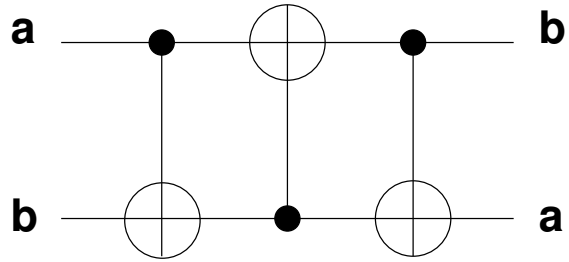
$$\mathrm{TOFFOLI}|1\rangle|1\rangle|x\rangle = |1\rangle|1\rangle|\bar{x}\rangle$$
$$\mathrm{TOFFOLI}|a\rangle|b\rangle|x\rangle = |a\rangle|b\rangle|x\rangle \qquad (a,b) \neq (1,1)$$

W bazie $\{000, 001, 010, 011, 100, 101, 110, 111\}$

$$\mathrm{TOFFOLI} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$



Bramki kwantowe można składać. Na przykład układ trzech bramek CNOT



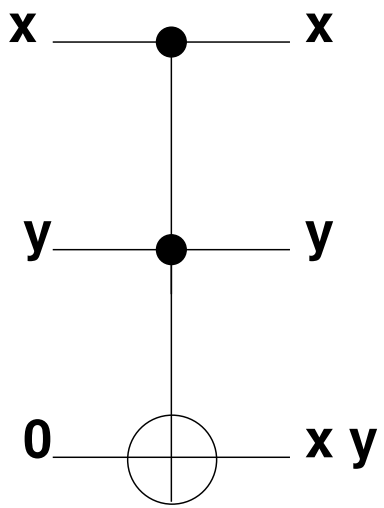
tworzy bramkę SWAP:

$$
\begin{aligned}
& \mathrm{CNOT}\ \mathrm{SWAP}\ \mathrm{CNOT}\ \mathrm{SWAP}\ \mathrm{CNOT}|a\rangle|b\rangle = \\
= \quad & \mathrm{CNOT}\ \mathrm{SWAP}\ \mathrm{CNOT}\ \mathrm{SWAP}|a\rangle|a\oplus b\rangle = \\
= \quad & \mathrm{CNOT}\ \mathrm{SWAP}\ \mathrm{CNOT}|a\oplus b\rangle|a\rangle = \\
= \quad & \mathrm{CNOT}\ \mathrm{SWAP}|a\oplus b\rangle|a\oplus b\oplus a\rangle = \\
= \quad & \mathrm{CNOT}|a\oplus b\oplus a\rangle|a\oplus b\rangle = \\
= \quad & |a\oplus b\oplus a\rangle|a\oplus b\oplus a\oplus a\oplus b\rangle = |b\rangle|a\rangle
\end{aligned}
$$

Twierdzenie

Bazę dla bramek odwracalnych stanowi trójka: NOT, CNOT, CCNOT.

Dowód:



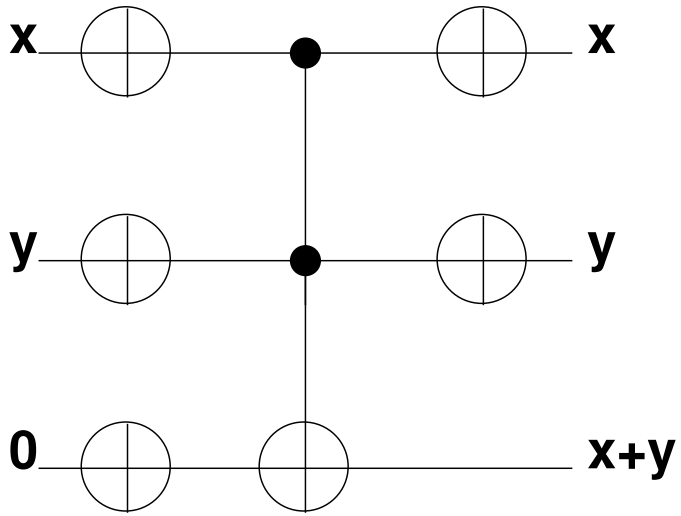


Tabela prawdy dla bramki „AND”:

x	y	CCNOT$(xy0)$
0	**0**	0 0 **0**
0	**1**	0 1 **0**
1	**0**	1 0 **0**
1	**1**	1 1 **1**

Tabela prawdy dla bramki „OR”:

x	y	$\bar{x}$	$\bar{y}$	CCNOT$(\bar{x}\bar{y}1)$
0	**0**	1	1	1 1 **0**
0	**1**	1	0	1 0 **1**
1	**0**	0	1	0 1 **1**
1	**1**	0	0	0 0 **1**

Bramka Hadamarda (Walsha)

Bramka Hadamarda zdefiniowana jest przez macierz

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

i służy do zamiany bazy $|0\rangle$, $|1\rangle$ na $H|0\rangle$, $H|1\rangle$.

Z definicji:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

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

Pytanie: Czy bramka H jest hermitowska?

Bramka H obraca bazę $|0\rangle, |1\rangle$. Nowa baza jest ortonormalna i można ją obrócić z powrotem do bazy prostej.

Właściwość 1: $H^2 = 1$.

$$\begin{aligned} HH|0\rangle &= H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \\ &= \frac{1}{2}2|0\rangle = |0\rangle. \end{aligned}$$

$$\begin{aligned} HH|1\rangle &= H\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) = \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \\ &= \frac{1}{2}2|1\rangle = |1\rangle. \end{aligned}$$

Właściwość 2: Baza H jest unormowana. Korzystając z poprzedniego wyniku otrzymujemy:

$$\langle 0|HH|0\rangle = \langle 0|0\rangle = 1,$$
$$\langle 1|HH|1\rangle = \langle 1|1\rangle = 1.$$

Właściwość 3: Baza H jest ortogonalna,

$$\langle 1|HH|0\rangle = \langle 1|0\rangle = 0.$$

Bramka Hadamarda używana jest w celu utworzenia równoważonej superpozycji stanów $|0\rangle$ i $|1\rangle$.

Przykład: w przypadku polaryzacji liniowej fotonu, H oznacza obrócenie płaszczyzny polaryzacji o $45°$.

Wielokubitowa transformata Hadamarda

Transformata H_n jest odwzorowaniem $\mathbb{R}^{2^n} \to \mathbb{R}^{2^n}$, przy czym $n = 0, 1, 2, \ldots$. Odwzorowywane liczby możemy zapisywać stosując notację binarną. H_n ma postać macierzy kwadratowej $2^n \times 2^n$ o wzorze rekurencyjnym

$$H_0 = 1, \qquad H_n = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}.$$

Powyższa definicja daje po kolei:

$$H_0 = 1,$$

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad \text{i tak dalej.}$$

W tym zapisie, w przestrzeni dwuwymiarowej bramka Hadamarda to H_1. Podana wcześniej definicja H_1 jest równoważna zapisowi

$$H_1|x\rangle = \frac{1}{\sqrt{2}}\left[(-1)^x|x\rangle + |1-x\rangle\right]$$

dla $x = 0, 1$.

Działanie bramki H_n na n-kubitowy rejestr $x \in \{0,1\}^n$ ma postać

$$H_n|x\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle,$$

gdzie „iloczyn” $x \cdot y$ to kombinacja AND i XOR,

$$x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n.$$

Zadanie: Sprawdź, poprawność wzoru $H_1|x\rangle = \frac{1}{\sqrt{2}}\left[(-1)^x|x\rangle + |1-x\rangle\right]$.

Policzmy działanie H_1 na oba wektory bazy obliczeniowej:

$$H_1|0\rangle = \frac{1}{\sqrt{2}}\Big[(-1)^0|0\rangle + |1-0\rangle\Big] = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]$$

$$H_1|1\rangle = \frac{1}{\sqrt{2}}\Big[(-1)^1|1\rangle + |1-1\rangle\Big] = \frac{1}{\sqrt{2}}\left[-|1\rangle + |0\rangle\right]$$

Zadanie: Korzystając z ogólnego wzoru na H_n policz $H_2|x\rangle$.

Mamy $H_n|x\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle$, więc przy $n=2$

$$\begin{aligned} H_2|00\rangle &= \frac{1}{2}\Big[(-1)^{0\cdot 0+0\cdot 0}|00\rangle + (-1)^{0\cdot 0+0\cdot 1}|01\rangle + \\ &\quad +(-1)^{0\cdot 1+0\cdot 0}|10\rangle + (-1)^{0\cdot 1+0\cdot 1}|11\rangle\Big] = \\ &= \frac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right] \end{aligned}$$

i podobnie pozostałe przypadki:

$$H_2|01\rangle = \frac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]$$
$$H_2|10\rangle = \frac{1}{2}\left[|00\rangle + |01\rangle - |10\rangle - |11\rangle\right]$$
$$H_2|11\rangle = \frac{1}{2}\left[|00\rangle - |01\rangle - |10\rangle + |11\rangle\right]$$

Wyniki są zgodne z podaną wcześniej postacią H_2:

$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Bramka zmiany fazy

Bramka zmiany fazy jest zdefiniowana przez macierz

$$F_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

Szczególny przypadek dla $\alpha = \pi$ ma postać

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

Widać, że F_π nie zmienia $|0\rangle$, natomiast odwraca znak przy $|1\rangle$,

$$F_\pi|0\rangle = |0\rangle, \qquad F_\pi|1\rangle = -|1\rangle.$$

Zmiana fazy $e^{i\alpha}$ odpowiada geometrycznie obrotowi stanu o kąt α. Fizycznie oznacza to obrót spinu elektronu lub płaszczyzny polaryzacji fotonu.

W literaturze spotyka się często bramki Pauliego. Są one oznaczane przez X, Y i Z, albo σ_x, σ_y i σ_z (są to tzw. macierze spinowe).

Bramki Pauliego

Bramki Pauliego w postaci macierzowej dane są przez

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Uwaga 1: bramka σ_x to NOT, zaś bramka σ_z to F_π.
Uwaga 2: bramki te reprezentują obroty o kąt π wokół odpowiednich osi, czyli obracają o 180° np. płaszczyznę polaryzacji fotonu.

Wśród bramek kwantowych można znaleźć zbiory bramek pozwalających na zbudowanie wszystkich obwodów. Udowadniane są **twierdzenia o uniwersalności bramek kwantowych** (patrz: M.Hirvensalo, par. 3.2.3). Dwa przykładowe podane są poniżej:

Twierdzenie

Używając jedynie bramek CNOT oraz bramek unarnych, można zbudować dowolny obwód kwantowy.

A.Barenco et al., PRA 52 (1995) 3457 [quant-ph/9503016].

Twierdzenie

Używając jedynie bramek Toffoliego (CCNOT) oraz Hadamarda (H), można zbudować dowolny obwód kwantowy.

Y.Shi, Quant. Inf. and Comp. 3 (2003) 84 [quant-ph/0205115].

Algorytmy kwantowe

Aby móc zrealizować jakikolwiek algorytm kwantowy, konieczne jest ustanowienie komunikacji pozwalającej na przesyłanie kubitów bez ich niszczenia.
Wprowadzamy rozróżnienie:

- **klasyczny kanał informacji** – pozwala na przesłanie bitów,
- **kwantowy kanał informacji** – pozwala na przesłanie kubitów.

Kanałem klasycznym jest np. telefon, list, mail, internet, kod flagowy...

Pytanie: Co może służyć za kanał kwantowy?

Czy Alicja, mając do dyspozycji tylko kanał klasyczny, może przesłać Bolkowi **nieznany** jej stan kwantowy?

Przypadek pierwszy: Alicja chce przesłać Bolkowi stan $|0\rangle$ albo stan $|1\rangle$.

- Alicja wysyła Bolkowi stan (na przykład) $|0\rangle$.
- Bolek odbiera stan, wykonuje pomiar. Dostaje 0, zaś stan, który mierzył nie ulega zmianie (a przynajmniej można zapewnić takie warunki, żeby nie uległ on zmianie).
- Oznacza to, że Alicja może przesłać taki stan, ale...
- ... stany bazy obliczeniowej odpowiadają klasycznym bitom!

Przypadek drugi: Alicja chce przesłać Bolkowi stan $a|0\rangle + b|1\rangle$, którego nie zna. Żeby to zrobić, musiałaby poznać współczynniki a i b.

- Jeśli wykona pomiar, otrzyma 0 lub 1 i zniszczy swój kubit.
- Chcąc oszacować liczby a i b trzeba wielokrotnie powtarzać pomiar aby otrzymać odpowiednią statystykę wyników. Niestety każdy pomiar zmienia mierzony kubit, a nieznanego kubitu nie można skopiować bez jego zniszczenia.
- Pomiary nie dają bezpośrednio informacji o a i b, tylko o $|a|^2$ i $|b|^2$. Nawet gdyby udało się poznać prawdopodobieństwa $|a|^2$ i $|b|^2$, nie pozwala to na jednoznaczne wyznaczenie a i b ze względu na możliwe fazy.

Widać więc, że dowolnego nieznanego stanu kwantowego nie można przesłać kanałem klasycznym. Jakakolwiek taka próba spowoduje zniszczenie kubitu i utratę informacji.

Protokół teleportacji kwantowej

Założenia:

- Alicja i Bolek są w posiadaniu pary EPR opisanej stanem splątanym $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Przyjmijmy, że pierwszy (lewy) kubit jest w posiadaniu Alicji, a drugi (prawy) w posiadaniu Bolka – cząstki są fizycznie rozseparowane.
- Dodatkowo Alicja posiada kubit $a|0\rangle + b|1\rangle$, który chce przesłać (teleportować) do Bolka.

Stan całego układu opisany jest przez stan

$$\begin{aligned} |\psi_0\rangle &= (a|0\rangle + b|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle), \end{aligned}$$

gdzie dwa lewe kubity znajdują się po stronie Alicji, a prawy kubit jest u Bolka.

Protokół:

1. Alicja wykonuje CNOT na kontrolowanych przez siebie kubitach, wykorzystując lewy jako kontrolny:

$$|\psi_1\rangle = (\mathrm{CNOT} \otimes 1)|\psi_0\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle).$$

2. Alicja wykonuje transformację Hadamarda na lewym kubicie

$$\begin{aligned} |\psi_2\rangle &= (H \otimes 1 \otimes 1)|\psi_1\rangle = \\ &= \frac{1}{2}[a(|0\rangle + |1\rangle)|00\rangle + a(|0\rangle + |1\rangle)|11\rangle + \\ &\quad + b(|0\rangle - |1\rangle)|10\rangle + b(|0\rangle - |1\rangle)|01\rangle], \end{aligned}$$

co można przepisać, wydzielając kubit Bolka (prawy), w postaci

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + \\ &\quad + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)]. \end{aligned}$$

3. Alicja przeprowadza pomiar swoich dwóch kubitów, ustalając stan całej trójki na jeden konkretny:

Pomiar Alicji	Stan układu po pomiarze
$\|00\rangle$	$\|00\rangle(a\|0\rangle + b\|1\rangle)$
$\|01\rangle$	$\|01\rangle(a\|1\rangle + b\|0\rangle)$
$\|10\rangle$	$\|10\rangle(a\|0\rangle - b\|1\rangle)$
$\|11\rangle$	$\|11\rangle(a\|1\rangle - b\|0\rangle)$

W każdym przypadku u Bolka cząstka jest w innym stanie.

4. Alicja przekazuje informację o swoim pomiarze Bolkowi za pomocą **kanału klasycznego**, np. mailem lub telefonicznie.

5. Bolek wykonuje jedną z czterech operacji na swojej cząstce:

Pomiar Alicji	Stan układu po obserwacji	Co robi Bolek
$\|00\rangle$	$\|00\rangle(a\|0\rangle + b\|1\rangle)$	nic
$\|01\rangle$	$\|01\rangle(a\|1\rangle + b\|0\rangle)$	NOT
$\|10\rangle$	$\|10\rangle(a\|0\rangle - b\|1\rangle)$	F_π
$\|11\rangle$	$\|11\rangle(a\|1\rangle - b\|0\rangle)$	F_π NOT

Sprowadza to kubit Bolka do stanu $a|0\rangle + b|1\rangle$.

Teleportacja polega na **przeniesieniu stanu kubitu**, nie fizycznego przeniesienia cząstek kodujących kubit. Stan jest **przenoszony**, a nie **kopiowany**, gdyż po stronie Alicji ulega on zniszczeniu.

Uwaga: Teleportacja jest możliwa do zrealizowania ze względu na **nierozróżnialność** cząstek w parze EPR.

Teleportacja była wykonana wielokrotnie, z wykorzystaniem coraz bardziej złożonych obiektów.

Zadanie: Poszukać informacji na temat doświadczeń badających teleportację różnych cząstek: fotonów, atomów itd.

Zadanie: Znaleźć informację o oszacowaniu, ile trwałaby teleportacja człowieka na Księżyc przy obecnym stanie technologii.

Teleportacja lub jakiś jej odpowiednik ma pełnić rolę szyny danych w komputerze kwantowym (chyba że wymyślimy coś lepszego).

Uwaga: różne źródła podają te same algorytmy w nieco innej konwencji. Niektóre operacje wraz z kolejnością ich wykonywania są kwestią umowy i można je do pewnego stopnia zmienić.

