Kubity

Ponieważ aparatura pomiarowa będzie traktowana jako stacjonarna, będziemy używali tylko jednej bazy uporządkowanej do wysyłania i odbierania kubitów. Nasuwającym się wyborem jest baza standardowa $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$. Wcześniej oznaczaliśmy ją jako $(|\uparrow\rangle,|\downarrow\rangle)$. Wspominaliśmy też, że pierwszy wektor w bazie wiążemy z wartością 0, a drugi wektor z wartością 1. Teraz, gdy będziemy używać wyłącznie jednej bazy, sensownie jest nadać ketom nazwy, które sugerowałyby, jak te kety mają się do bitów. Niech $|0\rangle$ oznacza $\begin{bmatrix}1\\0\end{bmatrix}$, a $|1\rangle$ oznacza $\begin{bmatrix}0\\1\end{bmatrix}$.

W ogólności kubit posiada formę $a_0|0\rangle+a_1|1\rangle$, gdzie $a_0^2+a_1^2=1$. W momencie pomiaru stan przeskakuje albo na $|0\rangle$ i wtedy odczytujemy wynik 0, albo na $|1\rangle$ i wtedy odczytujemy wynik 1. Pierwsza ewentualność ma prawdopodobieństwo a_0^2, a druga a_1^2.

Zazwyczaj będziemy dysponować systemem składającym się z więcej niż jednego kubitu, co oznacza, że będziemy musieli formować iloczyny tensorowe. Dla systemów z dwoma kubitami baza uporządkowana będzie miała postać:

$$\left(\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\right)$$

Można to zapisać jako $(|0\rangle\otimes|0\rangle,|0\rangle\otimes|1\rangle,|1\rangle\otimes|0\rangle,|1\rangle\otimes|1\rangle)$. Jak zauważyliśmy wcześniej, często dla wygody pomijamy symbole iloczynu tensorowego, dzięki czemu możemy ten iloczyn zapisać jeszcze bardziej zwięźle jako $(|0\rangle|0\rangle,|0\rangle|1\rangle,|1\rangle|0\rangle,|1\rangle|1\rangle)$. Wprowadzamy na końcu konwencję, by $|a\rangle|b\rangle$ zapisywać jako $|ab\rangle$, dzięki czemu otrzymujemy zapis $(|00\rangle,|01\rangle,|10\rangle,|11\rangle)$, który jest krótki i łatwy do odczytania.

Jak się to wszystko ma do bramek logicznych? Odpowiedź na to pytanie rozważymy już za chwilę. Zacznijmy od przyjrzenia się bramce *CNOT*.

Bramka *CNOT*

Klasyczna bramka *CNOT* przyjmuje dwa bity na wejściu i generuje dwa bity na wyjściu. Definiujemy ją następującą tabelą:

CNOT

Wejście		Wyjście	
x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Rozszerzamy to do kubitów w sposób naturalny – zamieniamy 0 na $|0\rangle$ i 1 na $|1\rangle$. Tabela przyjmuje postać:

CNOT

Wejście		Wyjście	
x	Y	x	$x \oplus y$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Można to samo zapisać zwięźlej, używając kompaktowej notacji dla iloczynów tensorowych:

CNOT

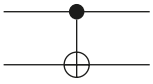
Wejście	Wyjście
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Na podstawie tej tabeli wiadomo, co się dzieje z bazowymi wektorami. Rozszerzamy to do kombinacji liniowych wektorów bazowych w sposób naturalny:

$$CNOT\,(r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle) = r|00\rangle + s|01\rangle + u|10\rangle + t|11\rangle$$

Bramka zamienia amplitudy prawdopodobieństwa dla $|10\rangle$ i $|11\rangle$.

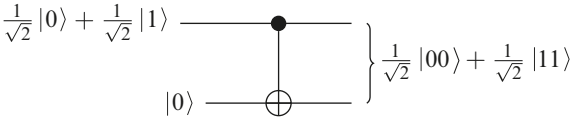
Używamy tego samego schematu, z którego korzystaliśmy poprzednio dla bramki *CNOT*, musimy jednak uważać na sposób, w jaki to interpretujemy. W przypadku bitów klasycznych bit, który wchodził na górną linię z lewej, wychodził na górnej linię z prawej niezmieniony. Nadal to zachodzi, jeśli kubit nagórnej linii znajdował się w stanie $|0\rangle$ lub $|1\rangle$, ale nie jest to prawdą dla pozostałych kubitów.



