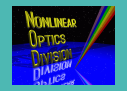
Zakład Optyki Nieliniowej

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



Informatyka kwantowa

wykład z cyklu

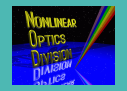
Zaproszenie do fizyki

Ryszard Tanaś

Umultowska 85, 61-614 Poznań

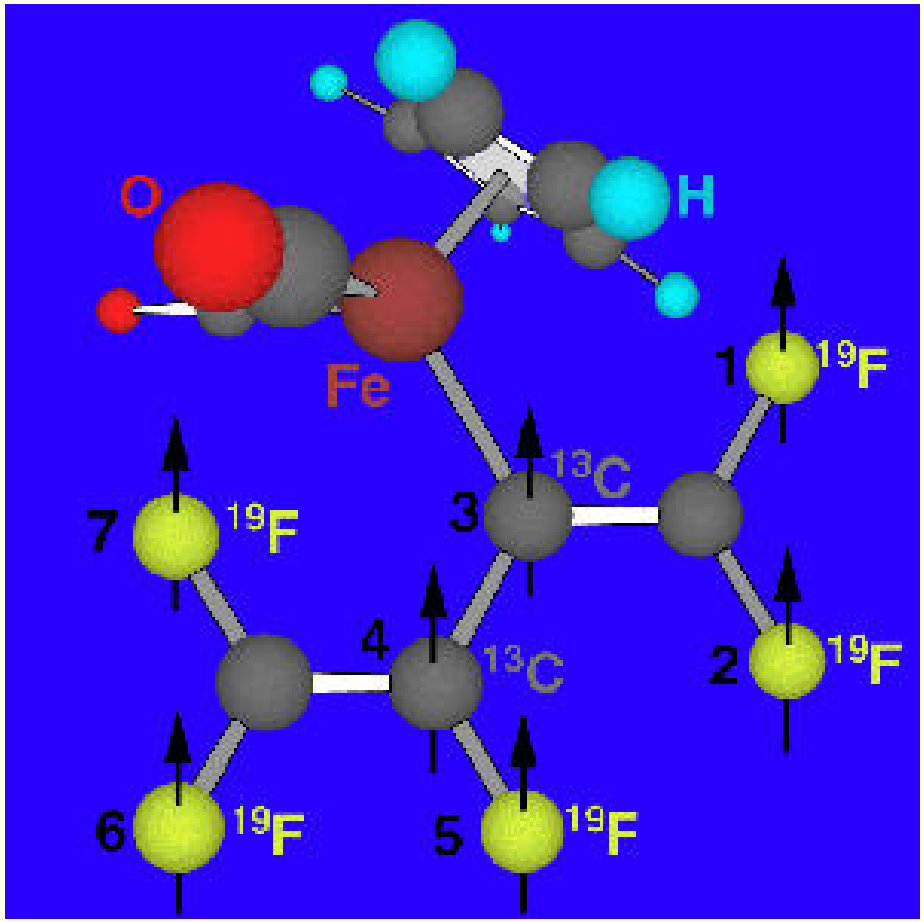
mailto:tanas@kielich.amu.edu.pl

Spis treści



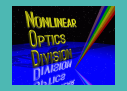
Komputer kwantowy liczy już do 15!

Rysunek 1: Wiedza i Życie, maj 2002



Rysunek 2: Isaac L. Chuang i jego procesor kwantowy

Informacja klasyczna — bit



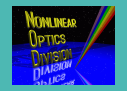
Definicja

Niech A będzie zdarzeniem losowym, które występuje z prawdopodobieństwem $P(A)$. Jeśli dowiadujemy się, że takie zdarzenie nastąpiło, to uzyskujemy

$$I(A) \quad = \quad \log \frac{1}{P(A)}$$

jednostek informacji. Jeśli logarytm jest przy podstawie 2, to jednostka informacji nazywa się bit. Zauważmy, że dla $P(A) = \frac{1}{2}$, $I(A) = 1$.

Informacja klasyczna — bit



Definicja

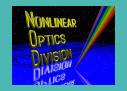
Niech A będzie zdarzeniem losowym, które występuje z prawdopodobieństwem $P(A)$. Jeśli dowiadujemy się, że takie zdarzenie nastąpiło, to uzyskujemy

$$I(A) \quad = \quad \log \frac{1}{P(A)}$$

jednostek informacji. Jeśli logarytm jest przy podstawie 2, to jednostka informacji nazywa się bit. Zauważmy, że dla $P(A) = \frac{1}{2}$, $I(A) = 1$.

Jeden bit to ilość informacji jaką uzyskujemy kiedy zachodzi jedna z dwóch alternatywnych możliwości,
np. kiedy poznajemy wynik rzutu monetą.

Informacja klasyczna — bit



Definicja

Niech A będzie zdarzeniem losowym, które występuje z prawdopodobieństwem $P(A)$. Jeśli dowiadujemy się, że takie zdarzenie nastąpiło, to uzyskujemy

$$I(A) \quad = \quad \log \frac{1}{P(A)}$$

jednostek informacji. Jeśli logarytm jest przy podstawie 2, to jednostka informacji nazywa się bit. Zauważmy, że dla $P(A) = \frac{1}{2}$, $I(A) = 1$.

Jeden bit to ilość informacji jaką uzyskujemy kiedy zachodzi jedna z dwóch alternatywnych możliwości,
np. kiedy poznajemy wynik rzutu monetą.

Przy rzucie kostką do gry $P(A) = \frac{1}{6}$ i poznanie wyniku daje
$I(A) = \log_2 6 \approx 2.58$ bitów.

Niech $\{A_1, A_2, \ldots, A_n\}$ będą zdarzeniami niezależnymi występującymi z prawdopodobieństwami $\{P(A_1), P(A_2), \ldots, P(A_n)\}$, wtedy

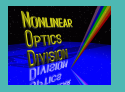





Niech $\{A_1, A_2, \ldots, A_n\}$ będą zdarzeniami niezależnymi występującymi z prawdopodobieństwami $\{P(A_1), P(A_2), \ldots, P(A_n)\}$, wtedy

$$H = \sum_i P(A_i) \log \frac{1}{P(A_i)} = -\sum_i P(A_i) \log P(A_i)$$

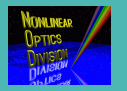
określa średnią informację (entropię) takiego źródła informacji.








Niech $\{A_1, A_2, \ldots, A_n\}$ będą zdarzeniami niezależnymi występującymi z prawdopodobieństwami $\{P(A_1), P(A_2), \ldots, P(A_n)\}$, wtedy



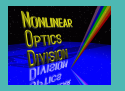
$$H = \sum_i P(A_i) \log \frac{1}{P(A_i)} = -\sum_i P(A_i) \log P(A_i)$$

określa średnią informację (entropię) takiego źródła informacji.

Weźmy np.

Zdarzenie	A_1	A_2	A_3
Prawdopodobieństwo	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$

Niech $\{A_1, A_2, \ldots, A_n\}$ będą zdarzeniami niezależnymi występującymi z prawdopodobieństwami $\{P(A_1), P(A_2), \ldots, P(A_n)\}$, wtedy



$$H = \sum_i P(A_i) \log \frac{1}{P(A_i)} = -\sum_i P(A_i) \log P(A_i)$$

określa średnią informację (entropię) takiego źródła informacji.

Weźmy np.

Zdarzenie	A_1	A_2	A_3
Prawdopodobieństwo	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$

wtedy

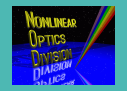
$$H = -\frac{1}{2} \log \frac{1}{2} - \frac{1}{3} \log \frac{1}{3} - \frac{1}{6} \log \frac{1}{6} \approx 1.46$$

Informacja jest wielkością fizyczną

Zasada Landauera

Wymazanie jednego bitu informacji w otoczeniu o temperaturze T wymaga straty energii (wydzielenia ciepła) o wartości co najmniej $kT \ln 2$

Informacja jest wielkością fizyczną



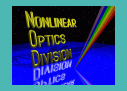
Zasada Landauera

Wymazanie jednego bitu informacji w otoczeniu o temperaturze T wymaga straty energii (wydzielenia ciepła) o wartości co najmniej $kT \ln 2$

Komputer jest układem fizycznym

Jeden bit informacji jest reprezentowany, w układach fizycznych z których zbudowane są obecne komputery, przez około 10^{10} atomów!

Informacja jest wielkością fizyczną



Zasada Landauera

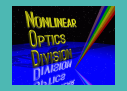
Wymazanie jednego bitu informacji w otoczeniu o temperaturze T wymaga straty energii (wydzielenia ciepła) o wartości co najmniej $kT \ln 2$

Komputer jest układem fizycznym

Jeden bit informacji jest reprezentowany, w układach fizycznych z których zbudowane są obecne komputery, przez około 10^{10} atomów!

Jeśli obecny trend w miniaturyzacji układów scalonych się utrzyma, to około roku 2020 jeden bit będzie reprezentowany przez jeden atom!

Informacja jest wielkością fizyczną



Zasada Landauera

Wymazanie jednego bitu informacji w otoczeniu o temperaturze T wymaga straty energii (wydzielenia ciepła) o wartości co najmniej $kT \ln 2$

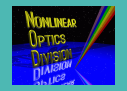
Komputer jest układem fizycznym

Jeden bit informacji jest reprezentowany, w układach fizycznych z których zbudowane są obecne komputery, przez około 10^{10} atomów!

Jeśli obecny trend w miniaturyzacji układów scalonych się utrzyma, to około roku 2020 jeden bit będzie reprezentowany przez jeden atom!

Fizyka w skali pojedynczego atomu to fizyka kwantowa — rządzą tu prawa mechaniki kwantowej.

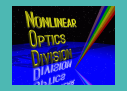
Informacja kwantowa — qubit (kubit)



Definicja

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy: dwa poziomy atomu, spin połówkowy, foton o dwóch wzajemnie ortogonalnych stanach polaryzacji, itp.