Uzupełnienie: macierz gęstości, entropia, twierdzenie Holevo.

W nowocześniejszym ujęciu mechanikę kwantową buduje się z wykorzystaniem **macierzy gęstości** ρ. Jest to opis ogólniejszy, gdyż pozwala uwzględnić fakt, że nie wszystko wiemy o opisywanym układzie. Dzieje się tak, ponieważ:

- zazwyczaj idealizujemy nasz opis,
- nie jesteśmy w stanie całkowicie zdefiniować granic układu,
- nie jesteśmy w stanie całkowicie zdefiniować procesów zachodzących wewnątrz układu (stosujemy np. przybliżenie cząstek swobodnych),
- nie jesteśmy w stanie całkowicie odciąć układ od jego otoczenia (wpływ środowiska powoduje często dekoherencję).

Formalizm macierzy gęstości pozwala na próby sformułowania teorii pomiaru kwantowego i kwantowej mechaniki statystycznej.

Właściwości operatora ρ:

- jest hermitowski, a więc ma rzeczywiste wartości własne,
- ma ortonormalny zupełny zbiór stanów własnych

$$\rho|i\rangle = p_i|i\rangle,$$

gdzie $\langle i|j\rangle = \delta_{ij}$ oraz $\sum_i |i\rangle\langle i| = 1$,

- układ ortonormalny i zupełny tworzy bazę, a więc ρ można zapisać w postaci

$$\rho = \sum_i p_i|i\rangle\langle i|.$$

Jeśli układ opisany jest funkcją falową ψ, to jego macierz gęstości ma postać

$$\rho = |\psi\rangle\langle\psi|.$$

Entropia jest miarą nieuporządkowania układu. Bez wykonania pracy przez siłę zewnętrzną, entropia układu nie zmaleje. W układach, w których energia nie jest tracona, $\Delta S = 0$.
Istnieje również entropia informacyjna, związana z przechowywaniem i przekazywaniem informacji. Jeśli entropia rośnie w układzie, dane są tracone. **Entropia von Neumanna** zdefiniowana jest jako

$$S = -\mathrm{Tr}(\rho \ \ln\rho).$$

Jeśli $\{|i\rangle\}$ to zbiór stanów własnych ρ, można ją zapisać w postaci diagonalnej jako $\rho = \sum p_i |i\rangle\langle i|$. W tym przypadku entropia przyjmuje postać

$$S = -\sum_i p_i \ \ln p_i.$$

Twierdzenie Holevo (1973)

Niech $\{\rho_1, \ldots, \rho_n\}$ będzie zbiorem stanów mieszanych, zaś $\{p_1, \ldots, p_n\}$ będzie odpowiadającym im rozkładem prawdopodobieństwa. Ilość informacji uzyskanej podczas pomiaru wykonanego na stanie $\rho = \sum p_i \rho_i$ ograniczona jest przez

$$I \leq S(\rho) - \sum_i p_i S(\rho_i).$$

A.Holevo, Problems of Information Transmission 9 (1973) 177.

Twierdzenie to oznacza w praktyce, że liczba bitów użytecznej klasycznej informacji, jaką można uzyskać z pojedynczego kubitu, wynosi jeden. Nie jest istotne, że kubity mogą być w superpozycji tysięcy stanów i że można wykonywać algorytm na wszystkich z nich jednocześnie. Odczyt wyniku wiąże się z koniecznością wykonania na końcu pomiaru, który zburzy charakter kwantowy mierzonego obiektu.

Kodowanie supergęste

C.H.Bennett, S.J.Wiesner, Phys. Rev. Lett. 69 (1992) 2881.

Pomimo twierdzenia Holevo, opracowano metodę zwaną **kodowaniem supergęstym** (lub po prostu kodowaniem gęstym), która pozornie pozwala na zakodowanie 2b informacji w pojedynczym kubicie.
Schemat:

- Alicja i Bolek mają po jednej cząstce z pary EPR.
- Alicja na swojej cząstce wykonuje jedną z czterech operacji unitarnych: 1, NOT, F_π, NOT F_π.
- Alicja wysyła swoją cząstkę do Bolka.
- Bolek wykonuje pomiar na obu cząstkach, wyznaczając operację wykonaną przez Alicję.
- Bolek otrzymuje jedną z czterech informacji, a więc 2 bity.

Przyjmijmy, że para EPR została przygotowana w stanie

$$\psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B),$$

gdzie lewy kubit (A) został u Alicji, a prawy (B) trafił do Bolka.
Alicja chce zakodować dwa bity klasyczne ab, więc:

1. jeśli $a = 1$, Alicja na swoim kubicie stosuje zmianę fazy F_π (dla przypomnienia, $F_\pi|0\rangle = |0\rangle$, $F_\pi|1\rangle = -|1\rangle$);
2. jeśli $b = 1$ Alicja na swoim kubicie stosuje negację NOT.

W ten sposób stan pary po transformacjach Alicji przybiera postać ψ_{ab}.

a	b	ψ_{ab}
0	0	$(\|00\rangle + \|11\rangle)/\sqrt{2}$
0	1	$(\|10\rangle + \|01\rangle)/\sqrt{2}$
1	0	$(\|00\rangle - \|11\rangle)/\sqrt{2}$
1	1	$(\|10\rangle - \|01\rangle)/\sqrt{2}$

Alicja przesyła swój kubit Bolkowi, który wykonuje pomiar na całej parze. Bramka pomiarowa Bolka dana jest przez

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

Ta bramka umożliwia rozróżnienie (odtworzenie) wszystkich czterech możliwych kombinacji bitów ab.

Zadanie: Pokazać, że macierz B jest unitarna, $B^\dagger = B^{-1}$.

Przykładowo, dla $ab = 00$ mamy:

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

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}\left[\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right] = \frac{1}{2}\left[\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}\right] =$$

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

Zadanie: Wykonać rachunki $B\psi_{ab}$ dla pozostałych trzech przypadków, $ab = 01$, $ab = 10$, $ab = 11$.

Ostatecznie pomiar Bolka powoduje zmianę stanu pary cząstek na stan zgodny z bitami Alicji.

a	b	ψ_{ab}	$B\psi_{ab}$
0	0	$(\|00\rangle + \|11\rangle)/\sqrt{2}$	$\|00\rangle$
0	1	$(\|10\rangle + \|01\rangle)/\sqrt{2}$	$\|01\rangle$
1	0	$(\|00\rangle - \|11\rangle)/\sqrt{2}$	$\|10\rangle$
1	1	$(\|10\rangle - \|01\rangle)/\sqrt{2}$	$\|11\rangle$

Wydaje się więc, że *kodowanie supergęste pozwala przesłać dwa bity klasycznej informacji za pomocą wymiany pojedynczej cząstki.*

Wytłumaczenie paradoksu w kodowaniu gęstym:

- Tak naprawdę, Alicja i Bolek **dwukrotnie** komunikowali się ze sobą, a więc **przesłali dwa bity informacji** w dwóch porcjach.
- Istotą kodowania gęstego jest, że pierwsza komunikacja (przesłanie cząstki EPR) mogła odbyć się dowolnie wcześniej, natomiast dopiero po przesłaniu drugiej cząstki przekazywane są dwa bity informacji.
- Informacja nie jest zakodowana w cząstce przesyłanej przez Alicję, ale w korelacji między cząstkami EPR. Dopóki cząstki są rozdzielone, korelacja nie jest bezpośrednio dostępna dla pomiarów.

Czy taki protokół przesyłania informacji jest bezpieczny? Przechwycenie przesyłanej cząstki przez Ewę blokuje kanał, ale nie pozwala na poznanie informacji, chyba, że Ewa zdobędzie obie cząstki.

Uwagi:

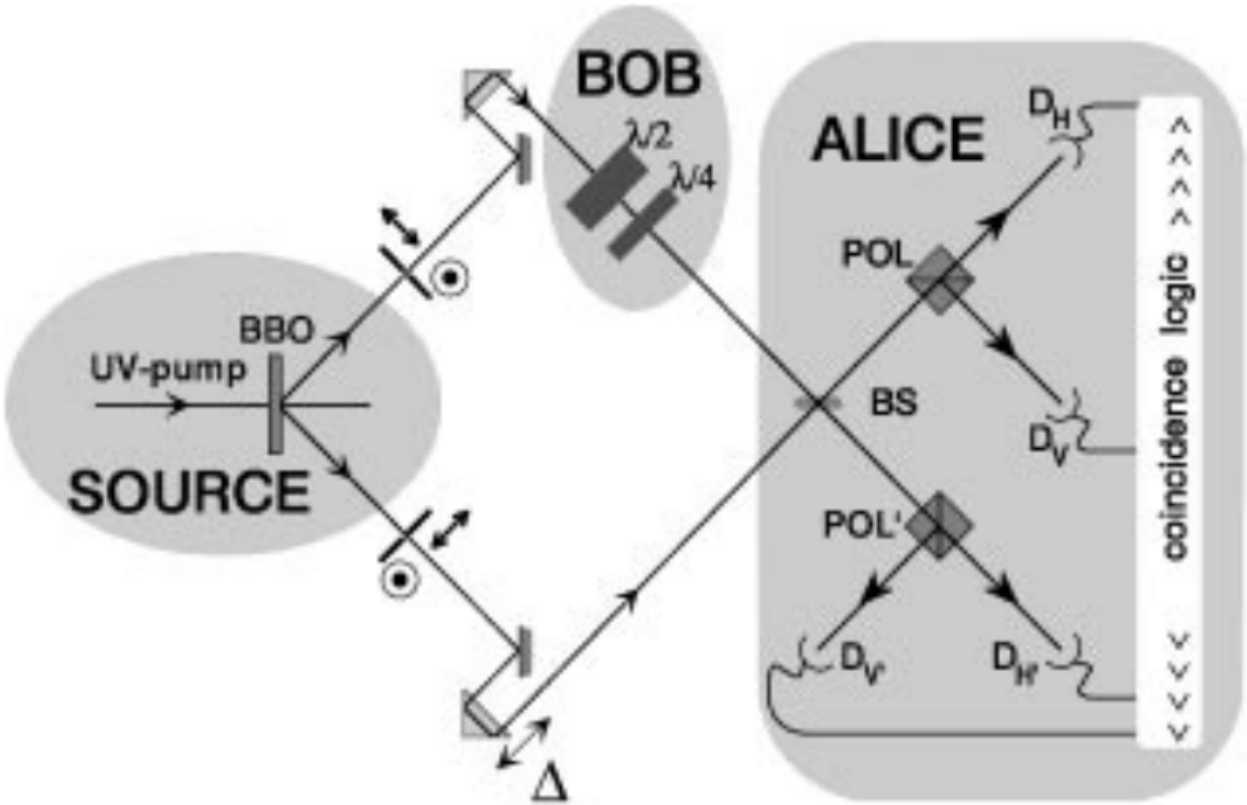
- Istnieje kilka wersji tego schematu, z różnymi przyporządkowaniami operacji Alicji do stanów i różnymi operacjami wykonywanymi przez Bolka.
- Pierwsza weryfikacja doświadczalna kodowania gęstego została dokonana w 1995 r. przez grupę A.Zeilingera. Użyto fotonów splątanych polaryzacją. Przesyłano jedną z trzech (a nie czterech) możliwych informacji, uzyskując zgodnie z teorią 1,58b w pojedynczym kanale kwantowym.

  K.Mattle et al., Phys. Rev. Lett. 76 (1996) 4656.

- Kilka lat później wykonano doświadczenie w oparciu o jądrowy rezonans magnetyczny, uzyskując przesył 2b informacji.

  X.Fang et al., Phys. Rev. A61 (2000) 022307.

Układ pomiarowy w doświadczeniu K.Mattle'a i innych na fotonach opierał się na badaniu koincydencji zliczeń cząstek.



Algorytm Deutscha

D.Deutsch, Proc. Royal Soc. London A 400 (1985) 97.

Algorytm Davida Deutscha pokazuje coś, co autor nazwał **kwantowym zrównolegleniem**. Ponieważ do obwodu kwantowego nie musimy wprowadzać czystego 0 lub czystej 1, ale ich kombinacje, obwód może wykonywać obliczenia na przygotowanej superpozycji.

Dana jest funkcja $f : \{0,1\} \to \{0,1\}$.
Problem: Określić, czy funkcja jest różnowartościowa.
Rozwiązanie klasyczne: Zbudować obwód realizujący $f(x)$ i wykorzystać go dwukrotnie, badając $f(0)$ i potem $f(1)$. Z wyników określić, czy funkcja jest różnowartościowa $f(0) \neq f(1)$.
Czas działania (klasycznie): Jeśli obwód potrzebuje czasu T na obliczenie wartości funkcji f, to całą operację przeprowadzić można w czasie $2T$.

Rozwiązanie za pomocą algorytmu kwantowego jest o połowę szybsze. Działanie funkcji f kodujemy w unitarnej operacji U_f następująco:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

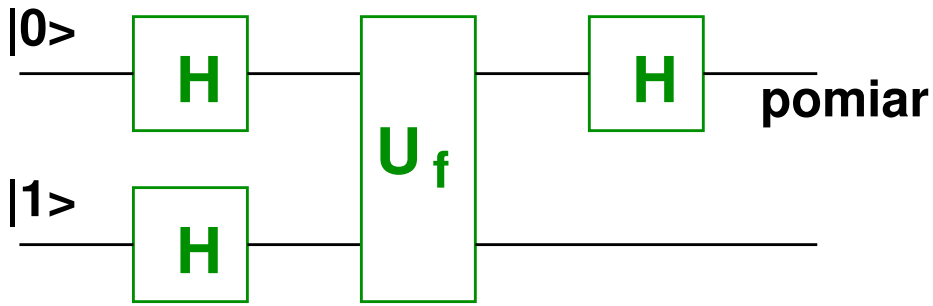
Uwagi:

1. U_f ma jednakową liczbę wejść i wyjść,
2. używanie U_f jest równoważne używaniu f, chociaż samego f do obwodu kwantowego wprowadzić nie można,
3. jeśli $f(x) = 1$, U_f zamienia drugi kubit na przeciwny, można więc zapisać działanie U_f jako

$$U_f|xy\rangle = \delta_{0\ f(x)}|xy\rangle + \delta_{1\ f(x)}|x\bar{y}\rangle,$$

gdzie δ_{ij} jest deltą Kroneckera ($\delta_{ii} = 1$, zero w pozostałych przypadkach).

Obwód zaproponowany przez Deutscha składa się z trzech bramek Hadamarda i jednej obliczającej funkcję f.



W pierwszym kroku oba bity są obracane przez bramkę H:

$$(H \otimes H)|01\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

W drugim kroku obliczana jest U_f,

$$
\begin{aligned}
& U_f \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
= \quad & \frac{1}{2}([\delta_{0\, f(0)}|00\rangle + \delta_{1\, f(0)}|01\rangle] - [\delta_{0\, f(0)}|01\rangle + \delta_{1\, f(0)}|00\rangle] + \\
+ \quad & [\delta_{0\, f(1)}|10\rangle + \delta_{1\, f(1)}|11\rangle] - [\delta_{0\, f(1)}|11\rangle + \delta_{1\, f(1)}|10\rangle]) = \\
= \quad & \frac{1}{2}\{|0\rangle[\delta_{0\, f(0)} - \delta_{1\, f(0)}](|0\rangle - |1\rangle) + |1\rangle[\delta_{0\, f(1)} - \delta_{1\, f(1)}](|0\rangle - |1\rangle)\} = \\
= \quad & \frac{1}{2}\{[\delta_{0\, f(0)} - \delta_{1\, f(0)}]|0\rangle + [\delta_{0\, f(1)} - \delta_{1\, f(1)}]|1\rangle\}(|0\rangle - |1\rangle).
\end{aligned}
$$

W trzecim kroku, do pierwszego kubitu stosujemy H:

$$\begin{aligned} & \frac{1}{2}\{[\delta_{0\,f(0)} - \delta_{1\,f(0)}]H|0\rangle + [\delta_{0\,f(1)} - \delta_{1\,f(1)}]H|1\rangle\}(|0\rangle - |1\rangle) = \\ = \quad & \frac{1}{2\sqrt{2}}\{[\delta_{0\,f(0)} - \delta_{1\,f(0)}](|0\rangle + |1\rangle) + \\ + \quad & [\delta_{0\,f(1)} - \delta_{1\,f(1)}](|0\rangle - |1\rangle)\}(|0\rangle - |1\rangle) = \\ = \quad & \frac{1}{2\sqrt{2}}(A|0\rangle + B|1\rangle)(|0\rangle - |1\rangle), \end{aligned}$$

gdzie

$$\begin{aligned} A &= \delta_{0\,f(0)} - \delta_{1\,f(0)} + \delta_{0\,f(1)} - \delta_{1\,f(1)}, \\ B &= \delta_{0\,f(0)} - \delta_{1\,f(0)} - \delta_{0\,f(1)} + \delta_{1\,f(1)}. \end{aligned}$$

Tak więc wynik działania algorytmu Deutscha na $|01\rangle$ to

$$\begin{aligned} D|01\rangle &= \frac{1}{2\sqrt{2}}(A|0\rangle + B|1\rangle)(|0\rangle - |1\rangle), \\ A &= \delta_{0\,f(0)} - \delta_{1\,f(0)} + \delta_{0\,f(1)} - \delta_{1\,f(1)}, \\ B &= \delta_{0\,f(0)} - \delta_{1\,f(0)} - \delta_{0\,f(1)} + \delta_{1\,f(1)}. \end{aligned}$$

Widać, że

- jeśli $f(0) = f(1)$ to $A = \pm 2$, $B = 0$,
- jeśli $f(0) \neq f(1)$ to $A = 0$, $B = \pm 2$.

