Wstęp do informatyki kwantowej

Andrzej Chmielowiec

Wydział Mechaniczno-Technologiczny
Politechniki Rzeszowskiej

7 lutego 2019

WYDZIAŁ
MECHANICZNO-
-TECHNOLOGICZNY
POLITECHNIKI RZESZOWSKIEJ

Podstawy matematyczne

Liczby niewymierne

Problem

Czy istnieje liczba wymierna, która jest rozwiązaniem równania

$$X^2 = 2$$

Liczby niewymierne

Problem

Czy istnieje liczba wymierna, która jest rozwiązaniem równania

$$X^2 = 2$$

Rozwiązanie

Skoro nie ma takiej liczby wymiernej, to wprowadźmy liczbę niewymierną o symbolu $\sqrt{2}$, która będzie rozwiązaniem tego równania

$$(\sqrt{2})^2 = 2$$

Problem

Czy istnieje liczba rzeczywista, która jest rozwiązaniem równania

$$X^2 = -1$$

Problem

Czy istnieje liczba rzeczywista, która jest rozwiązaniem równania

$$X^2 = -1$$

Rozwiązanie

Skoro nie ma takiej liczby rzeczywistej, to wprowadźmy liczbę nierzeczywistą o symbolu i, która będzie rozwiązaniem tego równania

$$i^2 = -1$$

Definicja

Liczbą zespoloną nazywamy liczbę postaci

$$z = a + bi,$$

gdzie a jest liczbą rzeczywistą określaną mianem części rzeczywistej, a b jest liczbą rzeczywistą określaną mianem części urojonej.

Definicja

Niech dane będą dwie liczby zespolone $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$$

Zatem i możemy traktować, tak samo jak niewiadomą x w równaniach.

Definicja

Niech dane będą dwie liczby zespolone $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$$

Zatem i możemy traktować, tak samo jak niewiadomą x w równaniach.

Przykład

$$(1 + 2i) + (2 + 3i) = 3 + 5i$$

Definicja

Niech dane będą dwie liczby zespolone $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$

$$\begin{aligned} z_1 \cdot z_2 &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= a_1 a_2 + a_1 b_2 i + a_2 b_1 i + b_1 b_2 i^2 \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i \end{aligned}$$

Zatem i możemy traktować, tak samo jak niewiadomą x w równaniach z tą różnicą, że zamiast i^2 wpisujemy -1.

Definicja

Niech dane będą dwie liczby zespolone $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$

$$\begin{aligned} z_1 \cdot z_2 &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= a_1 a_2 + a_1 b_2 i + a_2 b_1 i + b_1 b_2 i^2 \\ &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i \end{aligned}$$

Zatem i możemy traktować, tak samo jak niewiadomą x w równaniach z tą różnicą, że zamiast i^2 wpisujemy -1.

Przykład

$$(1 + 2i)(2 + 3i) = (2 - 6) + (3 + 4)i = -4 + 7i$$

Przykład

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$e_1 + e_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}(e_1 + e_2) = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Przykład

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R_{\pi/4} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

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

Definicja

Mnożenie wektora przez macierz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

Definicja

Mnożenie wektora przez macierz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

Przykład

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

Definicja

Mnożenie wektora przez macierz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

Przykład

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

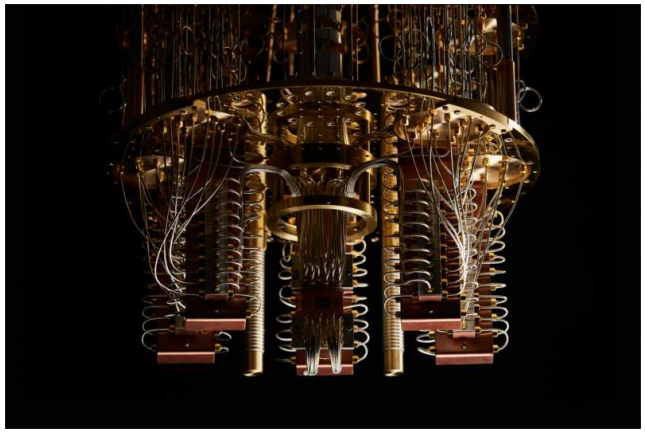
Przykład

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} - \frac{1}{2} \\ \frac{1}{2} + \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Bity i bramki kwantowe

WYDZIAŁ
MECHANICZNO-
-TECHNOLOGICZNY
POLITECHNIKI RZESZOWSKIEJ

IBM Q System One



IBM Q System One (2019)

20 bitów kwantowych dostępnych poza warunkami laboratoryjnymi

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Bit kwantowy – qbit

Definicja

Bitem kwantowym nazywamy system kwantowy posiadający dwa poziomy (stopnie swobody). Z matematycznego punktu widzenia często utożsamia się go z dwu-wymiarową przestrzenią Hilberta H_2, która posiada dwuelementową bazę $B = \{|0\rangle, |1\rangle\}$.