Informacja kwantowa — qubit (kubit)

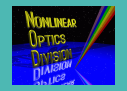


Definicja

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy: dwa poziomy atomu, spin połówkowy, foton o dwóch wzajemnie ortogonalnych stanach polaryzacji, itp.

Taki układ to qubit (quantum bit); po polsku kubit.

Informacja kwantowa — qubit (kubit)



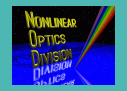
Definicja

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy: dwa poziomy atomu, spin połówkowy, foton o dwóch wzajemnie ortogonalnych stanach polaryzacji, itp.

Taki układ to qubit (quantum bit); po polsku kubit.

Klasyczny bit może przyjmować tylko dwie wartości $\{0, 1\}$; układ znajduje się albo w stanie 0 albo w stanie 1.

Informacja kwantowa — qubit (kubit)



Definicja

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy: dwa poziomy atomu, spin połówkowy, foton o dwóch wzajemnie ortogonalnych stanach polaryzacji, itp.

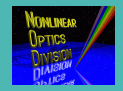
Taki układ to qubit (quantum bit); po polsku kubit.

Klasyczny bit może przyjmować tylko dwie wartości $\{0, 1\}$; układ znajduje się albo w stanie 0 albo w stanie 1.

Kubit (qubit) to dowolny stan kwantowy układu dwupoziomowego o stanach własnych $|0\rangle$ i $|1\rangle$, który może być superpozycją stanów własnych

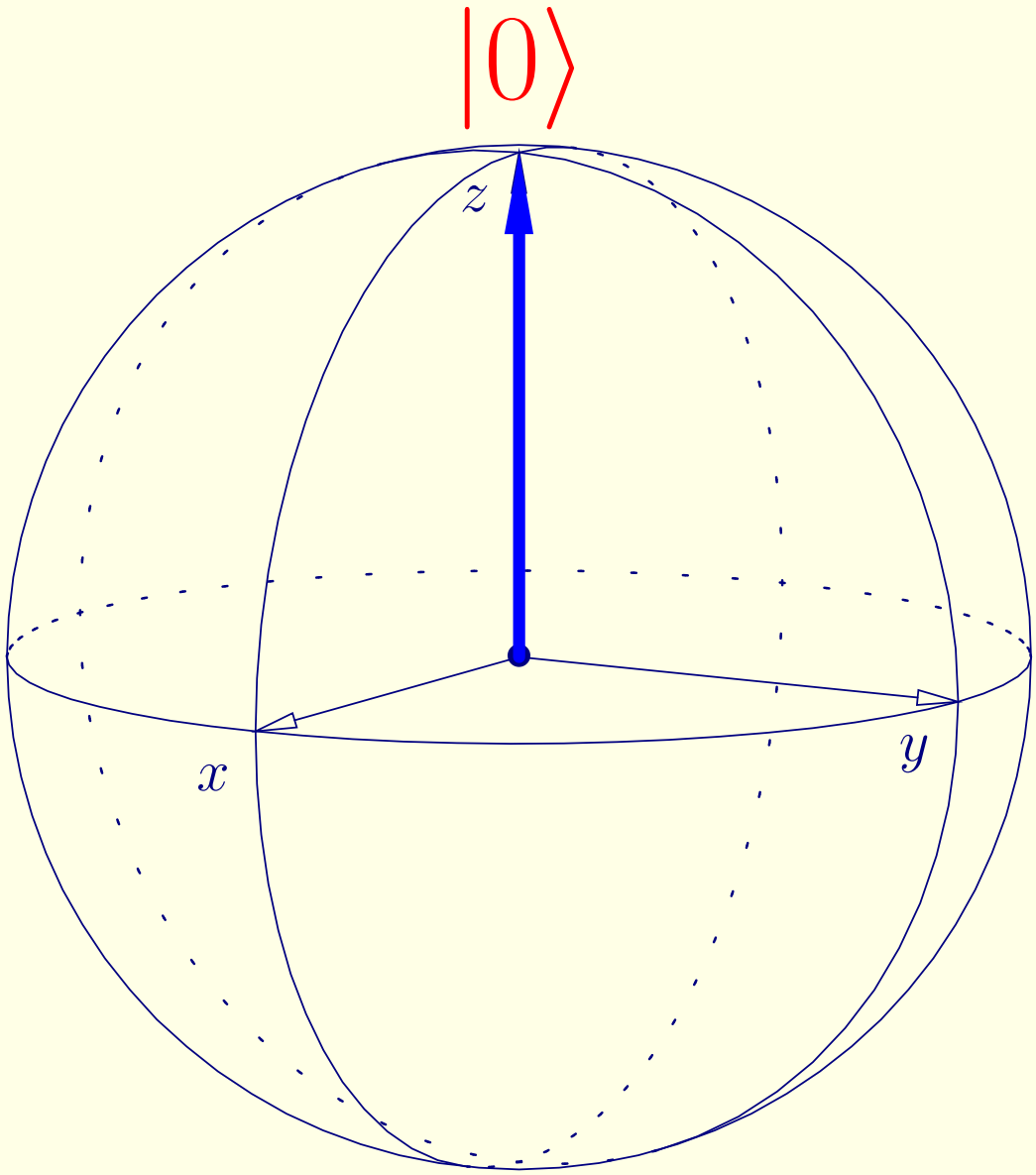
$$\begin{aligned} |\Psi\rangle &= a|0\rangle + b|1\rangle \\ & \\ & |a|^2 + |b|^2 = 1 \end{aligned}$$