Wniosek: Jeśli pomiar pierwszego kubitu daje $|0\rangle$, funkcja f jest stała, natomiast jeśli pomiar wynosi $|1\rangle$, to funkcja jest różnowartościowa.
Czas działania (kwantowo): Operacja U_f wykonana została tylko raz, więc czas wykonania algorytmu wynosi T.

Przykład. Niech $f(0) = 1$, $f(1) = 0$. Działanie bramki U_f dane jest wtedy przez:

$$U_f|0\rangle|0\rangle = |0\rangle|f(0) \oplus 0\rangle = |01\rangle$$
$$U_f|0\rangle|1\rangle = |0\rangle|f(0) \oplus 1\rangle = |00\rangle$$
$$U_f|1\rangle|0\rangle = |1\rangle|f(1) \oplus 0\rangle = |10\rangle$$
$$U_f|1\rangle|1\rangle = |1\rangle|f(1) \oplus 1\rangle = |11\rangle$$

Wejście: $|01\rangle$

Bramki H:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Bramka U_f:

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

Bramka H na pierwszej linii:

$$(H \otimes 1)\frac{1}{2}(|01\rangle - |00\rangle + |10\rangle - |11\rangle) = \cdots = \frac{1}{\sqrt{2}}|1\rangle(|1\rangle - |0\rangle)$$

Przykład. Niech $f(0) = 1$, $f(1) = 1$. Działanie bramki U_f dane jest wtedy przez:

$$U_f|0\rangle|0\rangle = |0\rangle|f(0) \oplus 0\rangle = |01\rangle$$
$$U_f|0\rangle|1\rangle = |0\rangle|f(0) \oplus 1\rangle = |00\rangle$$
$$U_f|1\rangle|0\rangle = |1\rangle|f(1) \oplus 0\rangle = |11\rangle$$
$$U_f|1\rangle|1\rangle = |1\rangle|f(1) \oplus 1\rangle = |10\rangle$$

Wejście: $|01\rangle$

Bramki H:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Bramka U_f:

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

Bramka H na pierwszej linii:

$$(H \otimes 1)\frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle) = \cdots = \frac{1}{\sqrt{2}}|0\rangle(|1\rangle - |0\rangle)$$

Cechy algorytmów kwantowych

Projektując algorytmy kwantowe należy wziąć pod uwagę, że

- zrównoleglenie obliczeń uzyskać można pracując na superpozycji stanów $|0\rangle$ i $|1\rangle$,
- w superpozycji uwzględnić można dodatkową zasadę zachowania, tworząc cząstki splątane.

Ograniczenia:

- pomiar niszczy strukturę kwantową, więc nie można uzyskiwać z algorytmu wyników pośrednich,
- końcowy pomiar daje wynik z pewnym prawdopodobieństwem,
- aby zwiększyć prawdopodobieństwo odczytania prawidłowego wyniku algorytm (albo jego część) należy wykonać wielokrotnie.

UWAGA

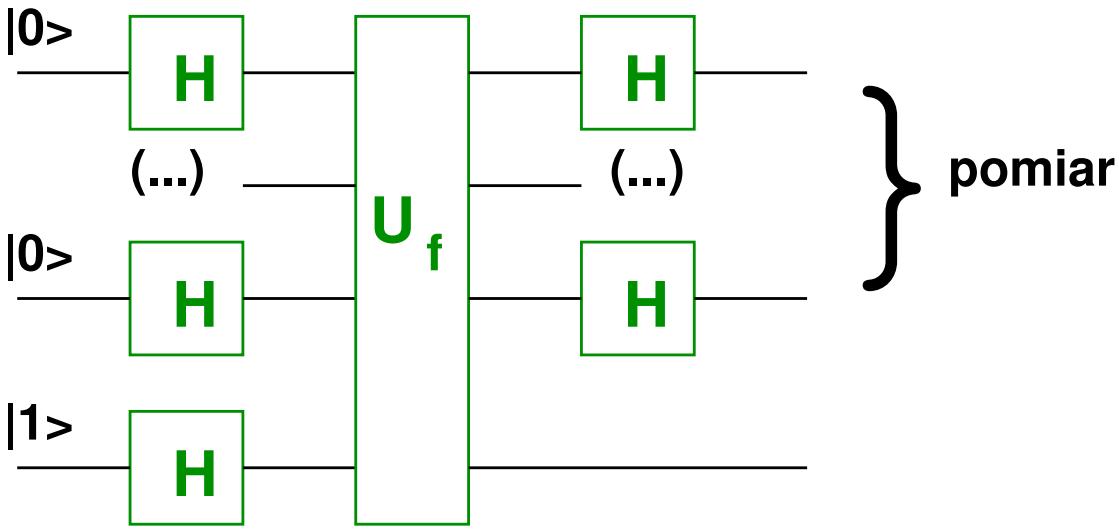
Układy kwantowe są bardzo skuteczne w przypadku niektórych problemów, bezużyteczne w przypadku innych!

Algorytm Deutscha–Jozsy

D.Deutsch, R.Jozsa, Proc. Royal Soc. London A 439 (1992) 553;

R.Cleve, A.Ekert, C.Macchiavello, M.Mosca, Proc. Royal Soc. London A 454 (1998) 339.

Jest to uogólnienie problemu Deutscha na funkcję n argumentów, $f : \{0,1\}^n \to \{0,1\}$. Wiemy, że f jest bądź stała [$f(x) = f(y)$ dla każdych dwóch argumentów], bądź zbalansowana [$f(x) = 0$ dla połowy argumentów].
Układ rozwiązujący problem, czy f jest stała, czy zbalansowana, ma postać:



Analiza tego algorytmu znajduje się m.in. w:

Z.Cao, J.Uhlmann, L.Liu, *Analysis of Deutsch–Jozsa Quantum Algorithm*, IACR Cryptology ePrint (2018), `eprint.iacr.org/2018/249.pdf`.

Stan wejściowy przygotowany jest jako $|0\rangle^n|1\rangle$.
$(n+1)$-kubitowa transformacja Hadamarda zamienia ten stan na

$$H_{n+1}|0\rangle^n|1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle).$$

Bramka U_f jest zdefiniowana podobnie jak poprzednio,

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

Użycie jej na stanie $H_{n+1}|0\rangle^n|1\rangle$ daje

$$U_f H_{n+1}|0\rangle^n|1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle).$$

Ponieważ jedynymi wartościami $f(x)$ są 0 i 1, stan układu można zapisać w postaci:

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

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

Do wszystkich kubitów oprócz ostatniego (prawego) stosujemy bramkę Hadamarda otrzymując

$$\frac{1}{\sqrt{2^{n+1}}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left[\sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right] (|0\rangle - |1\rangle).$$

Stan linii pomiarowych opisywany jest więc jako

$$\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \left[(-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle.$$

Prawdopodobieństwo zmierzenia stanu $|0\rangle^n$ dane jest przez podniesiony do kwadratu moduł współczynnika stojącego przy tym stanie.
Tak więc prawdopodobieństwo zmierzenia stanu $|0\rangle^n$ wynosi

$$P = \left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|^2.$$

Jeśli $f(x)$ jest funkcją stałą, $P \neq 0$.
Jeśli $f(x)$ jest funkcją zbalansowaną, $P = 0$.
Sprawdzając, czy pojawia się wynik $|0\rangle^n$ otrzymamy informację o funkcji f.

Algorytmy Deutscha i Deutscha-Jozsy zostały zrealizowane doświadczalnie pierwszy raz w 2003 r. z wykorzystaniem układu optycznego. W innym podejściu (tzw. „one-way computer") powtórzono doświadczenie cztery lata później.
Układy doświadczalne składały się z odpowiednio zestawionych interferometrów. We wszystkich przypadkach uzyskano zgodność z teorią.

M.Mohsani et al., Phys. Rev. Lett. 91 (2003) 187903.

M.S.Tame et al., Phys. Rev. Lett. 98 (2007) 140501.

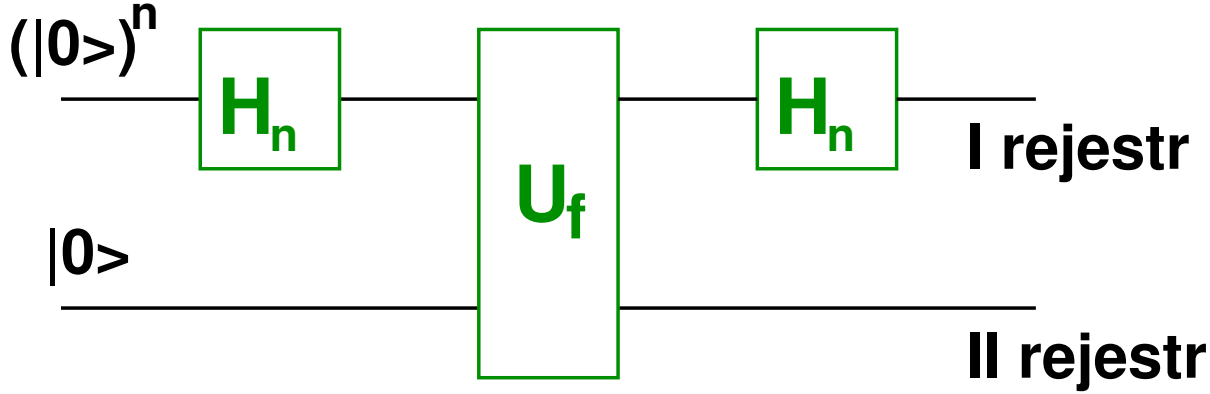
Algorytm Simona

D.R.Simon, SIAM Journal on Computing 26 (1997) 1474.

Algorytm Daniela Simona dotyczy efektywnego znalezienia okresu funkcji 2-do-1. Klasycznie problem ten ma złożoność wykładniczą (jest „trudny").

Dana jest funkcja 2-do-1 $f : \{0,1\}^n \to \{0,1\}^n$, która dla pewnego ciągu $a \in \{0,1\}^n$ ma właściwość: $f(x) = f(x \oplus a)$.
Problem: Znaleźć a.
Rozwiązanie klasyczne: Należy losować pary (x, y) sprawdzając, czy $f(x) = f(y)$.
Złożoność (klasycznie): Mając k losowań, możemy wylosować $k(k-1)/2$ różnych par. Każda z nich ma prawdopodobieństwo bycią tą właściwą równe $(1/2)^n$. Prawdopodobieństwo sukcesu równe jest Prob$= k(k-1)2^{-(n+1)}$. Np. dla ciągu 10 bitowego, aby Prob=95% potrzeba $k = 44,6$ losowań. Dla ciągu 1024b, $k = 1,3 \times 10^{154}$.

Obwód kwantowy realizujący algorytm Simona jest bardzo podobny do tego z algorytmu Deutscha.



Składa się z n-bitowych bramek Hadamarda i jednej obliczającej funkcję f:

$$H_n(|x\rangle)^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle,$$

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

Etap 1. Tworzymy równoważoną superpozycję wszystkich możliwych ciągów n-bitowych

$$H_n(|0\rangle)^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} (-1)^{0\cdot y}|y\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} |y\rangle.$$

Etap 2. Funkcja f:

$$U_f H_n(|0\rangle)^n|0\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y\in\{0,1\}^n} |y\rangle|f(y)\rangle.$$

Wykonujemy pomiar II rejestru. Odczyt wielkości $|f(y_0)\rangle$ świadczy o tym, że na rejestrze I jest stan $\frac{1}{\sqrt{2}}(|y_0\rangle + |y_0 \oplus a\rangle)$.

Etap 3. Kolejny obrót Hadamarda I rejestru:

$$H_n \frac{1}{\sqrt{2}}(|y_0\rangle + |y_0 \oplus a\rangle) = \left(\frac{1}{\sqrt{2}}\right)^{n+1} \sum_{y \in \{0,1\}^n} \left[(-1)^{y_0 \cdot y} + (-1)^{(y_0 \oplus a) \cdot y}\right] |y\rangle.$$

Pod sumą pozostają tylko stany, dla których $a \cdot y = 0$. Każdy z nich pojawi się w rejestrze I z Prob$= 1/2^{n-1}$.
Zgromadziwszy n liniowo niezależnych ciągów $y_1, \ldots, y_n$ rozwiązywany jest układ n równań liniowych $y_i \cdot a = 0$ i wyznaczane wszystkie n bitów ciągu a. **Potrzeba więc $\mathcal{O}(n)$ prób do rozwiązania problemu w przypadku kwantowym.**

Algorytm Grovera

L.K.Grover, Proc. 28th Annual ACM Symposium on the Theory of Computing (1996) 212.

Jest to optymalny algorytm przeszukiwania bazy danych. Można wykazać, że nie da się stworzyć szybszego algorytmu.

Mamy nieposortowaną bazę danych o $N = 2^n$ wpisach.
Problem: Znaleźć jeden konkretny wpis w.
Klasycznie: Przeszukiwanie będzie trwało $\mathcal{O}(N)$, gdyż każde zapytanie zwróci tylko „tak” lub „nie” i trzeba je wykonywać do skutku.

Cała przestrzeń stanów to $|w\rangle + |w^\perp\rangle$, gdzie $|w\rangle$ jest szukanym stanem, a $|w^\perp\rangle$ są wszystkimi innymi stanami. Oczywiście $\langle w|w^\perp\rangle = 0$.

Algorytm Grovera

Algorytm polega na wykonaniu na odpowiednio przygotowanym stanie serii obrotów:

$$R_{\text{Grover}} = U_w(U_sU_w)\dots(U_sU_w),$$

gdzie bramki zdefiniowane są następująco:

$$U_w = 1 - 2|w\rangle\langle w|, \qquad U_s = 2|s\rangle\langle s| - 1,$$

zaś s jest superpozycją wszystkich wpisów z bazy,

$$|s\rangle = H_N|0\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^N} |x\rangle.$$

Stan s jest tak wybrany, żeby jego przekrycie z dowolnym innym stanem było takie samo i wynosiło $\frac{1}{\sqrt{N}}$. W szczególności $\langle w|s\rangle = \frac{1}{\sqrt{N}}$.

Działanie bramek U_w i U_s można łatwo wyznaczyć:

$$
\begin{aligned}
U_w|w\rangle &= (1 - 2|w\rangle\langle w|)|w\rangle = |w\rangle - 2|w\rangle = -|w\rangle, \\
U_w|w^\perp\rangle &= (1 - 2|w\rangle\langle w|)|w^\perp\rangle = |w^\perp\rangle - 2 \cdot 0 = |w^\perp\rangle, \\
U_s|s\rangle &= (2|s\rangle\langle s| - 1)|s\rangle = 2|s\rangle - |s\rangle = |s\rangle, \\
U_s|s^\perp\rangle &= (2|s\rangle\langle s| - 1)|s^\perp\rangle = 0 - |s^\perp\rangle = -|s^\perp\rangle.
\end{aligned}
$$

Można je interpretować geometrycznie, jako odbicia względem hiperpłaszczyzn w 2^n-wymiarowej przestrzeni Hilberta.

U_w zmienia znak $|w\rangle$, nie zmienia $|w^\perp\rangle$, jest więc odbiciem względem hiperpłaszczyzny $|w^\perp\rangle$. **Jest obrotem o pewien kąt względem osi wyznaczonej przez $|w^\perp\rangle$.**

U_s jest odbiciem względem hiperpłaszczyzny, na której leży $|s\rangle$. **Jest obrotem o pewien kąt wokół osi wyznaczonej przez $|s\rangle$.**

Na wejście układu podajemy stan $|s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$.
Dokonujemy pojedynczego obrotu Grovera. U_w inaczej zadziała na $|w\rangle$ a inaczej na pozostałe stany, co daje:

$$\begin{aligned} U_s U_w |s\rangle &= U_s U_w \frac{1}{\sqrt{N}} \sum |x\rangle = \\ &\overset{(*)}{=} U_s \left[\frac{1}{\sqrt{N}} \sum |x\rangle - \frac{2}{\sqrt{N}} |w\rangle \right] = \\ &= U_s \left[|s\rangle - \frac{2}{\sqrt{N}} |w\rangle \right] = \\ &= |s\rangle - \frac{2}{\sqrt{N}} U_s |w\rangle. \end{aligned}$$

(*) Suma po x obejmuje również stan w, któremu U_w zmienia znak na przeciwny. Zamiast rozbijać sumę na $w + w^{\perp}$ zostawia się ją, natomiast w odejmuje dwukrotnie.