Elementy bazy zapisujemy w formie wektorowej jako

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

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Pomiar qbitu

Stan qbitu

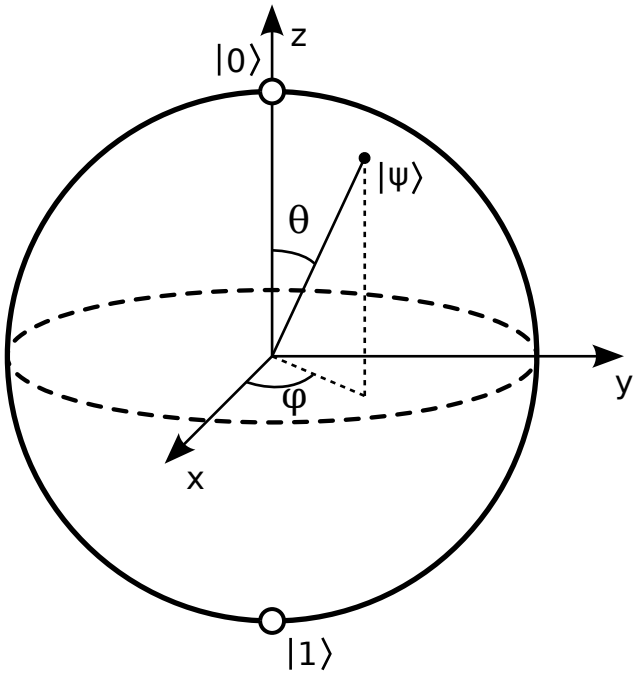
Stan bitu kwantowego reprezentowany jest przez wektor

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle ,$$

dla którego amplitudy α_i spełniają warunek $\alpha_0^2 + \alpha_1^2 = 1$.

Wynikiem pomiaru bitu kwantowego w takim stanie jest 0 z prawdopodobieństwem α_0^2 i 1 z prawdopodobieństwem α_1^2.

Sfera Blocha



Stan qbitu

$$
\begin{aligned}
|\psi\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \\
&= \cos\left(\frac{\theta}{2}\right)|0\rangle + \\
&\quad (\cos\varphi + i\sin\varphi)\sin\left(\frac{\theta}{2}\right)|1\rangle .
\end{aligned}
$$

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Bramka jednokrotna

Definicja

Przekształcenie pojedynczego qbitu jest nazywane bramką jednokrotną, jeżeli jest ono zadane przez pewne przekształcenie unitarne $U : H_2 \to H_2$.

Przekształcenie liniowe $|0\rangle \mapsto \alpha |0\rangle + \beta |1\rangle$, $|1\rangle \mapsto \gamma |0\rangle + \delta |1\rangle$ nazywamy unitarnym, jeżeli współczynniki spełniają warunek:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

co zapisujemy również jako $UU^* = I$.

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Bramka NOT (Pauli X)

Negacja qbitu zdefiniowana jest za pomocą następującego przekształcenia

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

Bramka ta neguje qbity przekazywane jako argumenty:

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

Bramki Y i Z:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bramka SQRT-NOT

Okazuje się, że bramkę NOT można zrealizować za pomocą złożenia dwóch identycznych przekształceń unitarnych

$$\sqrt{X} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$$

Bramka ta przekształca qbity w następujący sposób:

$$\begin{aligned} \sqrt{X}\,|0\rangle &= \frac{1+i}{2}\,|0\rangle + \frac{1-i}{2}\,|1\rangle\,, \\ \sqrt{X}\,|1\rangle &= \frac{1-i}{2}\,|0\rangle + \frac{1+i}{2}\,|1\rangle\,. \end{aligned}$$