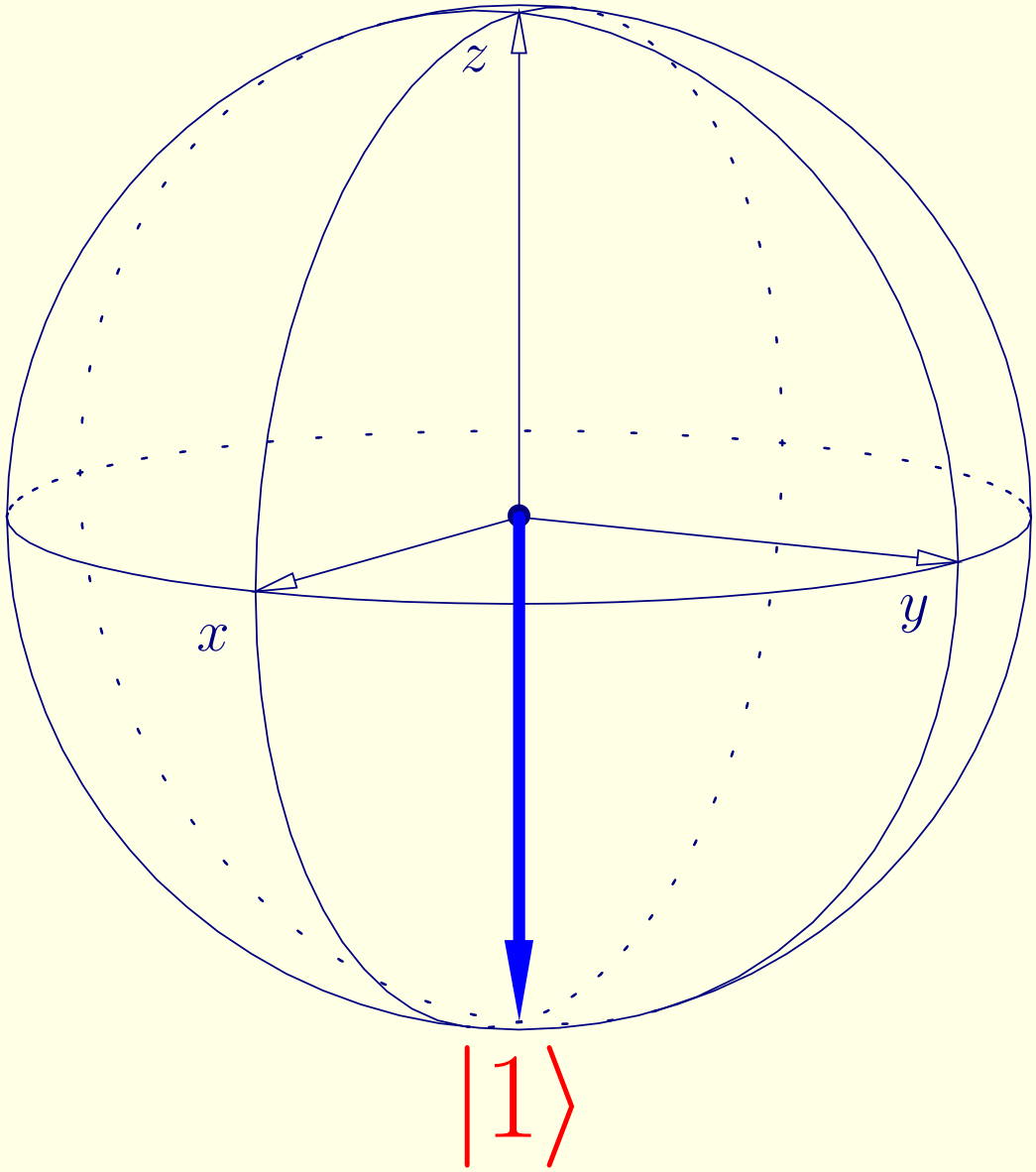
Kubit (spin) na sferze Blocha

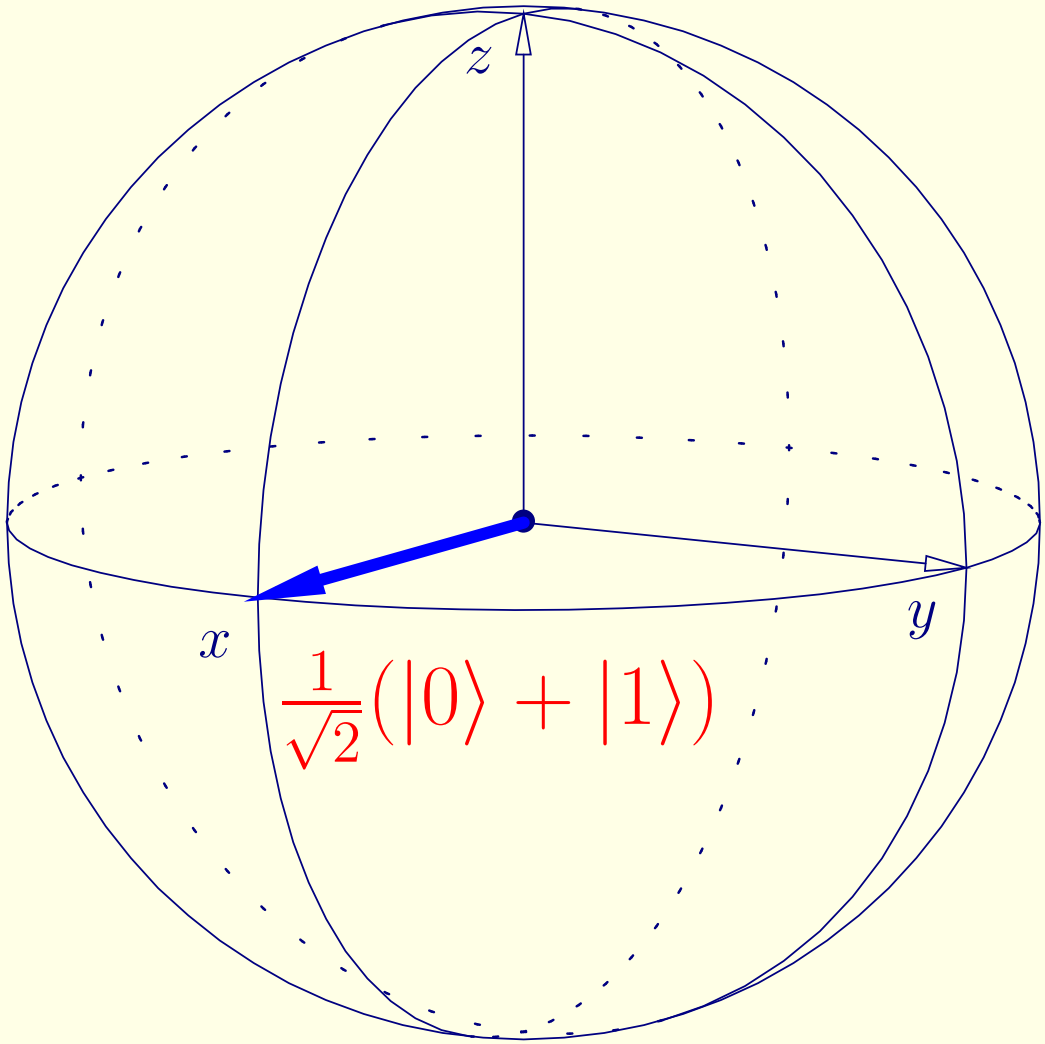


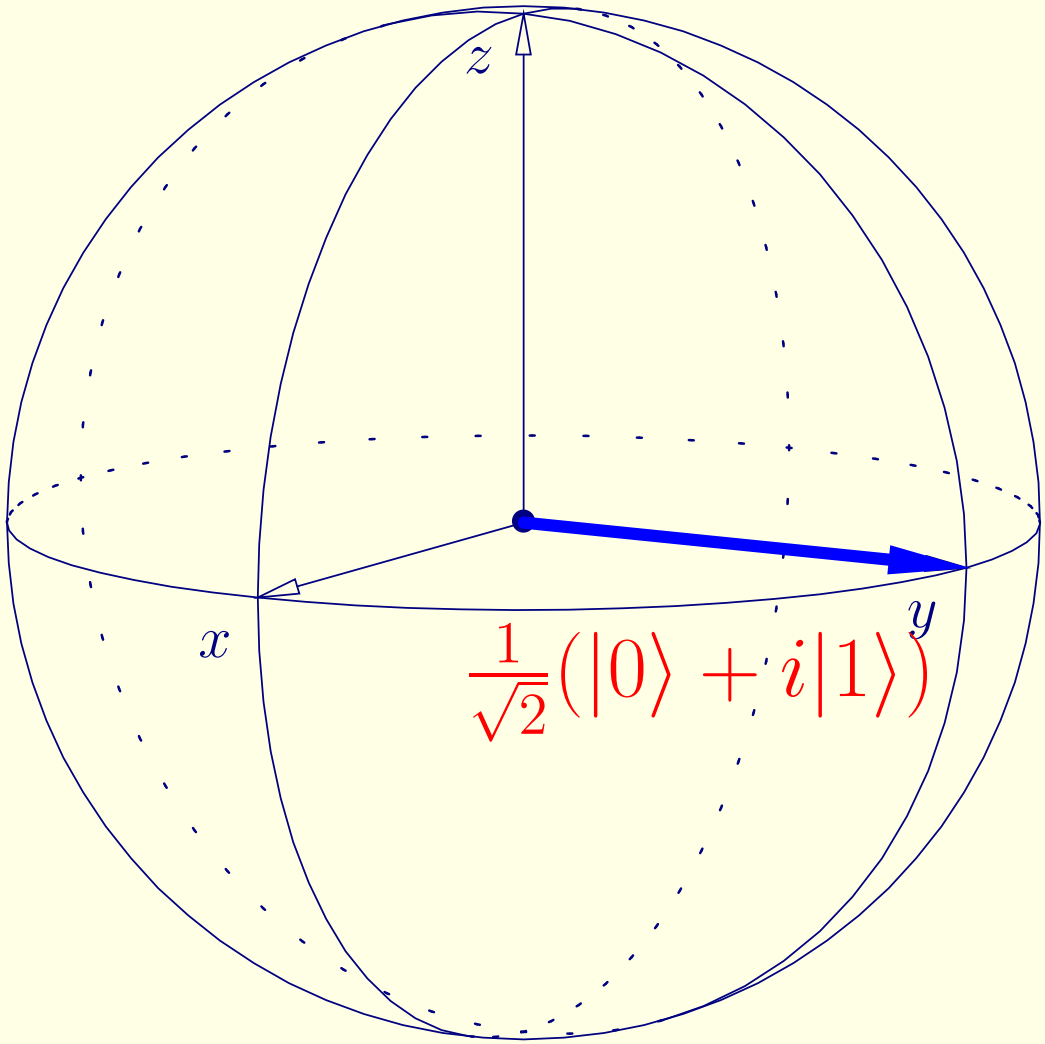


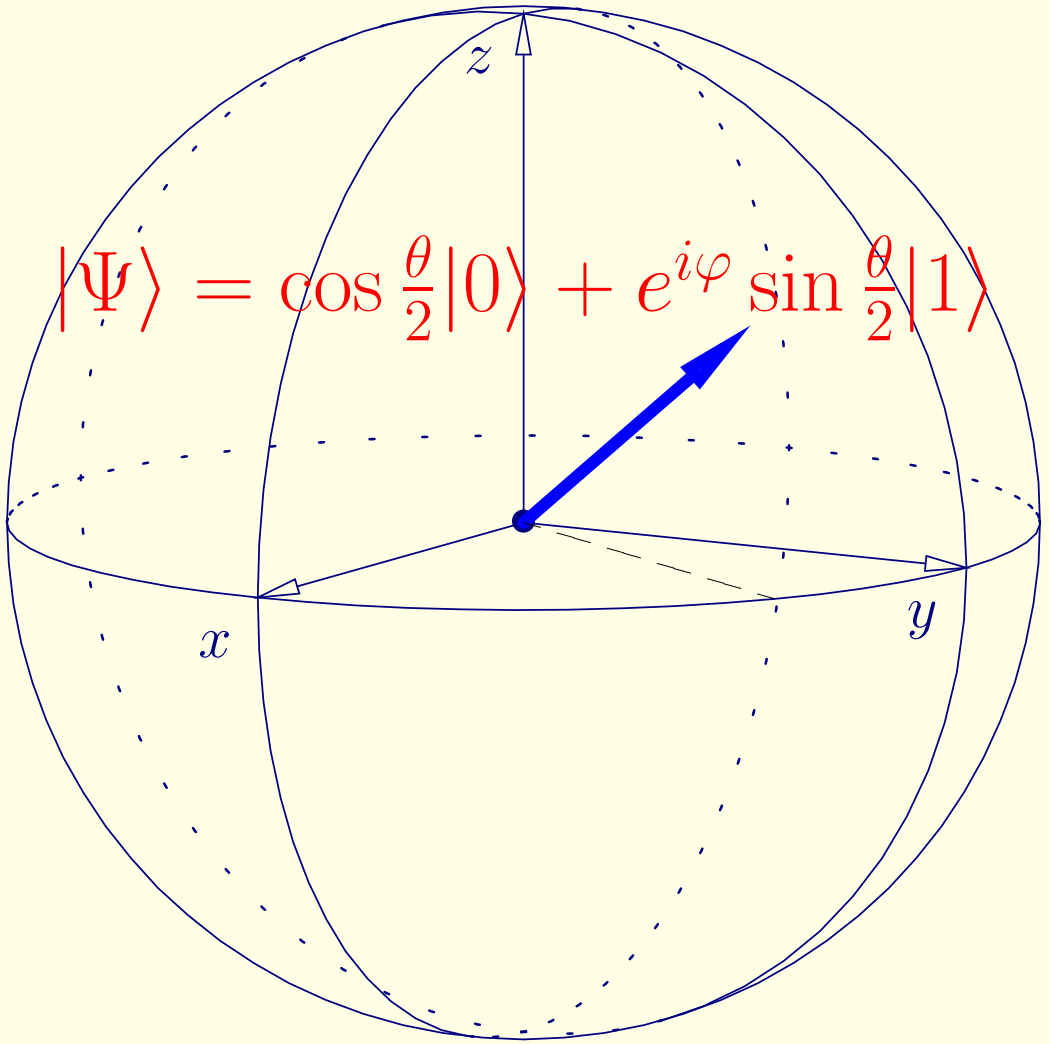




$|0\rangle$
z
x
y


z
x
y
|1⟩


z
x
y
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$


z
x
y
$\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$


$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$
z
x
y

Bramki kwantowe

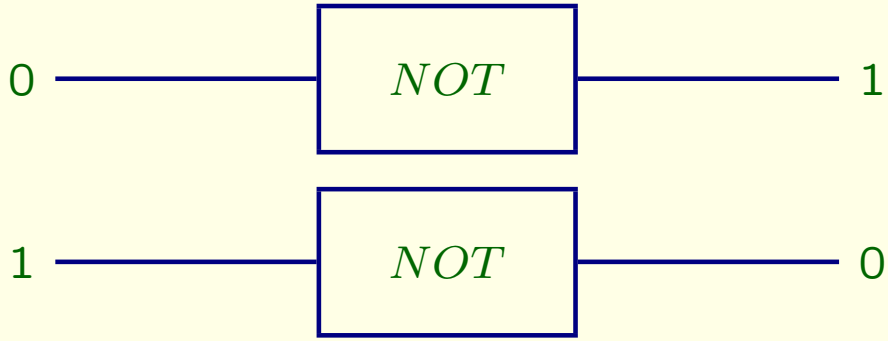
Klasyczne bramki logiczne