Działanie U_s na $|w\rangle$ można wyznaczyć z definicji $U_s = 2|s\rangle\langle s| - 1$:

$$\begin{aligned} U_s|w\rangle &= \left[2\frac{1}{\sqrt{N}}\sum_x |x\rangle \frac{1}{\sqrt{N}}\sum_{x'}\langle x'| - 1\right]|w\rangle = \\ &= \frac{2}{\sqrt{N}}\sum_x |x\rangle \frac{1}{\sqrt{N}}\sum_{x'}\langle x'|w\rangle - |w\rangle = \\ &= \frac{2}{\sqrt{N}}\frac{1}{\sqrt{N}}\sum_x |x\rangle - |w\rangle = \frac{2}{\sqrt{N}}|s\rangle - |w\rangle. \end{aligned}$$

Wracając do wyrażenia na stan po obrocie otrzymujemy:

$$\begin{aligned} U_s U_w|s\rangle &= |s\rangle - \frac{2}{\sqrt{N}}U_s|w\rangle = |s\rangle - \frac{2}{\sqrt{N}}\left(\frac{2}{\sqrt{N}}|s\rangle - |w\rangle\right) = \\ &= |s\rangle - \frac{4}{N}|s\rangle + \frac{2}{\sqrt{N}}|w\rangle = \frac{N-4}{N}|s\rangle + \frac{2}{\sqrt{N}}|w\rangle. \end{aligned}$$

Startowaliśmy ze stanu $|s\rangle$ będącego równoważoną superpozycją wszystkich wpisów z bazy. Po pojedynczym obrocie Grovera nowy stan ma zwiększoną domieszkę szukanego stanu $|w\rangle$. Można to sprawdzić licząc przekrycie (iloczyn skalarny) z szukanym stanem:

$$|\langle w|s\rangle|^2 = \left(\frac{1}{\sqrt{N}}\right)^2 = \frac{1}{N},$$

$$|\langle w|U_s U_w\ |s\rangle|^2 = \left(\frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}}\right)^2 = \frac{1}{N}\left(\frac{3N-4}{N}\right)^2 \approx \frac{9}{N}.$$

Jak widać, po obrocie stan układu zbliżył się do $|w\rangle$.

Ile obrotów należy wykonać, aby otrzymać maksymalne prawdopodobieństwo poprawnego wyniku algorytmu Grovera?
Działanie bramek U_w i U_s na superpozycje stanów można zapisać jako:

$$U_w(a|w\rangle + b|s\rangle) = \begin{pmatrix} |w\rangle & |s\rangle \end{pmatrix} \begin{pmatrix} -1 & \frac{-2}{\sqrt{N}} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

$$U_s(a|w\rangle + b|s\rangle) = \begin{pmatrix} |w\rangle & |s\rangle \end{pmatrix} \begin{pmatrix} -1 & 0 \\ \frac{2}{\sqrt{N}} & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Zadanie: Sprawdź, że powyższe przedstawienie macierzowe jest zgodne z definicją bramek i stanu $|s\rangle$. Warto pamiętać, że $\sum |x\rangle = |w^{\perp}\rangle + |w\rangle$.

Uzupełnienie: rozkład Jordana

Udowodniono twierdzenie, że każdą macierz kwadratową M można zapisać w postaci $M = SJS^{-1}$, gdzie J jest macierzą w postaci kanonicznej Jordana.

Oznacza to, że J jest blokowo diagonalna, z jedynkami występującymi ewentualnie zaraz nad główną przekątną każdego bloku:

$$J = \mathrm{diag}(J_1, J_2, \ldots, J_n),$$

gdzie wartości własnej α_k odpowiada blok

$$J_k = \begin{pmatrix} \alpha_k & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \alpha_k & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \alpha_k & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & \alpha_k & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & \alpha_k \end{pmatrix}.$$

Macierz $U_s U_w$ można przedstawić w postaci trygonometrycznej za pomocą rozkładu Jordana:

$$U_s U_w = \begin{pmatrix} 1 & \frac{2}{\sqrt{N}} \\ \frac{-2}{\sqrt{N}} & 1 - \frac{4}{N} \end{pmatrix} = \mathcal{U} \begin{pmatrix} e^{i2\alpha} & 0 \\ 0 & e^{-i2\alpha} \end{pmatrix} \mathcal{U}^{-1},$$

gdzie $\alpha = \arcsin(1/\sqrt{N})$, zaś

$$\mathcal{U} = \begin{pmatrix} -i & i \\ e^{i\alpha} & e^{-i\alpha} \end{pmatrix}.$$

Zadanie: Sprawdź, że

$$\mathcal{U}^{-1} = \frac{1}{e^{i\alpha} + e^{-i\alpha}} \begin{pmatrix} i\ e^{-i\alpha} & 1 \\ -i\ e^{i\alpha} & 1 \end{pmatrix}$$

i zweryfikuj rozkład $U_s U_w$.

Stosując t obrotów otrzymujemy operator

$$(U_s U_w)^t = \mathcal{U} \begin{pmatrix} e^{i2t\alpha} & 0 \\ 0 & e^{-i2t\alpha} \end{pmatrix} \mathcal{U}^{-1}.$$

Chcąc maksymalnie rozseparować stany $|s\rangle$ i $|w\rangle$ kąt obrotu musi być jak najbliższy $\pi/2$, czyli $2t\alpha \to \pi/2$. Stąd

$$t = \frac{\pi}{4\alpha} = \frac{\pi}{4 \arcsin(1/\sqrt{N})} \approx \sqrt{N}\frac{\pi}{4},$$

gdzie użyte przybliżenie dla niewielkich kątów ma postać $\arcsin(x) \approx x$.

Wniosek: Algorytm kwantowy potrzebuje $\mathcal{O}(\sqrt{N})$ prób, podczas kiedy algorytm klasyczny $\mathcal{O}(N)$.

Znajdowanie okresu funkcji

Dana jest funkcja

$$f : \{0,1\}^n \to \{0,1\}^m \Leftrightarrow \{0,1,\ldots,2^n-1\} \to \{0,1,\ldots,2^m-1\}$$

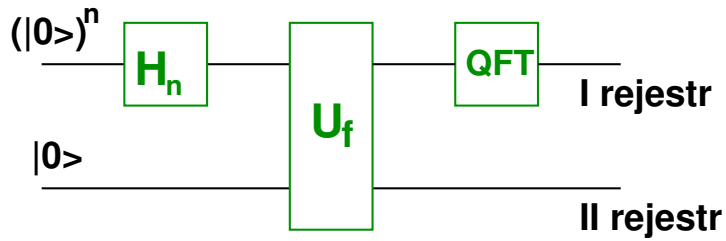
posiadająca okres r, $1 \ll r \ll 2^n$,

$$f(x) = f(x+\alpha r), \quad x+\alpha r \in \{0,1,\ldots,2^n-1\}$$

Problem: Znaleźć r.
Klasycznie: Jeśli $r \sim 2^{n/2}$, na średnio należy wykonać $\sqrt{r} \sim 2^{n/4}$ obliczeń funkcji f, aby mieć szansę znalezienia dwóch wartości argumentów różniących się o wielokrotność r. Czas działania jest wykładniczy w n, problem jest trudny.
Kwantowo: Algorytm kwantowy działa w czasie wielomianowym w n.

(1) Wejście jest $n+1$ kubitowe. Rejestr I (n kubitów) obracamy bramką Hadamarda:

$$H_n|0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle, \quad N \equiv 2^n.$$

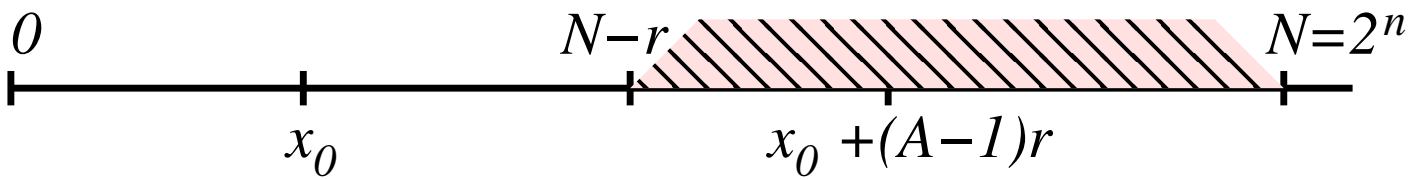


(2) Na rejestrach I i II umieszczamy bramkę U_f

$$U_f \frac{1}{\sqrt{N}} \sum_x |x\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle|f(x)\rangle.$$

(3) Jeśli wynik pomiaru rejestru II wyniósł $|f(x_0)\rangle$, $0 \leq x_0 < r$, to stan na rejestrze I ustalił się na

$$\frac{1}{\sqrt{A}} \sum_{\beta=0}^{A-1} |x_0 + \beta r\rangle, \qquad N - r \leq x_0 + (A-1)r < N.$$



Dygresja

Kwantowa transformata Fouriera (QFT)

$$\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}} |y\rangle$$

jest (dyskretnym) rzutowaniem stanu $|x\rangle$ na bazę $|y\rangle$.

Pomiar z rejestru II nie daje nam bezpośrednio informacji o r, ale

$$\mathrm{QFT}\frac{1}{\sqrt{A}} \sum_{\beta=0}^{A-1} |x_0 + \beta r\rangle = \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} \sum_{\beta=0}^{A-1} \exp\left(2\pi i \frac{x_0 + \beta r}{N} y\right) |y\rangle =$$

$$= \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} \exp\left(2\pi i \frac{x_0 y}{N}\right) \sum_{\beta=0}^{A-1} \exp\left(2\pi i \beta \frac{ry}{N}\right) |y\rangle.$$

Prawdopodobieństwo zmierzenia konkretnego stanu y' dane jest przez

$$\mathrm{Prob}(y') = \left| \langle y' | \mathrm{QFT} \frac{1}{\sqrt{A}} \sum_{\beta=0}^{A-1} |x_0 + \beta r\rangle \right|^2 ,$$

co można przekształcić (zadanie dla chętnych) do postaci

$$\mathrm{Prob}(y') = \frac{1}{NA} \frac{\sin^2(\pi r y' A/N)}{\sin^2(\pi r y'/N)}.$$

Można pokazać, że prawdopodobieństwo wylosowania y' odległego od kN/r $(k = 0, 1, ..., r-1)$ o co najwyżej $1/2$ wynosi nie mniej niż $4/\pi^2 \approx 0,4$. Jeśli k i r nie mają wspólnego dzielnika, to możliwe jest wyznaczenie r.
Prawdopodobieństwo, że dwa kolejno wylosowane k i k' nie mają wspólnego dzielnika jest duże $(6/\pi^2 \approx 0,6)$ i niezależne od N.
Wniosek: algorytm zakończy działanie w czasie wielomianowym, nie wykładniczym.

Bezpieczeństwo w układach kwantowych

Czy układy kwantowe są bezpieczniejsze niż klasyczne?

- Stany bazowe $|0\rangle$ i $|1\rangle$ można przeczytać i przesłać dalej.
- Stan $\alpha|0\rangle + \beta|1\rangle$ można przeczytać, otrzymując $|0\rangle$ bądź $|1\rangle$, czyli niszcząc informację o α i β. Takiego stanu nie można już odtworzyć.
- Czy stan kwantowy można skopiować? O tym za chwilę...
- Kubit łatwo ulega zniszczeniu, gdyż każde oddziaływanie może spowodować dekoherencję, czyli rozpad stanu kwantowego. Całkowita izolacja układu od środowiska jest niemożliwa.
- **To wszystko powoduje, że ani podsłuchu, ani większości innych „typowych" ataków nie da się w całości zamaskować.** (Chociaż można je niekiedy na tyle ukryć, że będą trudne do znalezienia...)

Twierdzenie o nieklonowaniu

W. K. Wootters, W. H. Żurek, Nature 299 (1982) 802.

Twierdzenie Wootersa – Żurka

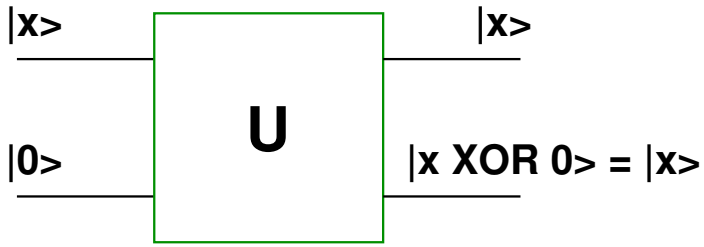
Nie istnieje kwantowa maszyna zdolna do tworzenia kopii nieznanego stanu kwantowego.

Istnienie takiej maszyny pozwalałoby na:

- skopiowanie nieznanego ciągu kubitów,
- wykonanie pomiaru na kopii,
- w konsekwencji poznanie ciągu kubitów bez ich zniszczenia.

Twierdzenie o nieklonowaniu jest podstawą do uznania idealnych kwantowych kanałów przesyłania danych jako **bezpiecznych**, czyli **niemożliwych do niezauważonego podsłuchania**.

Przykład: Twierdzenie o nieklonowaniu wydaje się łatwe do obalenia. Wystarczyć powinna na przykład operacja XOR z zerem.



$$U|x\rangle|0\rangle = |x\rangle|x \oplus 0\rangle = |x\rangle|x\rangle.$$

Co prawda dla wektorów bazowych wyniki są poprawne:

$$U|0\rangle|0\rangle = |0\rangle|0 \oplus 0\rangle = |0\rangle|0\rangle,$$
$$U|1\rangle|0\rangle = |1\rangle|1 \oplus 0\rangle = |1\rangle|1\rangle,$$

ale dla dowolnego kubitu już nie:

$$\begin{aligned} U(\alpha|0\rangle + \beta|1\rangle)|0\rangle &= \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq \\ &\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle). \end{aligned}$$

Dowód twierdzenia Woottersa – Żurka o nieklonowaniu

Przyjmijmy, że $|\chi\rangle$ jest nieznanym stanem kwantowym.
Maszyna kopiująca wykonywałaby więc operację polegającą na skopiowaniu tego stanu na inny stan $|\phi\rangle$. Reprezentujemy ją przez transformację unitarną $U : \mathcal{H}_2 \to \mathcal{H}_2$ tak, że

$$U|\chi\rangle|\phi\rangle = |\chi\rangle|\chi\rangle.$$

Załóżmy, że chcemy skopiować dwa stany, χ_1 oraz χ_2. Stany te nie są niczym ze sobą powiązane. Z definicji operatora U możemy napisać

$$\begin{cases} U|\chi_1\rangle|\phi\rangle = |\chi_1\rangle|\chi_1\rangle \\ U|\chi_2\rangle|\phi\rangle = |\chi_2\rangle|\chi_2\rangle \end{cases}$$

Drugie równanie sprzęgamy po hermitowsku, zgodnie z regułą $(AB)^\dagger = B^\dagger A^\dagger$, otrzymując:

$$\begin{cases} U|\chi_1\rangle|\phi\rangle = |\chi_1\rangle|\chi_1\rangle \\ \langle\phi|\langle\chi_2|U^\dagger = \langle\chi_2|\langle\chi_2| \end{cases}$$

Mnożąc oba równania stronami przez siebie otrzymujemy

$$\begin{aligned}\langle\phi|\langle\chi_2|U^\dagger U|\chi_1\rangle|\phi\rangle &= \Big(\langle\phi|\langle\chi_2|U^\dagger\Big)\Big(U|\chi_1\rangle|\phi\rangle\Big) = \\ &= \langle\chi_2|\langle\chi_2|\chi_1\rangle|\chi_1\rangle = \langle\chi_2|\chi_1\rangle\langle\chi_2|\chi_1\rangle = \\ &= \left(\langle\chi_2|\chi_1\rangle\right)^2.\end{aligned}$$

Z drugiej strony, ponieważ $U^\dagger U = 1$, mamy

$$\begin{aligned}\langle\phi|\langle\chi_2|U^\dagger U|\chi_1\rangle|\phi\rangle &= \langle\phi|\langle\chi_2|\chi_1\rangle|\phi\rangle = \langle\chi_2|\chi_1\rangle\langle\phi|\phi\rangle = \\ &= \langle\chi_2|\chi_1\rangle.\end{aligned}$$

Otrzymujemy więc

$$\langle\chi_2|\chi_1\rangle = (\langle\chi_2|\chi_1\rangle)^2,$$

czyli $\chi_1 = \chi_2$ lub $\langle\chi_2|\chi_1\rangle = 0$. Oba te warunki narzucają postać stanu χ_2 i są w sprzeczności z założeniem o jego dowolności.

Wnioski

- Kwantowa maszyna kopiująca zdolna kopiować dowolny stan nie istnieje.
- Kwantowa maszyna kopiująca istnieje dla stanów ortogonalnych, a więc stany bazowe możemy kopiować.

Oznacza to, że w idealnych obwodach kwantowych nie istnieje element działający jak rozgałęźnik, który pozwoliłby na powielanie stanów.