Bramka $S = \sqrt{Z}$

Okazuje się, że bramkę Z można zrealizować za pomocą złożenia dwóch identycznych przekształceń unitarnych

$$S = \sqrt{Z} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

Bramka $T = \sqrt{S}$

Okazuje się, że bramkę S można zrealizować za pomocą złożenia dwóch identycznych przekształceń unitarnych

$$T = \sqrt{S} = \begin{pmatrix} \frac{-1+i}{\sqrt{2}} & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

Bramka Hadamarda (H)

Bramka Hadamarda jest jedną z ważniejszych operacji na bitach kwantowych

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

Bramka ta neguje qbity przekazywane jako argumenty:

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

Ważna własność bramki H

$$H^2|0\rangle = |0\rangle, \quad H^2|1\rangle = |1\rangle.$$

System dwóch bitów kwantowych tworzy przestrzeń $H_4 = H_2 \otimes H_2$, gdzie $\otimes$ jest iloczynem tensorowym.

Iloczyn tensorowy

Jeżeli $V_1 = \mathrm{Lin}(\mathbf{x_1}, \mathbf{x_2})$ i $V_2 = \mathrm{Lin}(\mathbf{y_1}, \mathbf{y_2})$, to

$$V_1 \otimes V_2 = \mathrm{Lin}(\mathbf{x_1} \otimes \mathbf{y_1}, \mathbf{x_1} \otimes \mathbf{y_2}, \mathbf{x_2} \otimes \mathbf{y_1}, \mathbf{x_2} \otimes \mathbf{y_2}),$$

gdzie $\mathbf{x_i} \otimes \mathbf{y_j}$ są wektorami bazy iloczynu tensorowego V_1 i V_2 oznaczanymi przez $\mathbf{x_i y_j}$. Ponadto dla dowolnych wektorów $\mathbf{v_1} = \alpha_1 \mathbf{x_1} + \alpha_2 \mathbf{x_2}$, $\mathbf{v_2} = \beta_1 \mathbf{y_1} + \beta_2 \mathbf{y_2}$ mamy

$$\mathbf{v_1} \otimes \mathbf{v_2} = \sum_{i,j} \alpha_i \beta_j \mathbf{x_i y_j}.$$

MECHANICZNO-
-TECHNOLOGICZNY
POLITECHNIKI RZESZOWSKIEJ

Iloczyn tensorowy qbitów

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

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = (0,0,1,0)^T, \quad |11\rangle = (0,0,0,1)^T.$$

Stany rozkładalne i splątane

Jeżeli stan kwantowy $z \in H_4$ złożony z dwóch bitów kwantowych możemy zapisać jako iloczyn tensorowy stanów pojedynczych bitów, to taki stan z nazywamy **rozkładalnym**. Jeżeli operacja taka jest niemożliwa, to taki stan nazywamy **splątanym**.

Przykład stanu rozkładalnego

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \otimes \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]$$

Przykład stanu splątanego

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle .$$

Stany splątane

Uwaga!

Jeśli dwa qbity są w stanie splątanym $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, to obserwacja jednego z nich może dać wartość 0, bądź 1 z prawdopodobieństwem $\frac{1}{2}$. Nie jest jednak możliwe obserwowanie różnych wartości na tych qbitach (albo pomiar obu daje wartość 00, albo 11). Doświadczenia pokazały, że jest to prawdą także w przypadku qbitów odległych od siebie nawet o więcej niż 10 km.

Bramka dwukrotna

Definicja

Jednoczesne przekształcenie dwóch qbitów jest nazywane bramką dwukrotną, jeżeli jest ono zadane przez pewne przekształcenie unitarne $U : H_4 \to H_4$, gdzie $H_4 = H_2 \otimes H_2$.

Do zdefiniowania operacji na bramce dwukrotnej wykorzystujemy następującą reprezentację qbitów: $|00\rangle = (1,0,0,0)^T, |01\rangle = (0,1,0,0)^T, |10\rangle = (0,0,1,0)^T, |11\rangle = (0,0,0,1)^T$.