jednobitowe

Bramki kwantowe

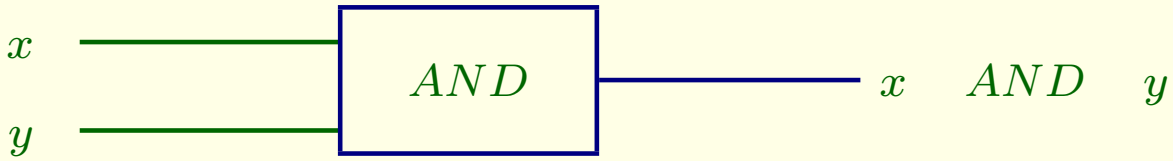
Klasyczne bramki logiczne

jednobitowe

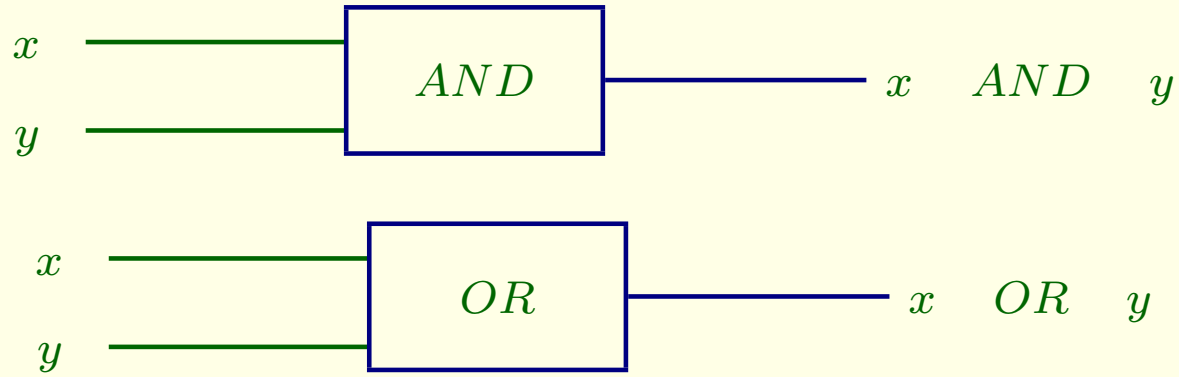


Bramki jednobitowe są odwracalne

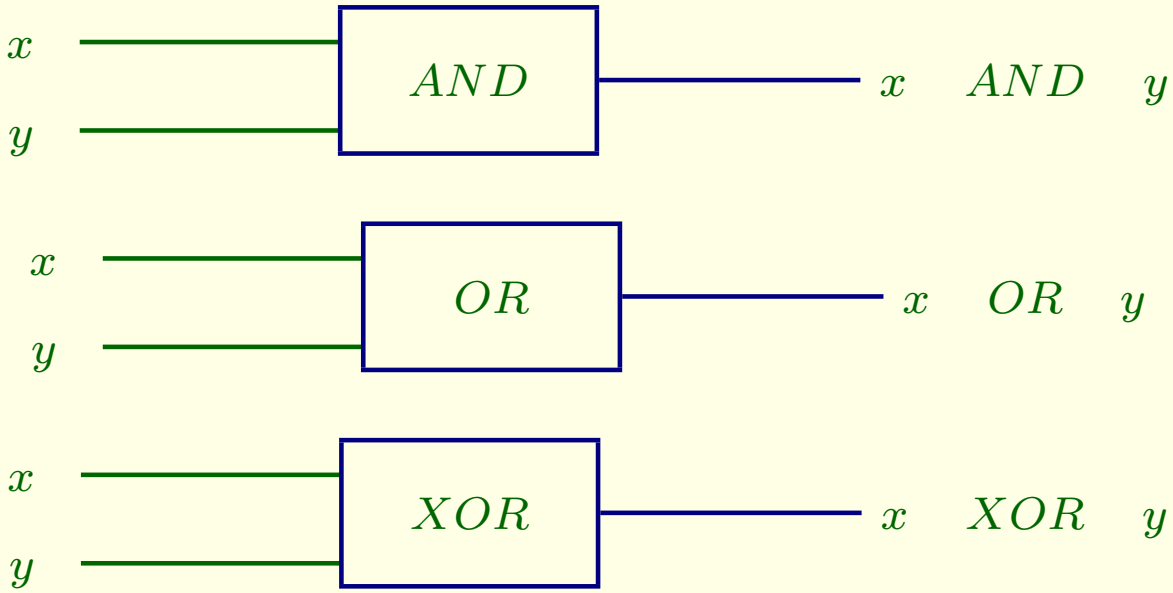
dwubitowe



dwubitowe

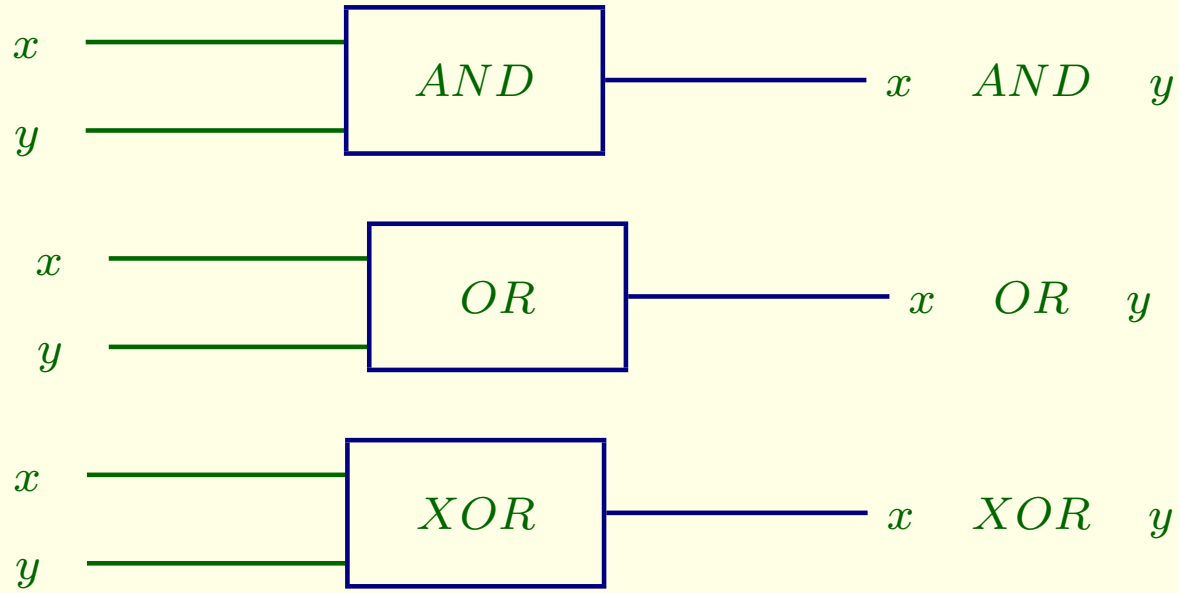


dwubitowe



Powyższe bramki dwubitowe są nieodwracalne

dwubitowe



Powyższe bramki dwubitowe są nieodwracalne

Bramka kontrolowane NOT

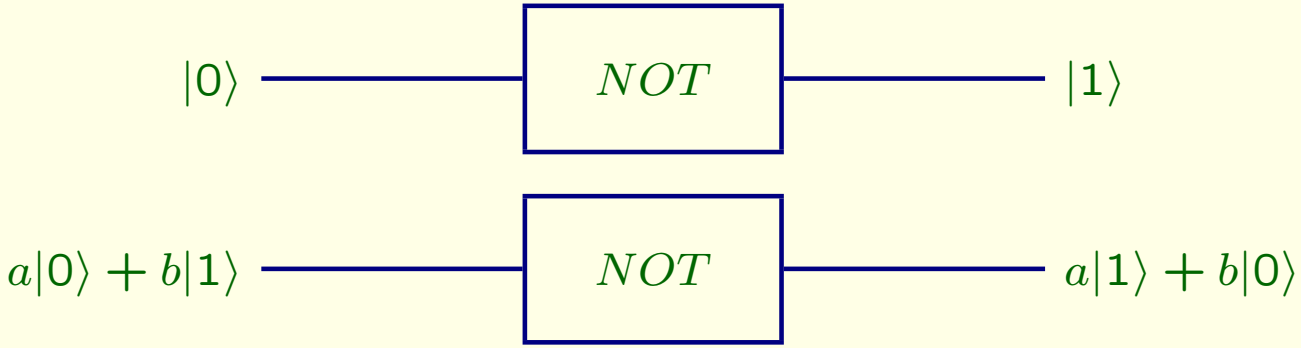
Ta bramka jest odwracalna!