Silniejsze twierdzenie o nieklonowaniu

R. Jozsa, *A stronger no-cloning theorem*, quant-ph/0204153.

Twierdzenie Jozsy

Niech $x_1, ..., x_n$ będą ortonormalnymi wektorami z $\mathcal{H}_n$. Niech O będzie wektorem jednostkowym z $\mathcal{H}_n$ zaś $r_1, ..., r_k$ będą stanami z przestrzeni liniowej $\mathcal{L}(\mathcal{H}_m)$ wszystkich kombinacji liniowych wektorów z $\mathcal{H}_m$. Całkowicie dodatnie odwzorowanie $V \in \mathcal{H}_n \otimes \mathcal{H}_n \otimes \mathcal{H}_m$ takie, że dla każdego $i = 1, ..., k$

$$V\Big[|x_i\rangle\langle x_i| \otimes |O\rangle\langle O| \otimes r_i\Big] = |x_i\rangle\langle x_i| \otimes |x_i\rangle\langle x_i| \otimes r_i'$$

istnieje wtedy i tylko wtedy, gdy istnieje całkowicie dodatnie odwzorowanie $V' \in \mathcal{L}(\mathcal{H}_n \otimes \mathcal{H}_m)$ takie, że dla każdego $i = 1, ..., k$

$$V'\Big[|O\rangle\langle O| \otimes r_i\Big] = |x_i\rangle\langle x_i| \otimes r_i''.$$

Interpretacja i uwagi:

- Klonowanie (odwzorowanie V) stanu x_i wraz z dodatkową informacją r_i jest możliwe, jeśli z samej tylko r_i możliwe jest odtworzenie stanu x_i.
- Jeśli dodatkowy stan r_i nie zawiera pełnej informacji o klonowanym stanie, to klonowanie nie jest możliwe.
- Dla $r_1 = r_2 = ... = r_k$ twierdzenie Jozsy jest tożsame z twierdzeniem Woottersa i Żurka.

Dyskusja: Teoria a praktyka.

- Jeśli do urządzenia wpuszczamy pojedynczą cząstkę, staje się ono bardzo mało wydajne, nie mówiąc o trudności technicznej manipulowania pojedynczą cząstką.
- W praktyce kubit tworzy często pakiet wielu cząstek. Taką paczkę można rozdzielić. Osłabiony sygnał idzie dalej przez obwód, natomiast jego odseparowana część może zostać przeczytana.
- Nie stoi to w sprzeczności z twierdzeniem Woottersa – Żurka, ponieważ żaden kubit nie jest powielany.
- Zupełnie inną techniką ataku jest splątanie swoich cząstek z cząstkami Alicji i próba wyznaczenia operacji, które Alicja na cząstkach przeprowadza. To również wykracza poza treść twierdzenia o nieklonowaniu.

Rozkład liczb na czynniki pierwsze: algorytm Shora

P.Shor, Proc.35th Annual Symposium on Foundations of Computer Science (1994).

P.Shor, SIAM J. Sci. Statist. Comput. 26 (1997) 1484.

Trudność rozkładu wielkich liczb na czynniki pierwsze leży u podstaw algorytmu szyfrującego RSA. Podanie efektywnego algorytmu zdolnego do takiego rozkładu w czasie wielomianowym powoduje konieczność opracowania nowych metod ochrony danych.

Mamy dużą n-bitową liczbę N.
Problem: rozłożyć liczbę N na czynniki pierwsze.
Klasycznie: algorytm Euklidesa jest powolny; do faktoryzacji liczb używa się obliczeń rozproszonych.
Kwantowo: istnieją algorytmy efektywne.

Cel:

- Szukamy nietrywialnych dzielników pewnej liczby (trywialny dzielnik dla N to 1 i N).
- Jeśli a jest nietrywialnym dzielnikiem N, to $\mathrm{NWD}(a, N) \neq 1$, czyli $N = ka$ dla jakiegoś $k \in \mathbb{N}$.
- Następnym etapem jest szukanie dzielnika liczby $k = N/a$ itd.
- Najtrudniejszym przypadkiem jest, gdy $N = pq$, gdzie p, q są dużymi liczbami pierwszymi.

Przykłady: Najmniejszymi liczbami pierwszymi są $p, q = 2, 3, 5, 7, \ldots$, więc liczbami, których rozkład może nas interesować, będą:

$$N = 2 \cdot 3 = 6 \quad \text{(nie jest brana pod uwagę)}$$
$$N = 3 \cdot 5 = 15$$
$$N = 3 \cdot 7 = 21 \quad \text{itd.}$$

Schemat algorytmu Shora

Algorytm składa się z części klasycznej i części kwantowej. Polega na znalezieniu nietrywialnych dzielników n-bitowej liczby N.

- (Pseudo)losowo wybieramy $a < N$ i liczymy (klasycznie) NWD, wykorzystując do tego celu np. algorytm Euklidesa:
  - jeśli $\mathrm{NWD}(a, N) \neq 1$ to znaleźliśmy nietrywialny dzielnik N,
  - jeśli $\mathrm{NWD}(a, N) = 1$ idziemy dalej.
- Liczby $a_i < N$ nie posiadające z N wspólnych dzielników tworzą grupę względem mnożenia modulo N. Każdy element tej grupy posiada rząd, będący najmniejszym r takim, że $a^r = 1(\mathrm{mod} N)$. Dla funkcji $f(x) = a^x(\mathrm{mod} N)$, r jest okresem, $f(x + r) = f(x)$.

Uzupełnienie: Grupą $G = (A, *)$ nazywamy niepusty zbiór A wraz z działaniem $*$ takim, że dla $\forall x, y, z \in A$

- działanie nie wyprowadza poza zbiór
- działanie jest **łączne**: $x * (y * z) = (x * y) * z$
- istnieje **element neutralny** 1: $x * 1 = 1 * x = x$
- istnieje **element odwrotny**: $x * x^{-1} = x^{-1} * x = 1$

Grupę nazywamy **przemienną** (abelową) jeśli działanie jest przemienne, $x * y = y * x$.

Zadanie: Podaj przykłady kilku grup przemiennych i nieprzemiennych.

- Wykorzystujemy algorytm kwantowy znajdowania okresu funkcji i wyznaczamy r. W dwóch przypadkach: gdy r jest nieparzyste lub gdy $a^{r/2} = -1(\mathrm{mod}N)$ algorytm zawodzi i należy zacząć od początku.
- Potrzeba jeszcze efektywnego algorytmu wyliczającego $f(x)$, ale jeśli przyjmiemy $x < 2^m$, to możemy zapisać

$$x = x_{m-1}2^{m-1} + x_{m-2}2^{m-2} + \cdots + x_0(\mathrm{mod}N).$$

Wtedy

$$a^x(\mathrm{mod}N) = (a^{2^{m-1}})^{x_m-1}(a^{2^{m-2}})^{x_m-2} \ldots a^{x_0}(\mathrm{mod}N),$$

zaś każde a^{2^α} jest łatwo wyliczalne przez iterowanie podnoszenia do kwadratu. Potrzeba do tego $\sim (\ln N)^3$ operacji.

- Znamy rząd r. Ponieważ r jest parzyste, mamy

$$a^r = 1(\mathrm{mod}N) \Rightarrow a^r = kN + 1 \Rightarrow kN = (a^{r/2} + 1)(a^{r/2} - 1).$$

Zauważmy, że jeśli r jest rzędem a, to $(a^{r/2} - 1)$ nie jest podzielne przez N. Stąd albo N jest dzielnikiem $a^{r/2} + 1$ (co nam nic nie daje), albo posiada nietrywialny wspólny czynnik zarówno z $(a^{r/2} + 1)$, jak i z $(a^{r/2} - 1)$, $\mathrm{NWD}(N, a^{r/2} + 1) \neq 1$. Daje nam to faktoryzację N. Jeśli N jest skonstruowane jako iloczyn dwóch liczb, to jest to jedyne rozwiązanie.
Wniosek: Algorytm działa dla r parzystych, o ile $a^{r/2} \neq -1(\mathrm{mod}N)$. Można oszacować, że mając r, prawdopodobieństwo poprawnego zakończenia algorytmu wynosi ponad 50% dla $N = pq$. Algorytm nie działa, jeśli $N = p^\alpha$, ale ten przypadek można efektywnie rozwiązać innymi metodami.

Przykład: Szukamy rozkładu $N = 15$. Losuję liczbę a, np. $a = 7$, czyli szukamy okresu funkcji $f(x) = 7^x (\mathrm{mod} 15)$.
Wyznaczamy rząd r funkcji f (tu klasycznie, ale znamy alg. kwantowy):

$$f(0) = 7^0 (\mathrm{mod} 15) = 1$$
$$f(1) = 7^1 (\mathrm{mod} 15) = 7$$
$$f(2) = 7^2 (\mathrm{mod} 15) = 4$$
$$f(3) = 7^3 (\mathrm{mod} 15) = 13$$
$$f(4) = 7^4 (\mathrm{mod} 15) = 1$$

skąd widać, że $r = 4$.
Liczymy NWD:

$$\mathrm{NWD}(N, a^{r/2} - 1) = \mathrm{NWD}(15, 7^{4/2} - 1) = \mathrm{NWD}(15, 48) = 3$$
$$\mathrm{NWD}(N, a^{r/2} + 1) = \mathrm{NWD}(15, 7^{4/2} + 1) = \mathrm{NWD}(15, 50) = 5$$

Ostatecznie otrzymujemy $15 = 3 \cdot 5$.

Wydajność algorytmów faktoryzacji

Problem faktoryzacji dużych liczb jest klasycznym przykładem problemu trudnego z punktu widzenia algorytmiki. Czas wykonania najszybszego algorytmu General Number Field Sieve (GNFS, ogólne sito ciała liczbowego) wynosi

$$\mathcal{O}\left(\exp[1,9(\ln\ N)^{1/3}(\ln\ \ln\ N)^{2/3}]\right)$$

gdzie $\ln\ N$ jest rzędu liczby bitów N.
Algorytm faktoryzacji Shora ma czas wykonania rzędu

$$\mathcal{O}\left((\ln\ N)^3\right)$$

czyli z zależności wykładniczej dostajemy zależność wielomianową od $\ln\ N$.
Najwolniejszym elementem algorytmu jest obliczenie funkcji $f(x) = a^x(\mathrm{mod}N)$.

Cechy algorytmu Shora:

- jest połączeniem kilku algorytmów, zawiera część klasyczną i część kwantową,
- należy zadbać o mechanizm „komunikacji" pomiędzy częścią kwantową a klasyczną, aby oddziaływania nie miały wpływu na tę pierwszą,
- algorytm zawiera część losową i przy niekorzystnym losowaniu należy go rozpocząć od nowa,
- algorytm nie da dobrego wyniku dla nieparzystego r oraz w przypadku $a^{r/2} = -1(\mathrm{mod}N)$; dla takich wartości należy go rozpocząć od nowa.

Przykład ten pokazuje niedeterminizm podejścia kwantowego i ograniczenia, jakie ono narzuca. Większość algorytmów klasycznych jest na tego typu warunki niewrażliwa.

Realizacja i inne algorytmy:

- Pierwsza praktyczna realizacja algorytmu Shora została dokonana w laboratorium IBM z wykorzystaniem NMR. Rozłożono 15 na $3 \cdot 5$.
  L.Vandersypen et al., Nature 414 (2001) 883 [arxiv:quant-ph/0112176].
- Kolejne dwa przypadki zrealizowano za pomocą układów optycznych, znów rozkładając liczbę 15.
  C.-Y.Lu et al., Phys. Rev. Lett. 99 (2007) 250504 [arXiv:0705.1684].
  B.P.Lanyon et al., Phys. Rev. Lett. 99 (2007) 250505 [arXiv:0705.1398].
  Zauważono, że wydajność całego zestawu jest niższa, niż wydajność idealnego obwodu kwantowego. Ważny jest rozwój technik pozwalających na doskonalszą realizację obwodów kwantowych.
- W 2012 dokonano rozkładu $21 = 3 \cdot 7$
  E.Martin-Lopez et al., Nature Photonics 6 (2012) 773 [arXiv:1111.4147].
- W latach 2012–2014, wykorzystując zamiast alg. Shora technikę AQC (*adiabatic quantum computing*) dokonano rozkładu liczby $143 = 11 \cdot 13$ oraz większych, aż do $56153 = 233 \cdot 241$.
  X.Nanyang et al., Phys. Rev. Lett. 108 (2012) 130501.
  N.S.Dattani, N.Bryans, [arXiv:1411.6758].

Uzupełnienie: Adiabatyczne obliczenia kwantowe (AQC) są równoważne tradycyjnym obwodom kwantowym. Proces adiabatyczny to taki, w którym nie ma wymiany ciepła z otoczeniem.
Schemat AQC:

- Tworzony jest hamiltonian $\mathcal{H}$, którego stan podstawowy jest rozwiązaniem szukanego problemu. Hamiltonian ten jest zazwyczaj skomplikowany.
- Budowany jest prostszy układ doświadczalny o hamiltonianie $\mathcal{H}'$. Układ ten umieszcza się w jego stanie podstawowym.
- W sposób adiabatyczny przekształca się układ prostszy tak, aby $\mathcal{H}' \to \mathcal{H}$. Na mocy twierdzenia adiabatycznego, układ po przekształceniach będzie w stanie podstawowym.
- Otrzymuje się w ten sposób szukane rozwiązanie problemu.

Praca przeglądowa o AQC:

T.Albash, D.A.Lidar, Rev. Mod. Phys. 90 (2018) 015002.

QKD czyli Quantum Key Distribution

- Największą słabością klasycznych protokołów szyfrujących jest pierwsza faza nawiązania połączenia, gdy strony muszą się wymienić kluczami.
- Kwantowe kanały komunikacji mają niewielką przepustowość i są drogie w eksploatacji.
- Podstawowym zastosowaniem sieci kwantowych jest zaufane i bezpieczne przesłanie między stronami klucza do klasycznego algorytmu szyfrującego.
- Protokoły kwantowej dystrybucji klucza nazywane są często kryptografią kwantową.

Tak więc:

- powstały teoretyczne algorytmy pozwalające na szyfrowanie transmisji,
- powstały ich implementacje i są one używane,
- algorytmy, łącza i urządzenia są powolne i mało wydajne, więc ich stosowanie do szyfrowania całego strumienia danych jest mocno nieefektywne,
- z tego powodu ograniczamy ich stosowanie do **bezpiecznego przesłania klucza** dla klasycznego algorytmu symetrycznego.

Dlatego poprawniej jest mówić o QKD, a nie o pełnej kryptografii.

Protokół BB84

C.H.Bennett, G.Brassard, Proc. IEEE Int. Conf. on Comp., Sys. and Sig. Proc. (1984) 175.

Celem jest bezpieczne przekazanie klucza od Alicji do Bolka. Nośnikiem informacji w kanale kwantowym są fotony. Alicja ma do wyboru dwie bazy polaryzowania fotonu:

Baza	0	1
prosta +		
skośna ×		

Pytanie: Bazy + i × nie są do siebie prostopadłe. Co o takiej sytuacji mówi twierdzenie o nieklonowaniu?

Pytanie: Jeśli Alicja wyśle foton zakodowany w jednej bazie, a Bolek postanowi go zmierzyć w drugiej, to jaki wynik może otrzymać?

Schemat działania protokołu:

- Alicja posiada klucz (ciąg bitów) do przesłania.
- Alicja koduje bity klucza polaryzując fotony, dla każdego bitu *losując* bazę polaryzacji.
- Alicja przesyła *kanałem kwantowym* spolaryzowane fotony do Bolka.
- Bolek mierzy polaryzację fotonów w *losowo wybranej* bazie.
- *Kanałem klasycznym* Alicja i Bolek uzgadniają, dla których fotonów ich bazy były zgodne, a dla których nie; te drugie się odrzuca.
- Na końcu może nastąpić faza korekcji błędów (nie jest częścią tego protokołu).

Algorytm przesłania klucza o długości N:

- Alicja losuje dwa ciągi bitów – a_n (klucz) i b_n (baza polaryzacji), $n \in \mathbb{N}$.
- Alicja koduje fotony zgodnie z informacjami z ciągów a_n i b_n, tworząc ciąg kubitów f_n.
- Alicja przesyła kanałem kwantowym f_n do Bolka.
- Bolek losuje ciąg b'_n, który określa, w jakich bazach będzie wykonywał pomiar polaryzacji fotonów.
- Po pomiarze Bolek otrzymuje ciąg a'_n.
- Alicja i Bolek publikują jawnie (kanałem klasycznym) swoje ciągi b_n i b'_n i odrzucają wyniki pomiarów przy niezgodnych bazach; na średnio połowa bitów zostanie odrzucona.
- Spośród zgodnych bitów część może być opublikowana w celu korekcji błędów.

W jakim celu używa się dwóch nieortogonalnych do siebie baz? Bazę prostą można zapisać jako:

$$\psi_{00} = |0\rangle,$$
$$\psi_{01} = |1\rangle.$$

Baza skośna to baza prosta obrócona o $45°$. Operatorem realizującym taki obrót jest bramka Hadamarda, więc

$$\psi_{10} = H\psi_{00} = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$\psi_{11} = H\psi_{01} = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Na przykład, jeśli wysłany został stan $|0\rangle$ i próbujemy go odczytać w bazie prostej, otrzymamy

$$\Big[|0\rangle\langle 0| + |1\rangle\langle 1|\Big]|0\rangle = |0\rangle.$$

Natomiast jeśli wysłany został stan $|0\rangle$ i próbujemy go odczytać w bazie skośnej $\{\psi_{10}, \psi_{11}\}$, otrzymamy

$$P_1 + P_2 = \Big[H|0\rangle\langle 0|H\Big]|0\rangle + \Big[H|1\rangle\langle 1|H\Big]|0\rangle.$$

Rzutowanie $|0\rangle$ na wektor bazowy ψ_{10} daje w wyniku

$$P_1 = (...) = \frac{1}{2}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\psi_{10},$$

zaś rzutowanie na ψ_{11} daje

$$P_2 = (...) = \frac{1}{2}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\psi_{11}.$$

Ostatecznie w wyniku pomiaru otrzymujemy $\frac{1}{\sqrt{2}}(\psi_{10} + \psi_{11})$, czyli losowo jeden z wektorów bazy skośnej.