Załóżmy, że na górze mamy kubit w stanie $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$, a na dole kubit w stanie $|0\rangle$.

Wejście wynosi $\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\otimes|0\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle$. Ten stan zostaje zamieniony przez bramkę *CNOT* na $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$.

Ten stan, jak pamiętamy z rozważań nad eksperymentem *EPR*, jest stanem splątanym. W rezultacie nie możemy już przypisywać oddzielnych stanów liniom górnym i dolnym. Schemat rysujemy w taki sposób:



Linie reprezentują nasze elektrony lub fotony. Są one oddzielonymi od siebie obiektami i mogą znajdować się bardzo daleko od siebie. Pamiętajmy jednak, że skoro są one splątane, każdy pomiar na jednym z nich wpłynie na drugi.

Ten przykład ilustruje też, w jaki sposób będziemy często używać tej bramki logicznej. Możemy wprowadzić do bramki dwa niesplątane kubity i użyć jej do ich splątania.

Kwantowe bramki logiczne

Zauważmy, że bramka *CNOT* permutuje bazowe wektory. Permutacja bazowych wektorów w uporządkowanej bazie ortonormalnej generuje inną uporządkowaną bazę ortonormalną. Wiemy, że każdej takiej bazie ortonormalnej odpowiada określona macierz ortogonalna. W zasadzie wszystkie odwracalne bramki, jakie przedstawiliśmy w poprzednim rozdziale, permutują wektory bazowe. Wszystkie odpowiadają macierzom ortogonalnym.

To pozwala zdefiniować kwantowe bramki logiczne. Są one operacjami, które mogą być opisane przez macierze ortogonalne.

Tak jak w przypadku klasycznych obliczeń, chcemy uzbierać małą kolekcję prostych bramek logicznych, które będzie można łączyć w obwody. Zaczniemy od przyjrzenia się najprostszym bramkom, takim, które działają tylko na jeden kubit.

Kwantowe bramki logiczne działające na jeden kubit

W klasycznym wydaniu odwracalnych obliczeń istnieją dwie możliwe operacje boolowskie, które można przeprowadzić na jednym bicie: identyczność, która pozostawia bit takim, jakim był, i *NOT*, która zamienia miejscami wartości 0 i 1. Dla kubitów istnieje nieskończenie wiele możliwych bramek logicznych!

Zacznijmy od dwóch bramek kwantowych odpowiadających klasycznej identyczności. Obie pozostawiają kubity $|0\rangle$ i $|1\rangle$ niezmienione. Następnie przyjrzyjmy się dwóm bramkom kwantowym, które odpowiadają zamianie miejscami wartości kubitów $|0\rangle$ i $|1\rangle$. Te cztery bramki nazwane zostały „transformacjami Pauliego" od nazwiska Wolfganga Pauliego.

Bramki I i Z

Bramka I jest po prostu macierzą identyczności (macierzą jednostkową) $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$.

Zobaczymy, jak I oddziałuje na dany kubit $a_0|0\rangle+a_1|1\rangle$.

$$I(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}a_0\\ a_1\end{bmatrix} = \begin{bmatrix}a_0\\ a_1\end{bmatrix} = a_0|0\rangle + a_1|1\rangle$$

Nie jest zaskoczeniem, że I działa jak identyczność i zostawia kubit niezmieniony.

Bramka Z jest zdefiniowana macierzą $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$.

I znów zobaczmy, jak Z działa na dany kubit $a_0|0\rangle+a_1|1\rangle$.

$$Z(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}a_0\\ a_1\end{bmatrix} = \begin{bmatrix}a_0\\ -a_1\end{bmatrix} = a_0|0\rangle - a_1|1\rangle$$

Z pozostawia niezmienioną amplitudę prawdopodobieństwa dla $|0\rangle$, ale zmienia znak amplitudy prawdopodobieństwa dla $|1\rangle$. Ale zobaczmy dokładniej, co właściwie robi Z.