Bramki kwantowe

jednobitowe

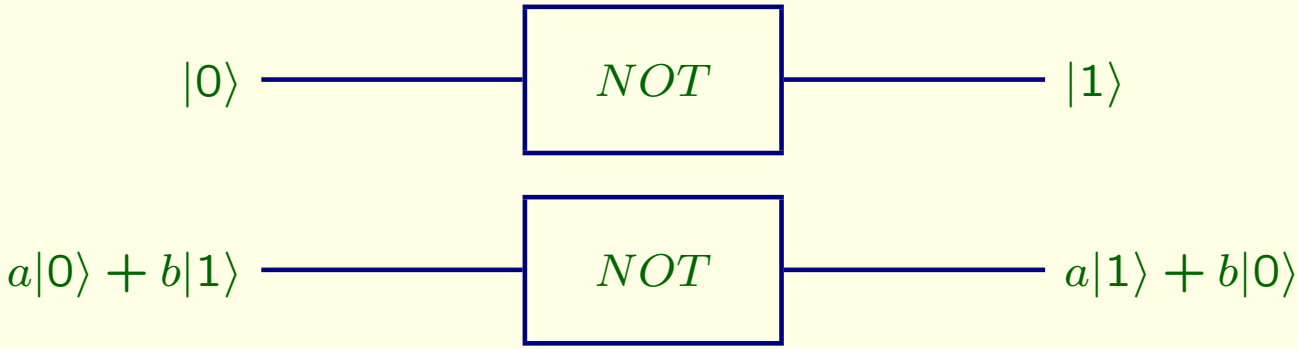
Bramki kwantowe

jednobitowe

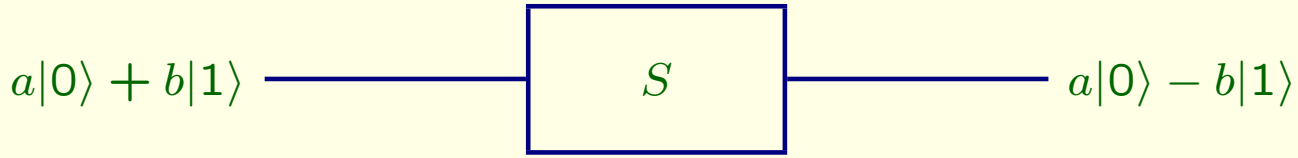


Bramki kwantowe

jednobitowe

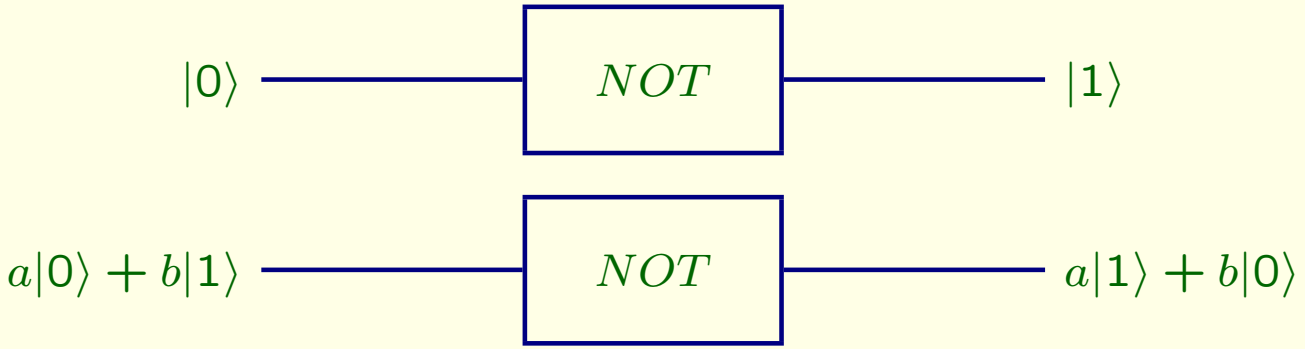


Zmiana fazy

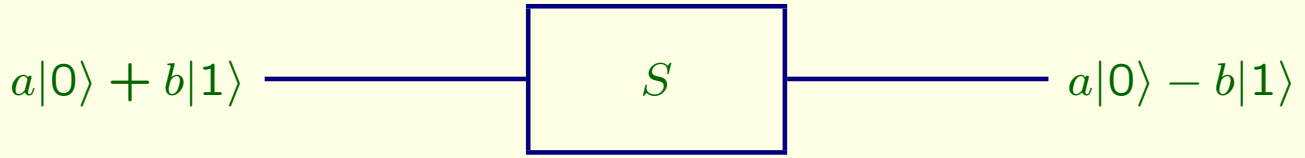


Bramki kwantowe

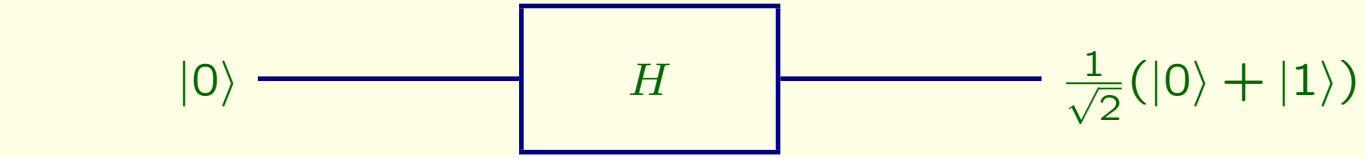
jednobitowe



Zmiana fazy

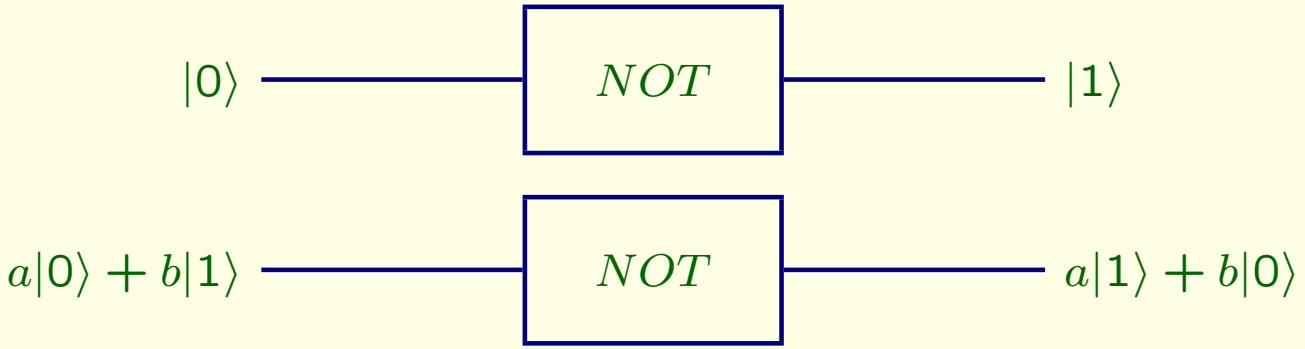


Bramka Hadamarda

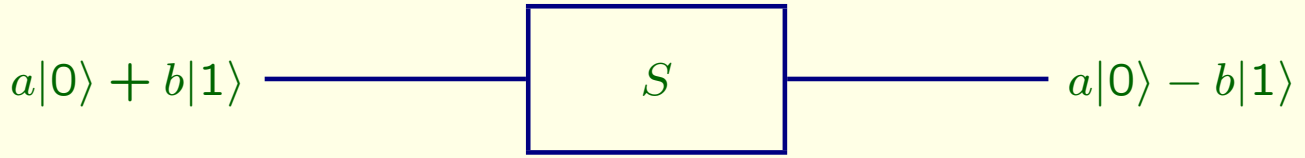


Bramki kwantowe

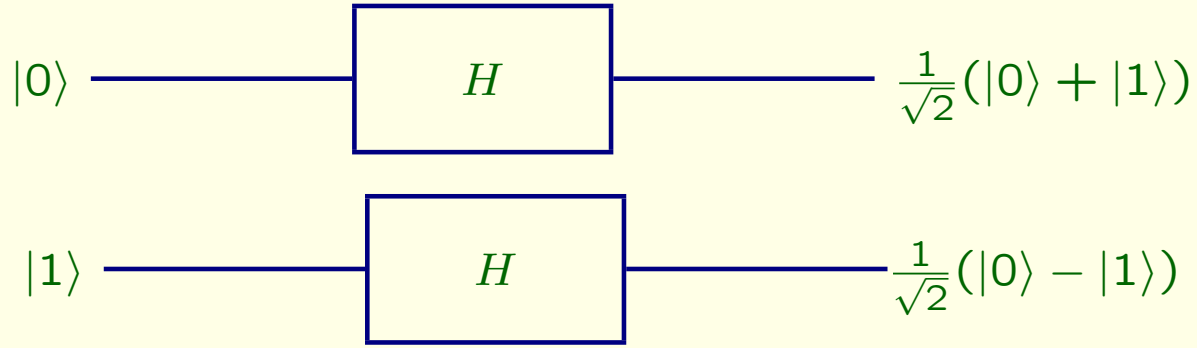
jednobitowe



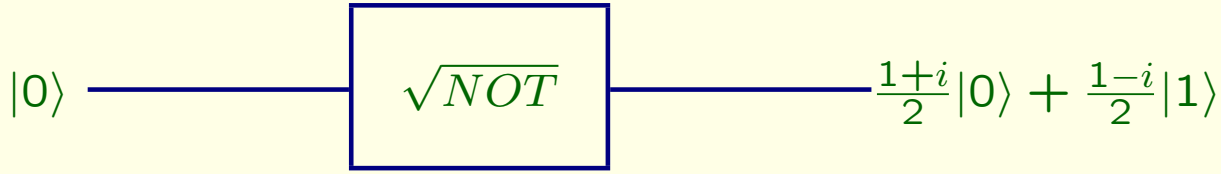
Zmiana fazy



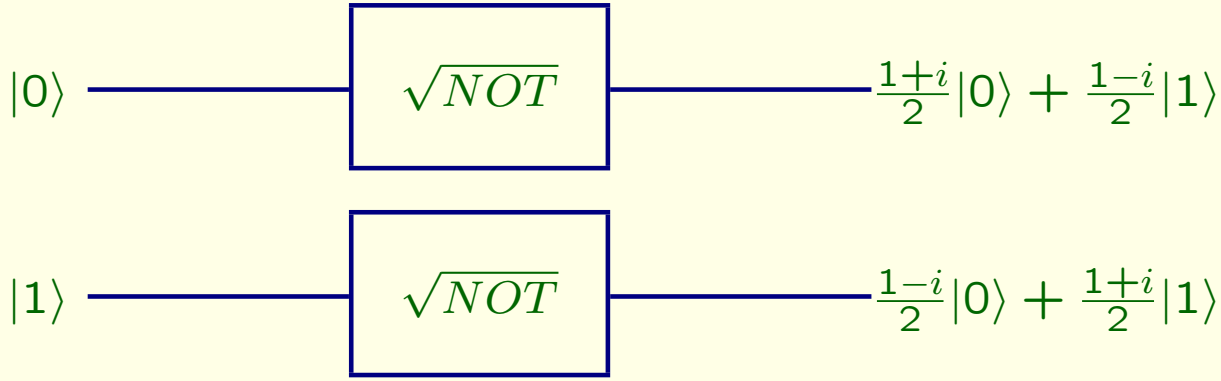
Bramka Hadamarda



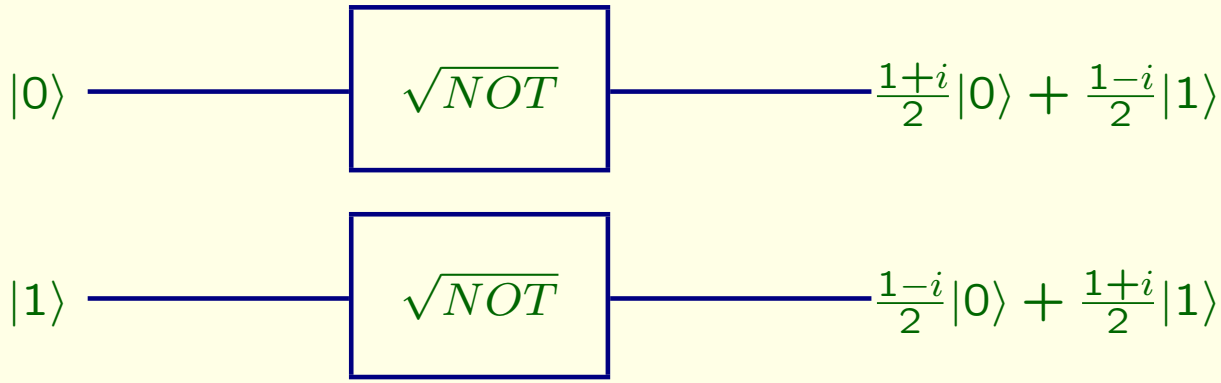
Pierwiastek z NOT



Pierwiastek z NOT



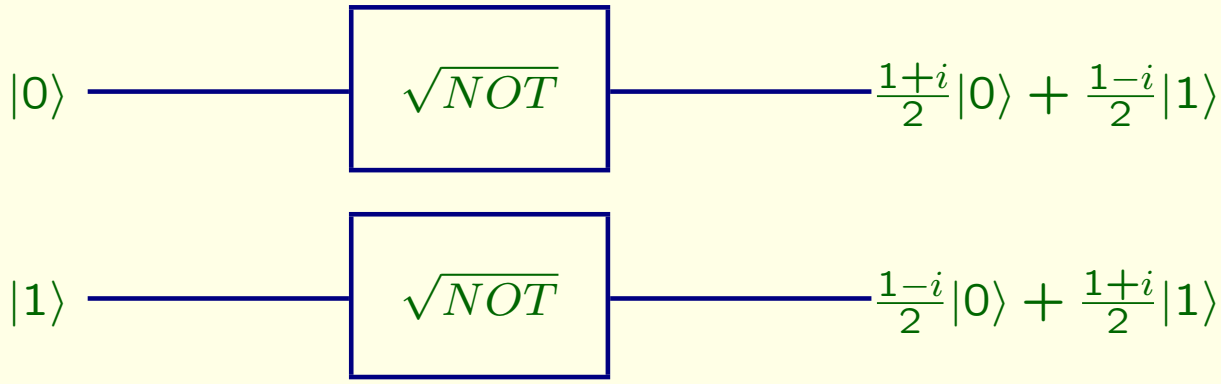
Pierwiastek z NOT



$$(\sqrt{NOT})^2 = NOT$$

W informatyce kwantowej liczba nietrywialnych bramek logicznych jest znacznie większa!

Pierwiastek z NOT



$$(\sqrt{NOT})^2 = NOT$$

W informatyce kwantowej liczba nietrywialnych bramek logicznych jest znacznie większa!

Interferencja kwantowa pozwala uzyskać operacje logiczne niedostępne w klasycznej informatyce

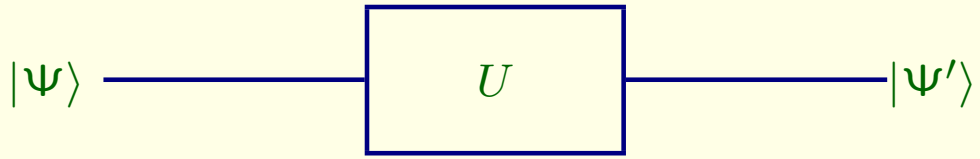
Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.





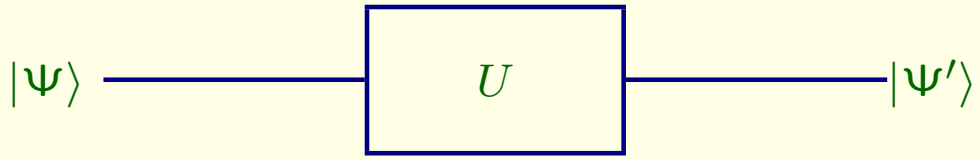

Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.

Bramka kwantowa to operacja przekształcająca stan kwantowy $|\Psi\rangle$ w nowy stan $|\Psi'\rangle$



Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.

Bramka kwantowa to operacja przekształcająca stan kwantowy $|\Psi\rangle$ w nowy stan $|\Psi'\rangle$

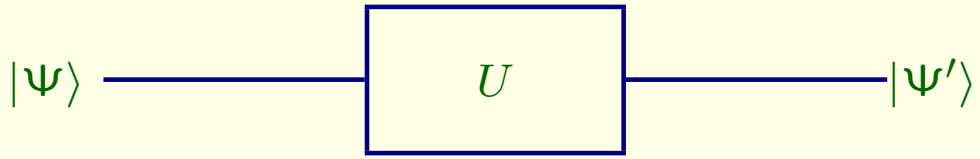


W bazie $\{|0\rangle, |1\rangle\}$, stany bazowe reprezentowane są przez macierze jednokolumnowe (wektory)

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

Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.

Bramka kwantowa to operacja przekształcająca stan kwantowy $|\Psi\rangle$ w nowy stan $|\Psi'\rangle$



W bazie $\{|0\rangle, |1\rangle\}$, stany bazowe reprezentowane są przez macierze jednokolumnowe (wektory)

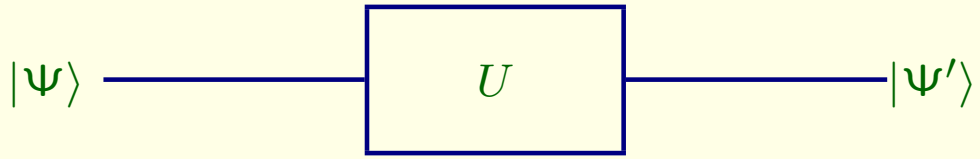
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

zaś jednokubitowa bramka U ma postać macierzy 2×2, np.

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

Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.

Bramka kwantowa to operacja przekształcająca stan kwantowy $|\Psi\rangle$ w nowy stan $|\Psi'\rangle$



W bazie $\{|0\rangle, |1\rangle\}$, stany bazowe reprezentowane są przez macierze jednokolumnowe (wektory)

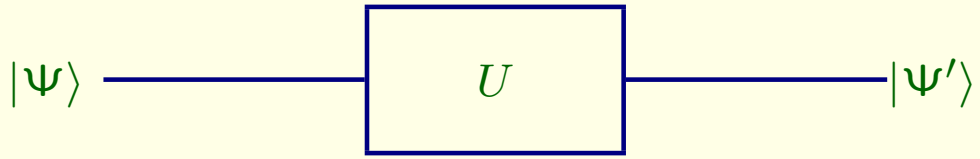
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

zaś jednokubitowa bramka U ma postać macierzy 2×2, np.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

Ewolucja stanów kwantowych (kubitów) opisywana jest równaniem Schrödingera.