Zadanie: Uzupełnij (...) w powyższych rachunkach.

Przykład: Alicja losuje ciąg bitów a_n, z którego utworzony zostanie klucz,

$$a_n = \{1, 1, 1, 0, 1, 0, 0\}.$$

Następnie losuje ciąg b_n wyznaczający bazy polaryzacji:

$$b_n = \{1, 0, 1, 1, 0, 1, 0\}.$$

Niech w ciągu b_n 0 oznacza bazę prostą (pr), a 1 bazę skośną (sk).
Bolek losuje swój własny ciąg b'_n, zgodnie z którym będzie odkodowywał otrzymane fotony,

$$b'_n = \{1, 1, 0, 0, 1, 1, 0\}.$$

Schematycznie można to zapisać w tabeli:

a_n	1	1	1	0	1	0	0
b_n	1	0	1	1	0	1	0
baza	sk	pr	sk	sk	pr	sk	pr
f_n	$\searrow\!\!\swarrow$	$\leftrightarrow$	$\searrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$	$\nearrow\!\!\swarrow$	$\updownarrow$
b'_n	1	1	0	0	1	1	0
baza	sk	sk	pr	pr	sk	sk	pr
f'_n	$\searrow\!\!\swarrow$					$\nearrow\!\!\swarrow$	$\updownarrow$
a'_n	1					0	0

Po porównaniu ciągów b_n i b'_n, co odbywa się kanałem klasycznym, część bitów zostaje uzgodniona i uznana za klucz. Niektóre bity z uzgodnionej części można ujawnić w celu dodatkowej kontroli błędów.

Uwagi:

- Trzy ciągi bitów klasycznych zostały wylosowane – algorytm wymaga użycia dobrego generatora liczb losowych (RNG).
- Jeśli szyfrowana miałaby być znana wiadomość, losowaniu podlegają tylko dwa ciągi: b_n i b'_n. W dalszym ciągu wymagany jest dobry RNG.
- Między Alicją a Bolkiem przesłano 7 fotonów; Bolek uzgodnił z Alicją 3 bity, czyli ok. 50% całkowitej liczby przesłanych cząstek.
- BB84 jest algorytmem nadmiarowym – w najprostszej sytuacji, aby uzgodnić N bitów klucza, należy przesłać $2N$ cząstek; jeśli przeprowadza się korekcję błędów, liczba przesłanych cząstek może wzrosnąć do $4N$ lub więcej.

Analizując bezpieczeństwo protokołu BB84 należy zastanowić się nad wieloma kwestiami, takimi jak:

- konstrukcją teoretyczną algorytmu,
- implementacją programistyczną,
- realizacją sprzętową.

W przypadku algorytmów kwantowych część implementacyjna może wprowadzać błędy, których model teoretyczny nie ma.

Ataki na BB84

R.Aggarwal et al., Int. J. Comp. App. 20 (2011) 28.

Ataki na algorytmy kwantowe mogą wykorzystywać:

- błędy teoretyczne w algorytmach
  - → błędy interpretacyjne
  - → błędy opisu matematycznego i fizycznego
  - → wyciek danych na pośrednich etapach algorytmu
- błędy w implementacji algorytmu
  - → błędy programistyczne
  - → konieczność użycia komputera klasycznego do opisu zjawisk kwantowych
  - → dyskretną reprezentację ciągłych parametrów fizycznych
- niedoskonałość realizacji sprzętowej
  - → wpływ środowiska
  - → opóźnienia, czas reakcji urządzeń
  - → trudność posługiwania się pojedynczą cząstką
  - → nieprecyzyjne sterowanie
  - → przeciążenie sprzętu

Atak **Intercept and Resend** (I/R). Jest to forma ataku Man-in-the-Middle.
Ewa włącza się w komunikację pomiędzy Alicję i Bolka:

- przechwytując ciąg fotonów f_n od Alicji,
- wykonując na nim pomiary w losowo wybranych bazach,
- odsyłając do Bolka powielone fotony, które zmierzyła.

Uwagi:

- Atak jest tym skuteczniejszy, im lepszy sprzęt jest użyty (wydajność detektorów, opóźnienia etc.).
- Ewa powinna wysyłać fotony do Bolka z taką samą częstotliwością, z jaką sama odbiera fotony od Alicji.
- Ingerencja Ewy zmniejsza statystyczną zgodność wyników Alicji i Bolka, więc można ją wykryć.
- W wydajniejszej wersji Ewa podsłuchuje również kanał klasyczny, zwiększając ryzyko swojego wykrycia.

Atak **Photon Number Splitting**. PNS jest możliwy, gdyż w praktyce trudno jest manipulować pojedynczymi cząstkami; używa się zamiast nich WCP (*weak coherent pulses*). Wtedy:

- paczka fotonów może zostać rozdzielona przez Ewę,
- Ewa może jedną część przechwycić...
- ...i poczekać na ogłoszenie przez Alicję i Bolka baz pomiarowych.
- Znając bazy, Ewa może wykonać pomiary na swoich fotonach bez wpływu na fotony Bolka, odtwarzając w ten sposób klucz.

Od strony technicznej atak ten jest dość trudny do przeprowadzenia, żeby nie zostać wykrytym, ale poprawnie wykonany daje możliwość poznania pełnego klucza.

Atak **Light Injection**. Atak ten skupia się na urządzeniu nadawczym Alicji.

- Ewa wysyła foton do nadajnika Alicji.
- Odbity foton wraca do Ewy niosąc informację o stanie polaryzatora Alicji.
- Ewa kontynuuje atak jako I/R, przesyłając odpowiednio spreparowany foton do Bolka.

W ten sposób Ewa wchodzi w posiadanie pełnej informacji o transmisji, praktycznie nie wprowadzając do niej większych zmian.

Atak **oślepiający detektor Bolka**. Rodzaj ataku I/R.

- Ewa przerywa transmisję pomiędzy Alicją i Bolkiem,
- odbiera sygnał od Alicji,...
- ...jednocześnie oślepiając detektor Bolka tak, że generuje w nim losowy ciąg bitów sprawiając wrażenie, że detektor odbiera sygnał od Alicji;
- Ewa poznaje klucz.

Ewa podszywa się pod Bolka, który nie ma możliwości uzgodnienia z Alicją klucza. Dopóki Alicja i Bolek nie nawiążą połączenia klasycznego, nie będą wiedzieli, że się ze sobą nie komunikują.

Sprawdza się również odporność algorytmów na ataki wykorzystujące **splątanie cząstek**. Jest to potencjalnie bardzo groźny atak, gdyż pozwala on na śledzenie stanów cząstek znajdujących się u Alicji i/lub Bolka. Trudnością jest oczywiście dokonanie odpowiedniego splątania.
BB84 jest na tego typu ataki w dużej mierze uodporniony.

- Ewa może zaatakować dokonując splątania swoich fotonów z fotonami Alicji.
- Można pokazać, że w tej sytuacji BB84 pozostaje bezpieczny (patrz notatki J.Preskilla), a atak jest możliwy do wykrycia.
- W wersji wykorzystującej pary EPR Ewa musi splątać swoje cząstki z cząstkami Alicji i cząstkami Bolka. Ten protokół również jest zabezpieczony przed takim atakiem.

Algorytm E91

A.Ekert, Phys. Rev. Lett. 67 (1991) 661.

Algorytm ten wykorzystuje splątanie cząstek tak, aby pomiar po jednej stronie pozwalał na jednoznaczne określenie stanu cząstek po drugiej stronie.

- Alicja i Bolek otrzymują po jednym fotonie z pary EPR. Pary te mogą być wytwarzane przez nich lub przez kogoś innego (Celinę).
- Cząstki w parach są tak skorelowane, że pomiar polaryzacji jednego daje jednoznacznie informację o polaryzacji drugiego.
- Alicja i Bolek losowo wybierają bazy i wykonują pomiary polaryzacji.
- Kanałem klasycznym publikują swoje wybory baz.
- W około połowie przypadków wybrali bazy tak samo – te wyniki posłużą do utworzenia klucza; pozostałe są odrzucane.

Przykład: Tworzone są pary cząstek splątanych w stanach

$$\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right).$$

Pierwsza trafia do Alicji, drugą otrzymuje Bolek; oboje robią pomiary w losowych bazach. Alicja wylosowała bazy: 1011010, Bolek wylosował bazy 1100110. Mają zgodność w pierwszym, szóstym i siódmym pomiarze,

$$(10), \ldots\text{niepoprawne}\ldots, (01), (01).$$

Umawiają się, że Bolek odwraca swoje wyniki i uzgadniają trzy bity 100. Gdyby cząstki były tworzone w stanach

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

Bolek nie musiałby zaprzeczać swoich pomiarów.

Algorytm Time-Reversed EPR

- Alicja i Bolek przygotowują ciągi kubitów, ustalając każdy z nich losowo w jednym z czterech stanów $|\uparrow_z\rangle, |\downarrow_z\rangle, |\uparrow_x\rangle, |\downarrow_x\rangle$.
- Ciągi kubitów są wysyłane do Celiny, która tworzy z nich pary EPR poprzez rzutowanie na bazę Bella.
- Celina ogłasza wyniki swojej operacji.
- W połowie przypadków, gdy Alicja i Bolek tworzyli stan wzdłuż tej samej osi, mają korelację i mogą użyć tego kubitu do dołączenia do klucza.
- Alicja i Bolek mogą też zweryfikować część swoich kubitów aby sprawdzić, czy Celina nie przeprowadziła ataku Man-in-the-Middle.
- W tym schemacie nie ma konieczności tworzenia i rozdzielania par EPR. Konieczne jest jednak dopuszczenie trzeciej strony do procesu tworzenia klucza; Celina może prowadzić centralną usługę pośredniczącą w generowaniu kluczy.

Uzupełnienie: istnieją cztery stany „maksymalnego splątania" pary cząstek, zwane stanami Bella:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Parę cząstek można wyrzutować na te stany, określone w jakiejś wybranej bazie. Wyniki będą różne dla cząstek przygotowanych w tych samych albo w różnych bazach.

Algorytm SARG04

V.Scarani et al., Phys. Rev. Lett. 92 (2004) 057901.

C.Branciard et al., Phys. Rev. A 72 (2005) 032301.

- Alicja koduje ciąg kubitów korzystając z dwóch nieortogonalnych do siebie baz ($\times$, $+$) w sposób identyczny jak w protokole BB84. Cały ciąg przesyła kanałem kwantowym do Bolka.
- Bolek dokonuje pomiarów w losowej bazie.
- Alicja ogłasza dwa stany, po jednym z każdej bazy: jeden stan który wysłała, drugi losowy z drugiej bazy.
- Jeśli Bolek dokonał pomiaru w bazie, w której kubit był zakodowany, ma zgodność z jednym ze stanów Alicji. Jeśli zmierzył w innej bazie i otrzymał stan Alicji, znowu ma zgodność. W tych przypadkach kubit jest odrzucany. Jeśli zmierzył w innej bazie i otrzymał wynik nie zgadzający się ze stanami Alicji, może wyznaczyć stan kubitu.
- Algorytm ma wydajność ok. 25%, ale jest bardziej odporny na podsłuch Ewy, gdyż bazy kodowania nie są ogłaszane publicznie.

Przykładowe wykorzystanie SARG04:

- Alicja wysyła do Bolka stan ψ_{00}.
- Alicja publicznie ogłasza, że wysłała jeden z dwóch stanów: ψ_{00} i ψ_{10}.
- Jeśli Bolek wykona pomiar otrzymanego stanu w bazie prostej (obliczeniowej), otrzyma zawsze ψ_{00}. Taki wynik należy odrzucić.
- Jeśli Bolek wykona pomiar w bazie skośnej (Hadamarda), otrzyma w połowie przypadków ψ_{10}, co również należy odrzucić. W drugiej połowie przypadków wynik pomiaru da ψ_{11}, co pozwala Bolkowi na oznaczenie ψ_{00} jako wysłanego przez Alicję stanu.

Jak widać, na średnio jeden przypadek na cztery pozwala na bezpieczne przekazanie informacji.

Testy poprawności i bezpieczeństwa polegają przede wszystkim na wprowadzeniu **nadmiarowości** do algorytmów.

- Testowanie bezpieczeństwa komunikacji w obwodach kwantowych polega przede wszystkim na sprawdzeniu statystyki. Poświęca się (ujawnia) część z przesłanej informacji i sprawdza jej zgodność po obu stronach, z uwzględnieniem możliwych błędów przesyłu. Jeśli zgodność bardzo różni się od oczekiwanej, całą komunikację należy powtórzyć.
- Aby wyeliminować błędy urządzeń stosuje się dodatkowe algorytmy korekcji niepoprawnych bitów. Polegają one w podstawowej wersji na wprowadzeniu dodatkowej nadmiarowości.
- Jak widać, aby zapewnić bezpieczeństwo komunikacji, trzeba przesłać kilkukrotnie więcej kubitów, niż wynosi długość wiadomości.

Algorytm KAK00

S.Kak, PRAMANA – J. Phys. 54 (2000) 709.

Subhash Kak zaproponował modyfikację BB84, zwiększając jego niezawodność.

- Alicja przygotowuje foton polaryzując go w osi 0° ($\updownarrow$), 45° ($\nearrow$) lub 90° ($\leftrightarrow$) i przesyła go do Bolka.
- Bolek ustawia swój polaryzator losowo w jednym z trzech ustawień po czym mierzy wynik; daje to dziewieć kombinacji.

Alicja	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\nearrow$	$\nearrow$	$\nearrow$	$\leftrightarrow$	$\leftrightarrow$	$\leftrightarrow$
Bolek	$\updownarrow$	$\nearrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow$	$\leftrightarrow$
pomiar	$\updownarrow$	$\nearrow$/nic	nic	$\updownarrow$/nic	$\nearrow$	$\leftrightarrow$/nic	nic	$\nearrow$/nic	$\leftrightarrow$

- Alicja i Bolek uzgadniają bazy, jawnie publikując, że użyli bazy prostej ($\updownarrow\leftrightarrow$) lub bazy skośnej ($\nearrow\!\!\swarrow$).
- Jeśli oboje użyli bazy prostej, to albo mają zgodność, albo Bolek niczego nie zmierzył, co pozwala na ustalenie wartości bitu w czterech przypadkach. Ewa ma 50% szansy na zgadnięcie bitu.
- Jeśli oboje użyli bazy skośnej, też mają zgodność, ale podsłuchująca Ewa jest w stanie ustalić ten bit, więc te przypadki są usuwane z klucza. Tych bitów można użyć do sprawdzenia poprawności przesyłu danych.
- Daje to skuteczność algorytmu na poziomie 4/9.

Alicja	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$	$\leftrightarrow$	$\leftrightarrow$
Bolek	$\updownarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\leftrightarrow$
pomiar	$\updownarrow$	$\nearrow\!\!\swarrow$/nic	nic	$\updownarrow$/nic	$\nearrow\!\!\swarrow$	$\leftrightarrow$/nic	nic	$\nearrow\!\!\swarrow$/nic	$\leftrightarrow$
bit klucza	0		0				1		1

Algorytm KAK06

S.Kak, Found. Phys. Lett. 19 (2006) 293.

Algorytm QKD z kilkukrotną wymianą informacji między stronami.

- Alicja i Bolek ustalają operacje unitarne U_A i U_B. Jest to wybór tajny, można go zmieniać przy każdym przesyłanym kubicie. Warunkiem jest, żeby operacje te komutowały, $U_A U_B = U_B U_A$. Dobrym przykładem są obroty wokół różnych osi.
- Alicja chce przesłać Bolkowi kubit X. Wysyła mu $U_A(X)$.
- Bolek odsyła Alicji $U_B U_A(X)$.
- Alicja odsyła Bolkowi $U_A^{-1} U_B U_A\ (X)$, ale ze względu na komutację operacji Alicji i Bolka jest to równe $U_B(X)$.
- Bolek stosuje U_B^{-1} i otrzymuje kubit X.

Nie znając operacji U_A i U_B podsłuch nie pozwala na odtworzenie kubitu X. Informacje o tych operacjach nie są przekazywane między Alicją i Bolkiem.

Metody korekcji błędów

Rzeczywiste działanie komputera kwantowego nie będzie idealne:

- dekoherencja stanów nastąpi ze względu na niedoskonałą izolację układu od otaczającego go środowiska;
- wszystkie transformacje realizowane przez bramki kwantowe będą w rzeczywistości tylko w przybliżeniu unitarne;
- powoduje to wyciek energii (informacji) z układu i konieczność wprowadzenia mechanizmów **korekcji błędów**.

Jeśli pojedyncza bramka wykonuje operację $U = U_0(1 + \mathcal{O}(\epsilon))$, gdzie odstępstwo od idealnego działania U_0 jest rzędu ϵ, to po zaaplikowaniu $\sim 1/\epsilon$ takich bramek błędy nagromadzą się.