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Przykład bramki dwukrotnej

Bramka CNOT (cX)

Warunkowa negacja qbitu zdefiniowana jest za pomocą następującego przekształcenia

$$cX = M_{\text{cnot}} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Bramka ta neguje drugi qbit w zależności od wartości pierwszego:

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

Analogicznie można zdefiniować bramki cY i cZ:

$$cY = \begin{pmatrix} I & 0 \\ 0 & Y \end{pmatrix}, \quad cZ = \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}.$$

Przykład bramki dwukrotnej

Dwukrotna bramka Hadamarda (H)

Iloczyn tensorowy dwóch jednokrotnych bramek Hadamarda daje nam bramkę dwukrotną

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

Jej działanie na dwu qbitowym argumencie wygląda następująco

$$H|x_0x_1\rangle = \frac{1}{2}(|00\rangle + (-1)^{x_1}|01\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_0+x_1}|11\rangle).$$

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Przykład bramki dwukrotnej

Działanie bramek dwukrotnych

Jeżeli bramka dwukrotna jest iloczynem tensorowym dwóch bramek jednokrotnych, to wynik jej działania tworzy rozkładalny stan bitów (bramka Hadamarda).

Jeżeli bramka dwukrotna nie może być reprezentowana jako iloczyn tensorowy bramek jednokrotnych, to jej działanie tworzy splątany stan bitów (bramka cX).

WYDZIAŁ MECHANICZNO-TECHNOLOGICZNY POLITECHNIKI RZESZOWSKIEJ

Kopiowanie bitów kwantowych

No-Cloning Theorem

Nie istnieje przekształcenie unitarne U takie, że dla dowolnego qbitu mamy:

$$U(|xa_1\rangle) = |xx\rangle \, .$$

Innymi słowy - nie ma możliwości skopiowania qbitu.

Niezależnie od braku możliwości kopiowania dowolnych stanów kwantowych należy podkreślić, że bez problemu możemy tworzyć kopie elementów bazy. Możemy zatem kopiować qbity $|0\rangle$ i $|1\rangle$.

Podstawowe algorytmy i programowanie kwantowe

WYDZIAŁ
MECHANICZNO-
-TECHNOLOGICZNY
POLITECHNIKI RZESZOWSKIEJ

Załóżmy, że Alicja chce przesłać Bobowi qbit w stanie

$$a\,|0\rangle + b\,|1\rangle.$$

Dodatkowo będziemy zakładali, że obie strony dysponują po jednym qbicie ze stanu splątanego

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

przy czym Alicja posiada qbit lewy, a Bob posiada qbit prawy. W użyciu są zatem 3 qbity, których stan dany jest wzorem:

$$s_0 = \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle).$$

$s_0 \to s_1$

Alicja stosuje bramkę cX na swoich bitach

$$s_1 = \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle).$$

$s_1 \rightarrow s_2$

Alicja stosuje bramkę H na pierwszym bicie (najbardziej lewym)

$$\begin{aligned} s_2 &= \frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \\ &\quad \frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle \\ &= \frac{1}{2}|00\rangle(a|0\rangle + b|1\rangle) + \frac{1}{2}|01\rangle(a|1\rangle + b|0\rangle) + \\ &\quad \frac{1}{2}|10\rangle(a|0\rangle - b|1\rangle) + \frac{1}{2}|11\rangle(a|1\rangle - b|0\rangle). \end{aligned}$$

Alicja sprawdza wartość bitów i wysyła wynik do Boba.

Przejście do właściwego stanu kwantowego

Bob odbiera bity przesłane przez Alicję i stwierdza w jakim stanie jest jego qbit

$$
\begin{aligned}
00 &\rightarrow s = a|0\rangle + b|1\rangle \rightarrow Is = a|0\rangle + b|1\rangle \\
01 &\rightarrow s = a|1\rangle + b|0\rangle \rightarrow Xs = a|0\rangle + b|1\rangle \\
10 &\rightarrow s = a|0\rangle - b|1\rangle \rightarrow Zs = a|0\rangle + b|1\rangle \\
11 &\rightarrow s = a|1\rangle - b|0\rangle \rightarrow ZXs = a|0\rangle + b|1\rangle
\end{aligned}
$$

Kwantowy algorytm faktoryzacji Shora

Idea

W celu wyznaczenia dzielnika liczby N losujemy liczbę $a \in \{1, \ldots, N-1\}$

1. Sprawdzamy, czy $(a, N) \neq 1$
2. Wyznaczamy liczbę r taką, że $a^r \equiv 1 \bmod N$
3. Co najmniej połowa liczb r będzie taka, że $(a^r - 1, N) \neq 1$

W punkcie 2 stosujemy kwantową transformatę Fouriera do wyznaczenia liczby r.