Algorytm Deutscha

David Deutsch jest jednym z ojców założycieli obliczeń kwantowych. W 1985 roku opublikował przełomowy artykuł opisujący kwantowe maszyny Turinga i obliczenia kwantowe[2]. Zamieścił w nim również poniższy algorytm – pierwszy historycznie algorytm, który pokazywał, że algorytm kwantowy może być szybszy od klasycznego.

Zagadnienie dotyczy funkcji z tylko jedną zmienną. Na wejściu możemy mieć 0 albo 1. Na wyjściu również otrzymujemy 0 lub 1. Istnieją cztery takie funkcje, które oznaczymy f_0, f_1, f_2 i f_3:

Funkcja f_0 odwzorowuje oba rodzaje wartości początkowych na 0, tzn. $f_0(0)=0$ i $f_0(1)=0$;
Funkcja f_1 odwzorowuje 0 na 0, a 0 na 1, tzn. $f_1(0)=0$, a $f_1(1)=1$;
Funkcja f_2 odwzorowuje 0 na 1, a 1 na 0, tzn. $f_2(0)=1$ i $f_2(1)=0$;
Funkcja f_3 odwzorowuje oba rodzaje wartości początkowych na 1, tzn. $f_3(0)=1$ i $f_3(1)=1$.

Funkcja f_0 i f_3 są funkcjami stałymi. Na wyjściu mamy zawsze to samo, niezależnie od wejścia. Funkcję nazywamy zbalansowaną, jeśli połowę swoich wejść odwzorowuje na 0, a połowę na 1. Zarówno f_1, jak i f_2 są zbalansowane.

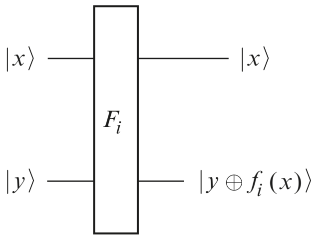
Pytanie Deutscha brzmi: jeśli dostaniemy jedną z tych funkcji, ile ewaluacji musimy przeprowadzić, żeby zdecydować, czy dana funkcja jest stała, czy zbalansowana. Jest bardzo ważne, byśmy dokładnie zrozumieli, o co pytamy. Nie pytamy o to, którą dokładnie z czterech funkcji dysponujemy, interesuje nas tylko to, czy dana funkcja jest stała, czy nie.

Klasyczna analiza wygląda następująco. Możemy dokonać ewaluacji naszej funkcji albo dla 0, albo dla 1. Jeśli zechcemy przeprowadzić ewaluację dla 0, mamy dwa możliwe scenariusze – otrzymamy albo 0, albo 1. Jeśli otrzymamy zero, wiemy tylko, że $f(0)=0$. Dana nam funkcja może być równa f_0 lub f_1. Ponieważ jedna z nich jest stała, a druga zbalansowana, musimy jeszcze raz obliczyć wartość funkcji, by zdecydować, która to z nich. W klasycznym podejściu trzeba przeprowadzić obliczenia zarówno do 0, jak i dla 1 – musimy więc użyć funkcji dwa razy.

Przypatrzmy się teraz kwantowej wersji tego pytania. Najpierw konstruujemy bramki logiczne odpowiadające tym czterem funkcjom. Rysunek na stronie 153 ilustruje bramki, gdzie i może wynosić 0, 1, 2 lub 3.

---

[2] *Quantum theory, the Church-Turing principle and the universal quantum computer*, „Proceedings of the Royal Society A" 400 (1818) s. 97–117.



Ilustracja informuje:

Jeśli na wejściu będziemy mieli $|0\rangle \otimes |0\rangle$, na wyjściu otrzymamy $|0\rangle \otimes |f_i(0)\rangle$.

Jeśli na wejściu będziemy mieli $|0\rangle \otimes |1\rangle$, to na wyjściu otrzymamy $|0\rangle \otimes |f_i(0) \oplus 1\rangle$.

Jeśli na wejściu będziemy mieli $|1\rangle \otimes |0\rangle$, to na wyjściu otrzymamy $|1\rangle \otimes |f_i(1)\rangle$.

Jeśli na wejściu będziemy mieli $|1\rangle \otimes |1\rangle$, to na wyjściu otrzymamy $|1\rangle \otimes |f_i(1) \oplus 1\rangle$.

Zauważmy, że dla każdego *i* jedno z pary: $f_i(0)$, $f_i(0) \oplus 1$ jest równe 0, a drugie z nich jest równe 1. Podobnie, dla każdego *i* jedno z pary $f_i(1)$, $f_i(1) \oplus 1$ jest równe 0, a drugie z nich jest równe 1.

Oznacza to, że każde z czterech możliwych wyjść zawsze daje elementy bazy standardowej, co oznacza, że macierz reprezentująca tę bramkę jest ortogonalna – wobec tego rzeczywiście dysponujemy tu kwantową bramką logiczną.

Chociaż na wejściu wprowadzamy dwa bity informacji i na wyjściu również dysponujemy dwoma bitami, informacja, jaką ta bramka udziela dla bitów klasycznych, $|0\rangle$ i $|1\rangle$, jest dokładnie taka sama, co dla funkcji poprzednio ewaluowanych dla 0 i 1. Górny kubit wyjściowy jest dokładnie taki sam, jak na wejściu, tak więc nie daje nam on żadnych nowych informacji. Wybór między $|0\rangle$ a $|1\rangle$ dla drugiego kubitu daje funkcję obliczaną na górnym kecie wejścia albo odwrotną odpowiedź. Jeśli znamy jedną z tych odpowiedzi, znamy również drugą.

Kwantowa wersja naszego pytania brzmi: jeśli dostaniemy losowo jedną z czterech bramek, jak wiele razy będziemy musieli użyć bramki, by móc określić, czy określająca ją funkcja f_i jest stała, czy zbalansowana.

Jeśli ograniczymy się do wprowadzania do bramki tylko $|0\rangle$ i $|1\rangle$, to analiza wygląda dokładnie tak samo, jak poprzednio. Będziemy musieli użyć bramki dwa razy. David Deutsch wykazał jednak, że jeśli możemy