Jednym z czynników powodujących powstanie błędów jest ciepło. Oddawanie energii do otoczenia jest procesem dysypacyjnym, nieodwracalnym. Układy klasyczne wymagają dobrych systemów chłodzących, które redukują szum elektroniki.
Układy kwantowe są bardzo wrażliwe na ciepło, dlatego większość implementacji zakłada umieszczenie procesora kwantowego wraz z pamięcią w kriostacie, w temperaturze bliskiej 0K.

Czy można stosować klasyczne metody korekcji błędów w układach kwantowych? Nie zawsze i nie wszystkie. Należy pamiętać, że:

- twierdzenie o zakazie klonowania nie pozwala na kopiowanie nieznanych kubitów bez niszczenia oryginałów,
- kubit nie jest bitem, błędy mogą zaburzać superpozycje stanów,
- błędy wpływające na względną fazę dwóch kubitów nie mają klasycznych odpowiedników,
- błędy klasyczne działają skokowo, tj. zmieniają $0 \leftrightarrow 1$; błędy kwantowe mogą mieć charakter ciągły, np. te zmieniające kąty, fazy,
- błędy mogą pojawić się z powodu splątania,
- nie można wykonywać pomiarów, bo te niszczą stany kwantowe.

Klasyczny **algorytm większościowy** (głosowania) zakłada, że prawdopodobieństwo wystąpienia kilku błędów jest znacznie mniejsze niż pojedynczego. Zamieniamy pojedynczy kubit na potrójny,

$$0 \to (000), \qquad 1 \to (111)$$

i wykonujemy korekcję wg schematu

$$(100) \to (000), \quad (010) \to (000), \quad (001) \to (000)$$

$$(011) \to (111), \quad (101) \to (111), \quad (110) \to (111).$$

Algorytm działa na zasadzie **nadmiarowości**.

W komputerze kwantowym może pojawić się kilka typów błędów.

Zmiana bitu (bit-flip)

$$|0\rangle \to |1\rangle, \qquad |1\rangle \to |0\rangle.$$

Jest to błąd klasyczny, który można poprawić znanymi metodami, np. algorytmem większościowym lub poprzez porównanie wyjść i wejść na niektórych bramkach kwantowych.
Zmiana bitu kodowanego jako polaryzacja fotonów wiązałaby się ze skręceniem płaszczyzny polaryzacji wiązki. W przypadku spinu elektronów, spin musiałby się odwrócić na przeciwny. W dobrze kontrolowanych układach takie spontaniczne operacje są mało prawdopodobne.
Zmiana bitu może zajść podczas niekontrolowanego oddziaływania układu z otoczeniem.

Zmiana fazy

W ogólności jest to transformacja typu

$$|\psi\rangle \to e^{i\alpha}|\psi\rangle.$$

Jeśli α jest nieduże, to późniejsze operacje mogą na taką zmianę fazy być niewrażliwe. Większość pomiarów również da ten sam wynik przed i po zmianie fazy.
Jednak α reprezentuje obrót stanu i jeśli ma odpowiednią wartość, może zmienić jeden stan bazowy na inny. Przykładowo, błąd typu

$$|0\rangle \to |0\rangle, \qquad |1\rangle \to -|1\rangle$$

zamieni stany bazy Hadamarda, co zniszczy późniejsze obliczenia.
Zmiana fazy nie posiada klasycznego odpowiednika, może zamienić stan na stan do niego ortogonalny.

Błąd mały jest to samoistna, powolna dekoherencja stanu kwantowego. Polega ona na niewielkiej zmianie udziału stanów bazowych w pełnym stanie układu, na przykład

$$a|0\rangle \to \sqrt{|a|^2 - |\epsilon|^2}|0\rangle + \epsilon|1\rangle.$$

Błąd taki będzie się akumulował.
Wynikają stąd ograniczenia m.in. na wielkość układu kwantowego, a w konsekwencji np. na odległość przesyłu kubitów bez konieczności stosowania wzmacniaczy.

Ponieważ:

- algorytmy korekcji błędów wymagają, aby bity najpierw odczytać
- pomiar zaburza stan kwantowy
- twierdzenie o nieklonowaniu nie pozwala na zrobienie kopii stanu

popularnym podejściem jest **kodowanie z nadmiarowością**, a potem wykonywanie pomiarów nie na wszystkich kubitach. Pozwala to na otrzymanie potrzebnych informacji bez niszczenia struktury paczki kubitów.

Przykładowy algorytm korekcji błędów wykorzystujący nadmiarowość i częściowe pomiary.

- Każdy kubit jest kodowany trzema kubitami, a więc

$$|0\rangle \to |000\rangle, \qquad |1\rangle \to |111\rangle.$$

- Z $|xyz\rangle$ mierzę dwie wielkości: $(y \oplus z, x \oplus z)$.
- Jeśli $x = y = z$, to wynik pomiaru będzie zawsze $(0, 0)$.
- Jeśli jest błąd na którymś kubicie, wynik pomiaru da co najmniej jedną 1.
- Co więcej, $(0, 1)$ wskazuje błąd na pierwszym kubicie (x), $(1, 0)$ na drugim (y), a $(1, 1)$ na trzecim (z).

Jest to prosta metoda wykrycia i naprawy błędnych kubitów, przypominająca nieco metodę sum kontrolnych Hamminga.

Ten algorytm działa też dla małych błędów ($\epsilon \ll 1$). Przyjmijmy, że mamy stan $a|0\rangle + b|1\rangle$.

$$|000\rangle \to \sqrt{1-|\epsilon|^2}|000\rangle + \epsilon|100\rangle,$$
$$|111\rangle \to \sqrt{1-|\epsilon|^2}|111\rangle - \epsilon|011\rangle.$$

- Jeśli zmierzę $(y \oplus z, x \oplus z)$, to wyrzutuję stan z błędem na stan poprawny w $(1-|\epsilon|^2) \times 100\%$ przypadków.
- W pozostałych $|\epsilon|^2 \times 100\%$ otrzymam wynik $(0,1)$ i wynikowym stanem po pomiarze będzie $a|100\rangle + b|011\rangle$, ale wynik $(0,1)$ sugeruje zamianę pierwszego kubitu, więc błąd koryguję.

Korekcja zmiany fazy (phase-flip). Błąd taki polega na zmianie czynnika fazowego przy stanie. Niektóre zmiany mogą prowadzić wręcz do odwrócenia bitu.

Aby móc korygować błędy zmiany fazy, należy na przykład zakodować znaki z nadmiarem. Każdy kubit będzie kodowany trzema trójkami kubitów, łącznie dziewięcioma kubitami, wg schematu Shora

$$|0\rangle \to 2^{-3/2}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle),$$
$$|1\rangle \to 2^{-3/2}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).$$

Nie mierząc faz w pojedynczych trójkach, co zburzyłoby ich stany, porównywać należy względne fazy par trójek, tak jak w przypadku błędu typu bit-flip.

Przykład: mamy do czynienia ze zmianą fazy na przeciwną dla kubitu $|1\rangle$:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{aligned} \sigma_z|0\rangle &= |0\rangle \\ \sigma_z|1\rangle &= -|1\rangle \end{aligned}$$

W bazie $\{|0\rangle, |1\rangle\}$ błąd ten nie jest bardzo dokuczliwy, ale w bazie Hadamarda $\{H|0\rangle, H|1\rangle\} = \{|+\rangle, |-\rangle\}$ powoduje on zmianę wektora bazowego:

$$\begin{aligned} |\pm\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \\ \sigma_z|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle, \\ \sigma_z|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle. \end{aligned}$$

Chcemy przesłać stan $\alpha|0\rangle + \beta|1\rangle$.
Zamieniamy każdy kubit na trójkę, według schematu Shora, w kilku krokach. Najpierw dokładamy $|00\rangle$ z prawej strony:

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|100\rangle.$$

Nazywamy kubity A, B i C, licząc od lewej. Używamy dwóch bramek CNOT sterowanych A: CNOT_{AB} i CNOT_{AC}:

$$\mathrm{CNOT}_{AB}\mathrm{CNOT}_{AC}[\alpha|000\rangle + \beta|100\rangle] = [\alpha|000\rangle + \beta|111\rangle].$$

Stan taki obracamy bramkami Hadamarda,

$$(H \otimes H \otimes H)[\alpha|000\rangle + \beta|111\rangle] = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle = \psi_0.$$

Pojawienie się błędu odwróci jeden z kubitów na przeciwny:

$$\alpha|++\rangle + \beta|--\rangle \to \alpha|-+\rangle + \beta|+-\rangle = \psi_A,$$
$$\alpha|++\rangle + \beta|--\rangle \to \alpha|+-\rangle + \beta|-+\rangle = \psi_B,$$
$$\alpha|++\rangle + \beta|--\rangle \to \alpha|+-\rangle + \beta|--+\rangle = \psi_C,$$

co oznacza, że odbiorca może odczytać ψ_0 lub ψ_A, lub ψ_B, lub ψ_C.
Wprowadza on operatory obrotu

$$\mathrm{NOT} = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

które w bazie obliczeniowej odwracają kubity,

$$\sigma_x|0\rangle = |1\rangle, \qquad \sigma_x|1\rangle = |0\rangle,$$

ale w bazie Hadamarda zmieniają znak jednego stanu:

$$\sigma_x|+\rangle = |+\rangle, \qquad \sigma_x|-\rangle = -|-\rangle.$$

Czyli działanie operatorów

$$x_{AB} = \sigma_x \otimes \sigma_x \otimes 1,$$
$$x_{AC} = \sigma_x \otimes 1 \otimes \sigma_x$$

na stany

$$\psi_0 = \alpha|++\rangle + \beta|--\rangle,$$
$$\psi_A = \alpha|-+\rangle + \beta|+-\rangle,$$
$$\psi_B = \alpha|+-\rangle + \beta|-+\rangle,$$
$$\psi_C = \alpha|+\rangle + \beta|-\rangle$$

wygląda tak:

$$x_{AB}\ \psi_0 = +\psi_0, \qquad x_{AC}\ \psi_0 = +\psi_0,$$
$$x_{AB}\ \psi_A = -\psi_A, \qquad x_{AC}\ \psi_A = -\psi_A,$$
$$x_{AB}\ \psi_B = -\psi_B, \qquad x_{AC}\ \psi_B = +\psi_B,$$
$$x_{AB}\ \psi_C = +\psi_C, \qquad x_{AC}\ \psi_C = -\psi_C.$$

Wynika stąd, że po obrotach x_{AB} i x_{AC} można zidentyfikować, czy i gdzie wystąpił błąd:

x_{AB}	x_{AC}	błąd
$+1$	$+1$	bez błędu
-1	-1	bit-flip A
-1	$+1$	bit-flip B
$+1$	-1	bit-flip C

Niestety, takich pomiarów nie można wykonać, bo są to operacje jednokubitowe, które zniszczą stan kwantowy!

Pomiary muszą być wykonywane **pośrednio**, poprzez operacje dwukubitowe. Bezpośredni pomiar któregokolwiek z kubitów zniszczyłby stan kwantowy i niesioną przez niego informację. Za operator pomiaru przyjmuje się więc

$$\mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (H \otimes H \otimes H).$$

Pomiar na stanie ψ_A:

$$\begin{aligned} & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (H \otimes H \otimes H)\psi_A = \\ = \ & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (\alpha|100\rangle + \beta|011\rangle) = \\ = \ & \alpha|111\rangle + \beta|011\rangle = (\alpha|1\rangle + \beta|0\rangle)|11\rangle. \end{aligned}$$

Pomiar na stanie ψ_B:

$$\begin{aligned} & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (H \otimes H \otimes H)\psi_B = \\ = \ & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (\alpha|010\rangle + \beta|101\rangle) = \\ = \ & \alpha|010\rangle + \beta|110\rangle = (\alpha|0\rangle + \beta|1\rangle)|10\rangle. \end{aligned}$$

Pomiar na stanie ψ_C:

$$\begin{aligned} & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (H \otimes H \otimes H)\psi_C = \\ = \ & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (\alpha|001\rangle + \beta|110\rangle) = \\ = \ & \alpha|001\rangle + \beta|101\rangle = (\alpha|0\rangle + \beta|1\rangle)|01\rangle. \end{aligned}$$

Jeśli wynik pomiaru dał na kubitach BC wynik $|11\rangle$ (wystąpił błąd na kubicie A, o czym dowiadujemy się bez wykonywania pomiaru na A), kubit A należy odwrócić.

W przypadku, gdy błąd nie wystąpił, do odbiorcy dociera poprawny, o czym on nie wie, stan ψ_0. Odbiorca wykonuje swoje operacje i zmienia ten stan:

$$\begin{aligned} & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (H \otimes H \otimes H)\psi_0 = \\ = \quad & \mathrm{CNOT}_{AB}\ \mathrm{CNOT}_{AC}\ (\alpha|000\rangle + \beta|111\rangle) = \\ = \quad & \alpha|000\rangle + \beta|100\rangle = (\alpha|1\rangle + \beta|0\rangle)|00\rangle. \end{aligned}$$

W tej sytuacji kubit A również trzeba odwrócić.

Ostatecznie w połowie przypadków otrzymujemy dobry stan, w połowie stan zaprzeczony. Jesteśmy w stanie wykryć i poprawić błędy.

Uwagi końcowe:

- Mogą również powstać bardziej skomplikowane błędy oraz kombinacje różnych błędów, jednak prawdopodobieństwo ich wystąpienia jest bardzo małe, co najwyżej rzędu $|\epsilon|^4$.
- Istnieją algorytmy, w których błąd nie propaguje się.
- Procedura korekcji błędów sama może być narażona na błąd.
- Istotne jest, aby poszukiwać błędów bez odczytu wiadomości.
- Zakładamy, że błędy na poszczególnych kubitach nie są ze sobą skorelowane, ale w ogólności tak być nie musi.

Podstawowe założenie algorytmów korekcji błędów

Informacja zakodowana nielokalnie jest niewrażliwa na powstawanie lokalnych błędów. Statystyczny wpływ środowiska na pojedynczy kubit, który sam z siebie nie niesie żadnej informacji, nie wpływa na informację zakodowaną w ciągu kubitów.

Symulowanie układów kwantowych

Istnieją urządzenia „działające na sposób kwantowy”, które wykonują operacje kwantowe i pozwalają na ich wykorzystanie do pewnych obliczeń. Nie są to jeszcze uniwersalne komputery kwantowe.

Komputery kwantowe są obecnie symulowane przez odpowiednie oprogramowanie w maszynach klasycznych. Symulatory te zawierają najczęściej odpowiednie języki programowania.

Język programowania QCL. Powstało kilka języków programowania, które symulują działanie komputera kwantowego. Jednym z nich jest QCL (Quantum Computation Language) autorstwa Bernharda Ömera.
Źródła wraz z dokumentacją dostępne są pod adresem:
`tph.tuwien.ac.at/~oemer/qcl.html`
Kompilacja i instalacja:

- pobrać i rozpakować źródła `qcl-0.6.7.tgz`,
- jeśli nie ma w systemie `libplotter` zakomentować odpowiednie dwie linie w `Makefile`,
- `make`
- `make install`

UWAGA: starsze źródła do poprawnej kompilacji wymagają wcześniejszej wersji kompilatora gcc. Wersja 0.6.7 (grudzień 2022) działa z nowymi dystrybucjami Linuksa.

Uruchomienie i niektóre opcje startowe

```
[marek ~]$ qcl --help
USAGE: qcl [options] [file] ...
QCL interpeter and quantum computer simulator

Startup Options:
-h, --help                  display this message
-b, --bits=n                set number of qubits (32)
-f, --dump-format=x,d,b     list vectors as HEX/DEC/BIN
```

Liczba kubitów określa pojemność rejestru, na którym można pracować. Jeśli program wymaga większego rejestru, należy uruchomić `qcl` z wyższą wartością `-bits=`.
Opcja `-dump-format` określa sposób podglądu stanu rejestru. Najczęściej interesuje nas wersja binarna **b**.

Ćwiczenie: przejrzyj pozostałe opcje `qcl`.

O czym trzeba pamiętać:

- Obiektom kwantowym nie przypisuje się wartości; opisuje się je pewnym wzorem, natomiast wartość ustalana jest podczas pomiaru.
- Podczas fizycznej realizacji algorytmu nie ma możliwości sprawdzania stanu działającej maszyny; `qcl` daje możliwość podglądu stanu komendą `dump`; nie jest ona pomiarem (`measure`) i nie zmienia stanu rejestrów.
- Pomiar redukuje funkcję falową. Wynik jest otrzymywany zgodnie z odpowiednim rozkładem prawdopodobieństwa. Po wykonaniu pomiaru algorytmu nie da się wznowić, trzeba całość przygotować i uruchomić od nowa.
- Niektóre operacje są nieodwracalne (`reset`, `measure`) i należy ich używać ostrożnie. Często zaczynają lub kończą algorytm.

Uruchomienie `qcl`:

```
[marek ~]$ qcl
```

Ustawienie szerokości rejestru na 64 kubity:

```
[marek ~]$ qcl -b 64
```

12-kubitowy rejestr, zrzut kubitów w postaci binarnej:

```
[marek ~]$ qcl -b 12 -f b
```

Wyjście z programu poprzez komendę `exit`.