Bramka kwantowa to operacja przekształcająca stan kwantowy $|\Psi\rangle$ w nowy stan $|\Psi'\rangle$



W bazie $\{|0\rangle, |1\rangle\}$, stany bazowe reprezentowane są przez macierze jednokolumnowe (wektory)

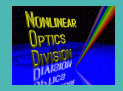
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

zaś jednokubitowa bramka U ma postać macierzy 2×2, np.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}, \quad \sqrt{NOT} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$$

Działanie bramki wygląda tak

$$NOT|0\rangle$$








Działanie bramki wygląda tak

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






Działanie bramki wygląda tak

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






Działanie bramki wygląda tak

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






Działanie bramki wygląda tak

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

$H|0\rangle$






Działanie bramki wygląda tak

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

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

Działanie bramki wygląda tak

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

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

Działanie bramki wygląda tak

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

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

Działanie bramki wygląda tak

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

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

$$\sqrt{NOT}|0\rangle$$

Działanie bramki wygląda tak

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

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

$$\sqrt{NOT}|0\rangle = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Działanie bramki wygląda tak

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

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

$$\sqrt{NOT}|0\rangle = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1+i}{2} \\ \frac{1-i}{2} \end{pmatrix}$$

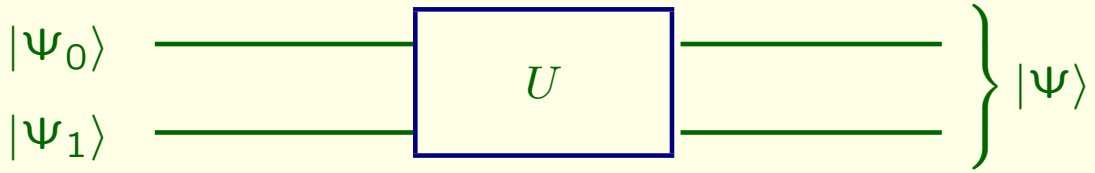
Działanie bramki wygląda tak

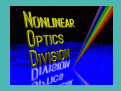
$$NOT|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

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

$$\sqrt{NOT}|0\rangle = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1+i}{2} \\ \frac{1-i}{2} \end{pmatrix} = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$$

dwubitowe

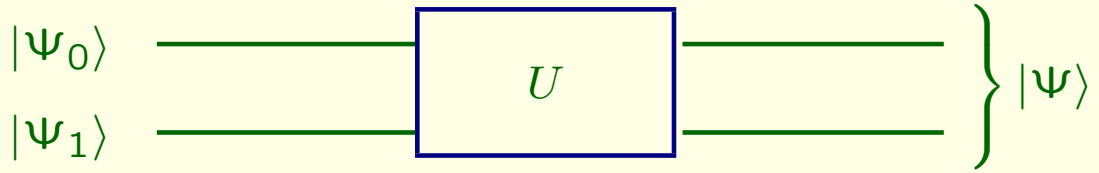









dwubitowe



Bazę w przestrzeni dwukubitowej tworzą stany $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Dwukubitowa bramka U opisywana jest w tej bazie macierzą 4×4, np.

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

Weźmy

$$|\Psi_0\rangle \quad = \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$






Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$






Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$CNOT|\Psi_0\rangle|\Psi_1\rangle$$

Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

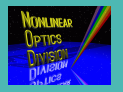
$$CNOT|\Psi_0\rangle|\Psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} =$$

Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$CNOT|\Psi_0\rangle|\Psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$








Weźmy

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$CNOT|\Psi_0\rangle|\Psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

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

Weźmy

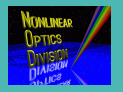
$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad |\Psi_1\rangle = |1\rangle$$

$$|\Psi_0\rangle \otimes |\Psi_1\rangle = |\Psi_0\Psi_1\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$CNOT|\Psi_0\rangle|\Psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

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

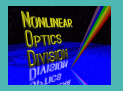
Otrzymaliśmy stan, który nie daje się rozseparować na iloczyn dwóch stanów (kubitów). Taki stan nazywamy stanem splątanym.








Stan $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ jest znaną parą EPR. Pomiar jednego kubitu da 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Ale jeśli pomiar pierwszego kubitu dał 0 to drugiego musi dać 1, i na odwrót! Niezależnie od tego jak daleko od siebie oddalone są oba kubity!

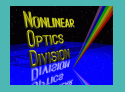







Stan $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ jest znaną parą EPR. Pomiar jednego kubitu da 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Ale jeśli pomiar pierwszego kubitu dał 0 to drugiego musi dać 1, i na odwrót! Niezależnie od tego jak daleko od siebie oddalone są oba kubity!

Układy wielokubitowe możemy traktować jako rejestry kwantowe, na których możemy wykonywać kwantowe operacje logiczne (unitarna ewolucja) lub pomiary.








Stan $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ jest znaną parą EPR. Pomiar jednego kubitu da 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Ale jeśli pomiar pierwszego kubitu dał 0 to drugiego musi dać 1, i na odwrót! Niezależnie od tego jak daleko od siebie oddalone są oba kubity!

Układy wielokubitowe możemy traktować jako rejestry kwantowe, na których możemy wykonywać kwantowe operacje logiczne (unitarna ewolucja) lub pomiary.

Stan

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






Stan $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ jest znaną parą EPR. Pomiar jednego kubitu da 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Ale jeśli pomiar pierwszego kubitu dał 0 to drugiego musi dać 1, i na odwrót! Niezależnie od tego jak daleko od siebie oddalone są oba kubity!

Układy wielokubitowe możemy traktować jako rejestry kwantowe, na których możemy wykonywać kwantowe operacje logiczne (unitarna ewolucja) lub pomiary.

Stan

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \end{aligned}$$

Stan $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ jest znaną parą EPR. Pomiar jednego kubitu da 0 lub 1 z prawdopodobieństwem $\frac{1}{2}$. Ale jeśli pomiar pierwszego kubitu dał 0 to drugiego musi dać 1, i na odwrót! Niezależnie od tego jak daleko od siebie oddalone są oba kubity!

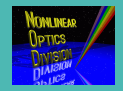
Układy wielokubitowe możemy traktować jako rejestry kwantowe, na których możemy wykonywać kwantowe operacje logiczne (unitarna ewolucja) lub pomiary.

Stan

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \end{aligned}$$

jest dwukubitowym rejestrem kwantowym w stanie superpozycji z jednakowymi amplitudami,w którym liczby od $0-3$ reprezentowane są z takim samym prawdopodobieństwem. Dla reprezentacji większych liczb potrzebujemy rejestrów wielokubitowych.

Procesor Chuanga to procesor 7 kubitowy.








Procesor Chuanga to procesor 7 kubitowy.

Bramki wielokubitowe można konstruować z bramek jedno- i dwukubitowych.






Procesor Chuanga to procesor 7 kubitowy.

Bramki wielokubitowe można konstruować z bramek jedno- i dwukubitowych.

W ten sposób możemy konstruować komputer kwantowy!






Procesor Chuanga to procesor 7 kubitowy.

Bramki wielokubitowe można konstruować z bramek jedno- i dwukubitowych.

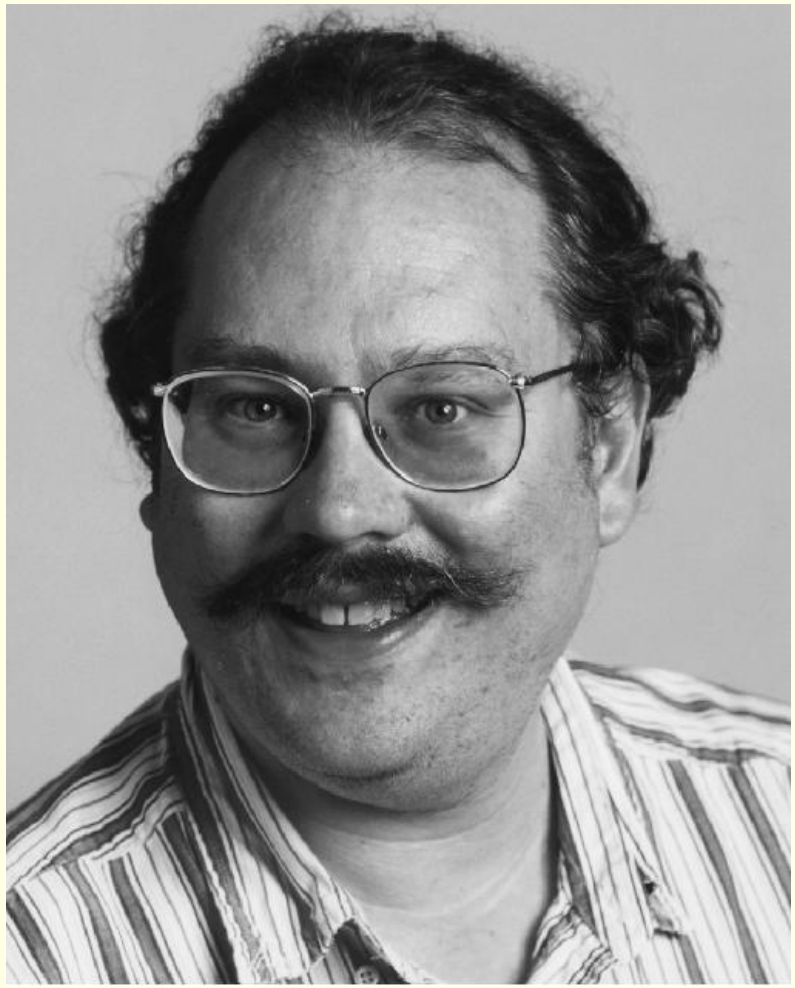
W ten sposób możemy konstruować komputer kwantowy!

Co taki komputer potrafi?