Główna dokumentacja do `qcl` to:
B. Ömer, *A Procedural Formalism for Quantum Computing*
Podstawowe wyrażenia:

```
// ...                    komentarz
/* ... */                  komentarz
int real complex          typy stałych
boolean string            typy stałych
^ + - * / mod             operatory arytmetyczne
== != < <= > >=           operatory logiczne
not and or xor            operatory logiczne
&                         konkatenacja rejestrów
#                         długość wyrażenia
sin cos tan cot           funkcje trygonometryczne
sinh cosh tanh coth       funkcje hiperboliczne
exp log log(x,n) sqrt     inne funkcje
Re Im abs conj            funkcje na liczbach zespolonych
ceil floor                zaokrąglenia
max min                   dowolna liczba argumentów
gcd lcm                   dowolna liczba argumentów
random()                  liczba losowa <0,1)
```

Stałe deklarujemy poprzez `const`, np.

```
qcl> const seed=random()
```

Zmienne można definiować z lub bez ich typu, np.

```
qcl> complex z=(0,1)
qcl> y=exp(z*pi)
```

Drukowanie na wyjściu poprzez `print`, zapytanie użytkownika o wartość poprzez `input`.

Raz zadeklarowanych funkcji i operatorów nie można przedefiniować. Opcja `-allow-redefines` ukrywa komunikaty o błędach i po cichu ignoruje próby przedefiniowania elementu.

Deklaracja i odwołanie się do rejestru:

```
qureg a[n]    deklaruje n-kubitowy rejestr
quconst       deklaruje stały rejestr
quvoid        deklaruje pusty rejestr
qufunct       deklaracja funkcji
a             odwołanie do rejestru a
a[i]          odwołanie do qubitu i rejestru a
a[i:j]        odwołanie do qubitów od i do j rejestru a
a[i\j]        odwołanie do qubitu od i do i+j-1 rejestru a
a&b           konkatenacja rejestrów a i b
```

Inne polecenia:

```
dump           wypisuje stan maszyny
load save      ładuje (zapisuje) stan maszyny
reset          zeruje wszystkie kubity (*)
shell          uruchomienie podpowłoki
exit           wyjście z (pod)powłoki
list           wydrukuj wgrane definicje i rejestry
print          wydrukuj na ekranie
measure q,m    mierzy rejestr q i zapisuje wynik do m (*)
measure q      mierzy rejestr q i zapomina wynik (*)
```

(*) Uwaga: `reset` i `measure` są nieodwracalne!

Polecenie `input`:

```
input "tekst", n   wyświetl tekst i czekaj na
                   wpisanie wartości n
input 'plik.qcl'   wgranie pliku
<< plik.qcl        wgranie pliku
```

Przykład: implementacja operatora SWAP

```
extern qufunct CNot(qureg q,quconst c);

qufunct Swap(qureg a,qureg b) {
  int i;
  if #a != #b { exit "Swap: unmatching register sizes"; }
  for i=0 to #a-1 {
    CNot(a[i],b[i]);
    CNot(b[i],a[i]);
    CNot(a[i],b[i]);
  }
}
```

Jak widać, SWAP może być zrealizowany przez trzy bramki CNOT, jak podawałem wcześniej.

W qcl są trzy pętle: for, until, while, np.

```
qcl> int i
qcl> for i=10 to 2 step -2 { print i^2; }
```

Niektóre zdefiniowane operatory:

```
Matrix2x2                       deklaracja macierzy unitarnej
Matrix4x4                       deklaracja macierzy unitarnej
Matrix8x8                       deklaracja macierzy unitarnej
Rot(real theta, qureg q)        obrót pojedynczego qubitu
Mix(qureg q)                    bramka Hadamarda
CPhase(real phi, qureg q)       dopisanie exp(i phi) jeśli |q>=|1...1>
```

Niektóre zdefiniowane funkcje:

```
Perm2, Perm4 ... Perm64         permutacje
Fanout(quconst a,quvoid b)      F|i,j> = |i,i xor j>
Swap(qureg a,qureg b)           S|i,j> = |j,i>
Not(qureg a)
CNot(qureg a, quconst c)
```

Ćwiczenie: przejrzyj pliki dołączone do `qcl` i znajdź inne zdefiniowane funkcje i operatory:
default.qcl, examples.qcl, linalg.qcl, modarith.qcl, primes.qcl

Ćwiczenie: uruchom `qcl`, wgraj i uruchom algorytm Shora. Ten algorytm rozłamuje efektywnie RSA.

```
qcl> << shor.qcl
qcl> shor(15)
: chosen random x = 7
: measured zero in 1st register. trying again ...
: chosen random x = 8
: measured 64 , approximation for 0.25 is 1 / 4
: possible period is 4
: 8 ^ 2 + 1 mod 15 = 5 , 8 ^ 2 - 1 mod 15 = 3
: 15 = 5 * 3
[0/32] 1 |0>
```

Przykład: deklaracja rejestru, sprawdzenie jego stanu...

```
qcl> qureg a[1]
qcl> dump
: STATE: 1 / 32 qubits allocated, 31 / 32 qubits free
1 |0>
qcl> Not(a)
[1/32] 1 |1>
qcl> dump a
: SPECTRUM a: <0>
1 |1>
qcl> Not(a)
[1/32] 1 |0>
qcl> dump a
: SPECTRUM a: <0>
1 |0>
```

`qureg x[2]`, `dump`, `dump x`, `Not(x)`

Przykład: bramka Hadamarda, czyli obrót bazy...

```
qcl> qureg x[1]
qcl> H(x)
[1/32] 0.70711 |0> + 0.70711 |1>
qcl> H(x)
[1/32] 1 |0>
qcl> Not(x)
[1/32] 1 |1>
qcl> H(x)
[1/32] 0.70711 |0> - 0.70711 |1>
qcl> H(x)
[1/32] 1 |1>
```

`H(x)` (to samo co: `Mix(x)`)

Przykład: bramka `V(alfa,x)` dopisze fazę do `|1>`:

```
V(alfa) |1> = exp(i alfa) |1>
```

```
qcl> qureg x[1]
qcl> H(x)
[1/32] 0.70711 |0> + 0.70711 |1>
qcl> V(pi/2,x)
[1/32] 0.70711 |0> + 0.70711i |1>
```

`V(alfa,x)` (to samo co: `CPhase(alfa,x)`), `pi`, `i`

Przykład: różnica pomiędzy `dump` a `measure`. Poniższy zestaw poleceń trzeba powtórzyć 3-4 razy.

```
qcl> qureg x[1]
qcl> H(x)
[1/32] 0.70711 |0> + 0.70711 |1>
qcl> measure x
[1/32] 1 |1>
qcl> measure x
[1/32] 1 |1>
qcl> measure x
[1/32] 1 |1>
```

```
measure x
```

Ćwiczenie: sprawdź działanie symulatora BB84 dostępnego pod adresem `fredhenle.net/bb84/demo.php`

Ćwiczenie: sprawdź działanie symulatora BB84 autorstwa Roberta Dźwierzyńskiego, dostępnego pod adresem `kft.umcs.lublin.pl/mgozdz`
Przeanalizuj kod a potem go uruchom.

Ćwiczenie: w kodzie `bb84.qcl` znajdź te fragmenty, które są bezpośrednio związane z algorytmem. Na ich podstawie napisz swój własny kod realizujący schemat BB84.

Teleportacja człowieka?

Możliwości techniczne do przeprowadzenia teleportacji człowieka oszacowali studenci 4. roku fizyki Uniwersytetu Leicester w 2013 r. Publikacja w wiadomościach uczelnianych w tym momencie nie jest już dostępna.

- aby oszacować informację zawartą w człowieku postanowiono zliczyć pary DNA wchodzące w skład każdej komórki
- dało to około 10 Gb informacji zawartej w każdej komórce
- założono, że każda komórka zawiera całą informację konieczną do odtworzenia komórki dowolnego typu w organizmie
- w ten sposób typowy ludzki mózg zawiera $2,6 \cdot 10^{42}$ b
- zakładając przesył na poziomie 30 GHz, czas transferu wyniósłby $4,85 \cdot 10^{15}$ lat, czyli 350 tyś. razy wiek Wszechświata

P. Zhang et al., Phys. Rev. Lett. 112 (2014) 130501.

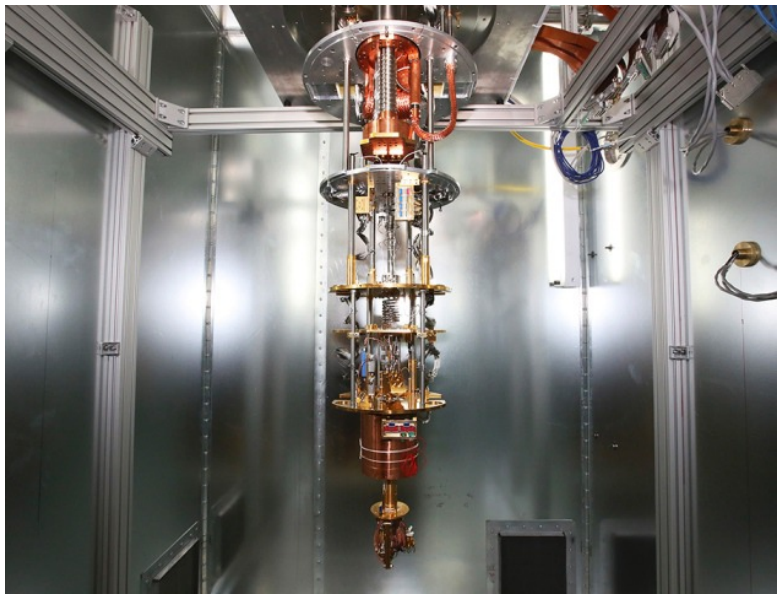
Grupa z Univ. Bristol we współpracy z Nokią

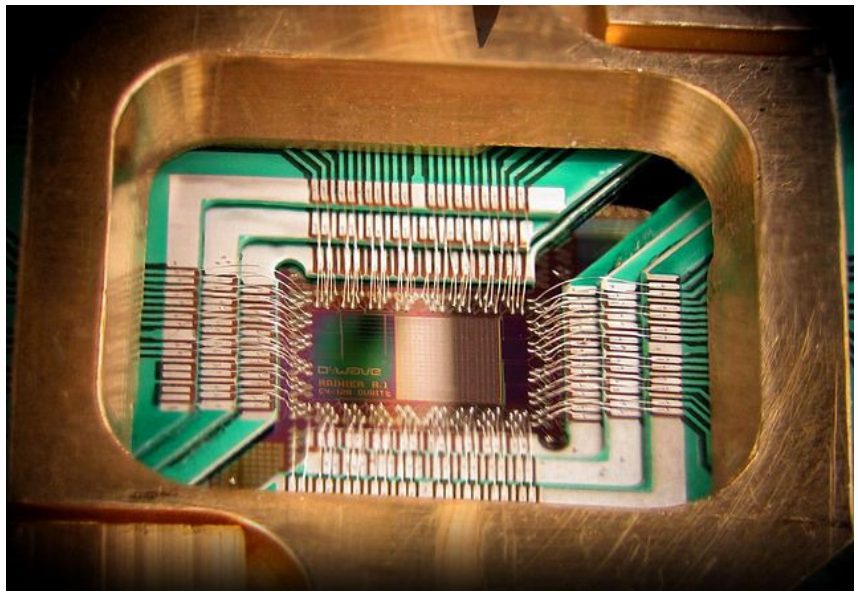
- zbudowała mikrochip do realizacji QKD
- można go wbudować w urządzenia przenośne
- nośnikiem są fotony
- możliwość uwierzytelniania transkacji (płacenie telefonem, korzystanie z bankomatu)
- w planach możliwość szyfrowania połączeń, korzystania z internetu („NSA-proof phone”)

www.dwavesys.com

D-Wave 2000Q:

- kriostat -273C = 0.015K
- procesor w postaci siatki 2000 kubitów realizujący algorytm minimalizacji dwuwymiarowego pola
- pobiera (tylko) 25kW mocy – 100 razy mniej niż tradycyjny superkomputer





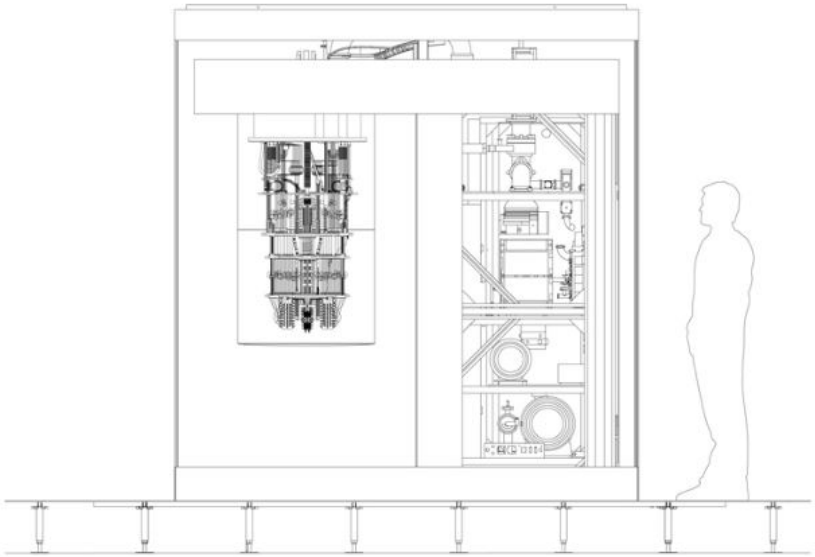
www.ibm.com/quantum

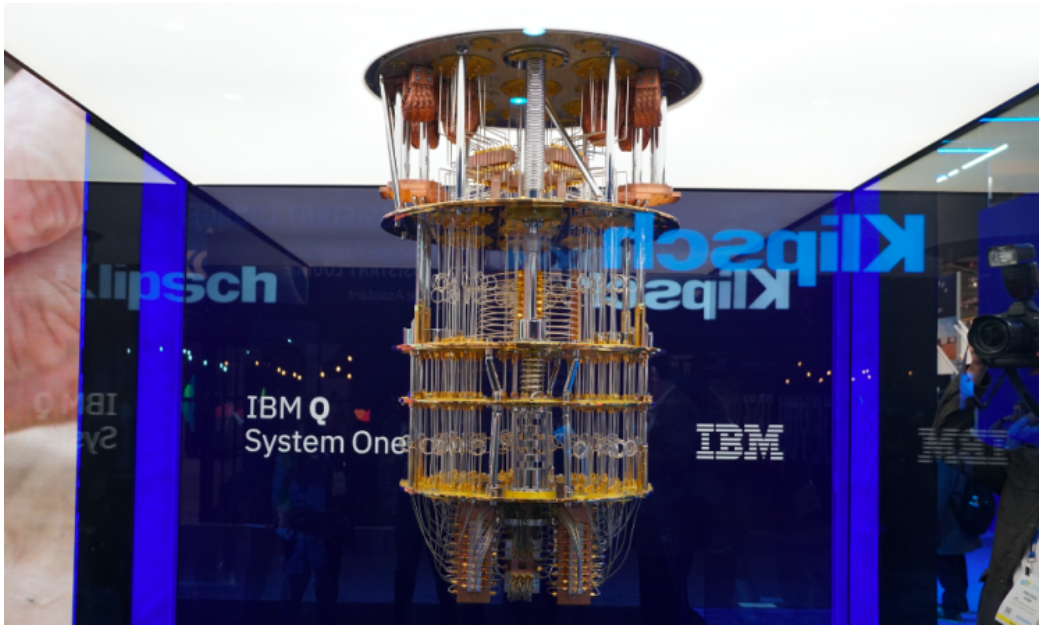
IBM Quantum (wcześniej Q System One):

...world's first integrated quantum computing system for commercial use...

...universal approximate superconducting quantum computer...

- komputery mają ustaloną liczbę kubitów
  - zaczynając od 5, potem 12 i 20 (Tokyo)
  - Falcon 27 kubitów (2019)
  - Hummingbird 65 kubitów (2020)
  - Eagle 127 kubitów (2021)
  - Osprey 433 kubity (2022)
  - w planach: Condor 1121, Flamingo 1386+, Kookaburra 4158+...
- posiadają autokalibrację
- procesory umieszczone w kriostacie
- dostęp on-line poprzez IBM Quantum oraz oparty na Pythonie język do pisania algorytmów QISKit (open-source)




IBM Q
System One
IBM

Podsumowanie

- Komputer kwantowy w niektórych sytuacjach jest wydajniejszy od maszyn klasycznych, w innych jego użycie może być zupełnie nieopłacalne.
- Zrównoleglenie kwantowe pozwala na obróbkę wielu danych wejściowych jednocześnie.
- Zawsze gdzieś w algorytmie pojawi się pomiar, który wyrzutuje superpozycję stanów na jeden konkretny.
- Algorytmy kwantowe często są statystyczne, wymagają połączenia z algorytmem klasycznym, wymagają powtórzenia algorytmu.
- Układy kwantowe zapewniają zwiększone bezpieczeństwo danych (twierdzenie o nieklonowaniu).
- Teoria wyprzedza technologię: trudności techniczne w stworzeniu odpowiednich maszyn.