Algorytm Shora



Rysunek 3: Peter Shor

Motywacja

- Systemy kryptograficzne z kluczem publicznym wykorzystują fakt, że rozkład dużej liczby na czynniki jest trudny (czasochłonny)






Motywacja

- Systemy kryptograficzne z kluczem publicznym wykorzystują fakt, że rozkład dużej liczby na czynniki jest trudny (czasochłonny)
- Najszybszy obecnie algorytm wymaga czasu

  $\sim \exp[(\frac{64}{9})^{1/3}(\ln \ln N)^{2/3}]$

  faktoryzacja liczby 400 cyfrowej wymagałaby 10^{10} lat

Motywacja

- Systemy kryptograficzne z kluczem publicznym wykorzystują fakt, że rozkład dużej liczby na czynniki jest trudny (czasochłonny)
- Najszybszy obecnie algorytm wymaga czasu

  $\sim \exp[(\frac{64}{9})^{1/3}(\ln \ln N)^{2/3}]$

  faktoryzacja liczby 400 cyfrowej wymagałaby 10^{10} lat
- W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciągu 8 miesięcy

Motywacja

- Systemy kryptograficzne z kluczem publicznym wykorzystują fakt, że rozkład dużej liczby na czynniki jest trudny (czasochłonny)
- Najszybszy obecnie algorytm wymaga czasu

  $\sim \exp[(\frac{64}{9})^{1/3}(\ln \ln N)^{2/3}]$

  faktoryzacja liczby 400 cyfrowej wymagałaby 10^{10} lat
- W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciągu 8 miesięcy
- Algorytm kwantowy Petera Shora wymaga czasu

  $\sim (\ln N)^{2+\epsilon}$

  komputer kwantowy, który faktoryzowałby liczbę 130 cyfrową w ciągu miesiąca, sfaktoryzowałby liczbę 400 cyfrową w czasie krótszym niż 3 lata

Algorytm RSA

(Ron Rivest, Adi Shamir, Len Adleman)

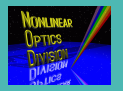
Kryptografia z kluczem publicznym

Klucz publiczny:	$\{e, N\}$
Klucz prywatny:	$\{d, N\}$
Szyfrowanie:	$C = M^e \mod N$
Deszyfrowanie:	$M = C^d \mod N$

Jak to działa?

- Mnożymy dwie duże liczby pierwsze p i q

  $\boxed{N = pq}$








Jak to działa?

- Mnożymy dwie duże liczby pierwsze p i q

  $$\boxed{N = pq}$$

- Znajdujemy funkcję Eulera

  $$\boxed{\varphi(N) = N - p - q + 1 = (p-1)(q-1)}$$






Jak to działa?

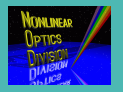
- Mnożymy dwie duże liczby pierwsze p i q

  $\boxed{N = pq}$

- Znajdujemy funkcję Eulera

  $\boxed{\varphi(N) = N - p - q + 1 = (p-1)(q-1)}$

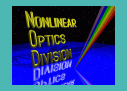
- Wybieramy losowo $\boxed{e < \varphi(N)}$ względnie pierwsze z $\varphi(N)$.








Jak to działa?



- Mnożymy dwie duże liczby pierwsze p i q

  $\boxed{N = pq}$

- Znajdujemy funkcję Eulera

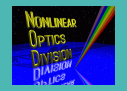
  $\boxed{\varphi(N) = N - p - q + 1 = (p-1)(q-1)}$

- Wybieramy losowo $\boxed{e < \varphi(N)}$ względnie pierwsze z $\varphi(N)$.

- Ujawniamy $\boxed{e \text{ i } N}$ — to jest nasz klucz publiczny.

  Teraz każdy może użyć naszego klucza publicznego do zaszyfrowania informacji przesyłanej do nas.

Jak to działa?



- Mnożymy dwie duże liczby pierwsze p i q

  $\boxed{N = pq}$

- Znajdujemy funkcję Eulera

  $\boxed{\varphi(N) = N - p - q + 1 = (p-1)(q-1)}$

- Wybieramy losowo $\boxed{e < \varphi(N)}$ względnie pierwsze z $\varphi(N)$.

- Ujawniamy $\boxed{e \text{ i } N}$ — to jest nasz klucz publiczny.

  Teraz każdy może użyć naszego klucza publicznego do zaszyfrowania informacji przesyłanej do nas.

- Wyznaczamy $\boxed{d < \varphi(N)}$ takie, że $\boxed{de = 1 \mod \varphi(N)}$.

  To jest nasz klucz prywatny, którego pilnie strzeżemy !!!

Przykład

Weźmy: $p = 11$, $q = 13$;

$N = 11 * 13 = 143$;

$\varphi(N) = 10 * 12 = 120$

wybieramy: $e = 7$;

$(120 - 1)/7 = 17$ jest całkowite;

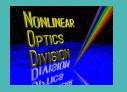
$d = 120 - 17 = 103$.

Weźmy: $\boxed{M = 31}$ (to jest wiadomość do zaszyfrowania)

Szyfrujemy: $\boxed{31^7 \mod 143 = 125}$

Rozszyfrowujemy: $\boxed{125^{103} \mod 143 = 31}$

Przykład



Weźmy: $p = 11$, $q = 13$;

$N = 11 * 13 = 143$;

$\varphi(N) = 10 * 12 = 120$

wybieramy: $e = 7$;

$(120 - 1)/7 = 17$ jest całkowite;

$d = 120 - 17 = 103$.

Weźmy: $\boxed{M = 31}$ (to jest wiadomość do zaszyfrowania)

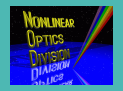
Szyfrujemy: $\boxed{31^7 \mod 143 = 125}$

Rozszyfrowujemy: $\boxed{125^{103} \mod 143 = 31}$

Jeśli chcesz się pobawić z większymi liczbami to ściągnij program autorstwa Michała Tanasia demostrujący działanie algorytmu RSA i łamanie szyfru. Do skompilowania programu pod Linuksem potrzebne są biblioteki GNU MP 4.1 oraz QT 3.x dostępne w Internecie. Po skompilowaniu programu można go uruchomić klikając na RSA demo poniżej. Pamiętaj jednak, że faktoryzacja jest problemem trudnym obliczeniowo!

RSA demo

Kwantowa faktoryzacja

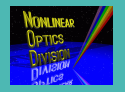


Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.






Kwantowa faktoryzacja

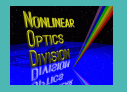


Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

Kwantowa faktoryzacja



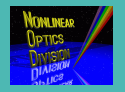
Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

Kwantowa faktoryzacja



Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

B

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

B	1	2	4	8

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

B	1	2	4	8	1	2	4	8

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

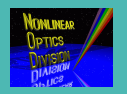
- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

B	1	2	4	8	1	2	4	8	1	2	4	8

Kwantowa faktoryzacja



Chcemy sfaktoryzować liczbę N, $N = 15$. Wybieramy liczbę losową $1 < X < N - 1$ względnie pierwszą z N, tzn. taką, że $NWD(N, X) = 1$, powiedzmy $X = 2$.

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

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

- Wykonujemy operację $B = X^A \mod N$, wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

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

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem $r = 4$

B	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

Komputer kwantowy potrafi szybko znajdować okres funkcji!

- Jeśli r jest nieparzyste, to wybieramy inne X i zaczynamy procedurę od nowa. Jeśli r jest parzyste, obliczamy $P = X^{r/2} - 1$ lub $P = X^{r/2} + 1$ i sprawdzamy czy P jest dzielnikiem N. W naszym przykładzie $r = 4$ i $P = 2^{4/2} - 1 = 3$ lub $P = 2^{4/2} + 1 = 5$.



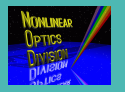



- Jeśli r jest nieparzyste, to wybieramy inne X i zaczynamy procedurę od nowa. Jeśli r jest parzyste, obliczamy $P = X^{r/2} - 1$ lub $P = X^{r/2} + 1$ i sprawdzamy czy P jest dzielnikiem N. W naszym przykładzie $r = 4$ i $P = 2^{4/2} - 1 = 3$ lub $P = 2^{4/2} + 1 = 5$.

Hurra !!!

$15/3 = 5$

$15/5 = 3$







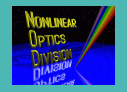

- Jeśli r jest nieparzyste, to wybieramy inne X i zaczynamy procedurę od nowa. Jeśli r jest parzyste, obliczamy $P = X^{r/2} - 1$ lub $P = X^{r/2} + 1$ i sprawdzamy czy P jest dzielnikiem N. W naszym przykładzie $r = 4$ i $P = 2^{4/2} - 1 = 3$ lub $P = 2^{4/2} + 1 = 5$.

Hurra !!!

$15/3 = 5$

$15/5 = 3$

Ten wynik udało się już uzyskać eksperymentalnie!



- Jeśli r jest nieparzyste, to wybieramy inne X i zaczynamy procedurę od nowa. Jeśli r jest parzyste, obliczamy $P = X^{r/2} - 1$ lub $P = X^{r/2} + 1$ i sprawdzamy czy P jest dzielnikiem N. W naszym przykładzie $r = 4$ i $P = 2^{4/2} - 1 = 3$ lub $P = 2^{4/2} + 1 = 5$.

Hurra !!!

$15/3 = 5$

$15/5 = 3$

Ten wynik udało się już uzyskać eksperymentalnie!

Komputer kwantowy liczy już do 15!






Kryptografia kwantowa

Czy zbudowanie komputera kwantowego spowoduje, że bezpieczne przesyłanie informacji stanie się niemożliwe?






Kryptografia kwantowa

Czy zbudowanie komputera kwantowego spowoduje, że bezpieczne przesyłanie informacji stanie się niemożliwe?

Nie!

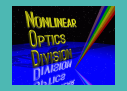
Kryptografia kwantowa

Czy zbudowanie komputera kwantowego spowoduje, że bezpieczne przesyłanie informacji stanie się niemożliwe?

Nie!

Bezpieczne przesyłanie informacji zapewnia
kryptografia kwantowa.

Kryptografia kwantowa



Czy zbudowanie komputera kwantowego spowoduje, że bezpieczne przesyłanie informacji stanie się niemożliwe?

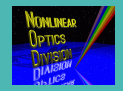
Nie!

Bezpieczne przesyłanie informacji zapewnia
kryptografia kwantowa.

Popularny wyklad na temat kryptografii kwantowej można znaleźć na mojej stronie:
`http://zon8.physd.amu.edu.pl/~tanas/`

Tam też można znaleźć ten wykład oraz program ilustrujący działanie RSA.

Zaproszenie do fizyki



Studiujcie fizykę kwantową!






Zaproszenie do fizyki

Studiujcie fizykę kwantową!

a może

Informatykę kwantową?!

Zaproszenie do fizyki

Studiujcie fizykę kwantową!

a może

Informatykę kwantową?!

Powodzenia!






Koniec