Poza klasycznymi ograniczeniami: moc i potencjał obliczeń kwantowych

*Pranav CHALLA**

* Uczeń, Queen Elzabeth's School

Wyobraź sobie komputer łamiący zaledwie w kilka sekund kody, których odszyfrowanie klasycznym komputerom zajęłoby miliony lat. Wyobraź sobie komputer, który mógłby przetwarzać wiele różnych zestawów danych jednocześnie. To wszystko właśnie umożliwiają nam obliczenia kwantowe – dzięki wykorzystaniu praw mechaniki kwantowej (fundamentalnych zasad rządzących zachowaniem najmniejszych cząstek) i manipulacji ich niezwykłymi właściwościami zwiększają prędkości obliczeń do poziomów nieosiągalnych dla klasycznych komputerów.

Dwie kluczowe właściwości kwantowe, które omówię, to *superpozycja* i *splątanie*.

Superpozycja

Jak wiadomo, klasyczne komputery wykorzystują bity istniejące w stanie 0 lub 1, natomiast komputery kwantowe używają kubitów (bitów kwantowych), które dzięki zjawisku superpozycji mogą istnieć w stanach 0, 1 lub obu jednocześnie. Aby lepiej zrozumieć zjawisko superpozycji, przeanalizujmy jego matematyczne podstawy. Stan kwantowy można zapisać jako:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

α i β są tu liczbami zespolonymi spełniającymi warunek normalizacji $|\alpha|^2 + |\beta|^2 = 1$. Tutaj $|\alpha|^2$ i $|\beta|^2$ odpowiadają prawdopodobieństwom znalezienia kubitu w stanach $|0\rangle$ i $|1\rangle$.

Na przykład stan $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ oznacza, że prawdopodobieństwa tego, że kubit po pomiarze znajdzie się w stanie $|0\rangle$ i $|1\rangle$, są równe.

Zjawisko superpozycji jest kluczowe dla obliczeń kwantowych, gdyż pozwala na równoczesne przetwarzanie danych. Ponieważ jeden kubit może przechowywać informacje o dwóch stanach jednocześnie, dwa kubity w superpozycji mogą reprezentować cztery stany ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$), a n kubitów może reprezentować jednocześnie 2^n stanów. To umożliwia bardziej efektywne algorytmy wyszukiwania, takie jak algorytm Grovera, który może przeszukiwać N nieposortowanych elementów w czasie $\sqrt{N}$, przełamując klasyczny limit N wyszukiwań dla listy nieposortowanych elementów.

Algorytm Grovera działa poprzez proces znany jako *wzmocnienie amplitudy*. Wyobraźmy sobie zestaw 32 elementów, z których jeden jest oznaczony jako poprawny. Na początku ustawiana jest superpozycja 5 kubitów, z których każdy z 32 stanów odpowiada jednemu elementowi. Następnie stosowane są operatory kwantowe zwiększające prawdopodobieństwo wyboru poprawnego elementu. Proces ten jest powtarzany, aż wszystkich 5 kubitów odzwierciedli stan $|1\rangle$ lub $|0\rangle$, odpowiadający właściwemu elementowi.

Splątanie

Splątanie kwantowe to właściwość, dzięki której dwie cząstki kwantowe stają się ze sobą powiązane. Jeśli dwie cząstki są splątane, pomiar jednej dostarcza informacji o drugiej. Dobrym porównaniem jest para butów. Wyobraźmy sobie, że każdą parę butów umieszczamy w osobnym pudełku. Otwierając jedno pudełko i znajdując but lewy, możemy być pewni, że w drugim pudełku znajduje się but prawy. Różnica polega na tym, że buty nie mogą znajdować się w superpozycji, a kubity mogą.

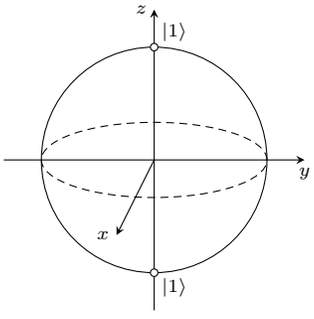
Rozważmy na przykład stan dwóch splątanych kubitów:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

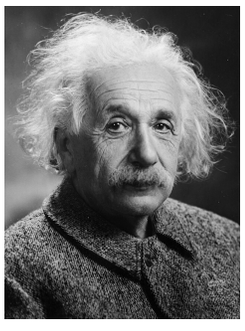
Jeśli jako wynik pomiaru pierwszego kubitu otrzymamy $|0\rangle$, to drugi kubit również będzie w stanie $|0\rangle$. Jeśli pierwszy kubit będzie w stanie $|1\rangle$, drugi

Niektóre algorytmy szyfrowania, na przykład RSA, oparte są na trudności rozkładu dużych liczb na czynniki pierwsze. W 1994 roku Peter Shor wskazał algorytm, który rozwiązuje to w czasie zaledwie $O(\log(N)^2)$. Więcej o algorytmie Shora można przeczytać w Δ_{17}^{12}.

Wszystkie możliwe stany kubitu można przedstawić jako punkty na sferze w trójwymiarowej przestrzeni. Bieguny tej sfery reprezentują stany $|1\rangle$ i $|0\rangle$, a *równik* reprezentuje stany będące w idealnej superpozycji. Ta reprezentacja została nazwana sferą Blocha na cześć fizyka Felixa Blocha.



Koncepcja cząstek natychmiastowo oddziałujących na siebie na odległość była tak nieintuicyjna, że Albert Einstein nazwał splątanie kwantowe „upiornym działaniem na odległość".



również będzie w $|1\rangle$. Ta korelacja występuje niezależnie od odległości między kubitami, co umożliwia poziom koordynacji nieosiągalny dla klasycznych bitów. Oznacza to, że prawdopodobieństwo zaobserwowania stanów $|01\rangle$ lub $|10\rangle$ jest równe 0.

Zastosowania splątania kwantowego są szeroko rozpowszechnione w algorytmach kwantowych. Na przykład splątanie kwantowe umożliwia zastosowanie supergęstego kodowania, czyli algorytmu kwantowego, który pozwala na przesyłanie większej liczby klasycznych bitów informacji przy użyciu mniejszej liczby kubitów. Innym zastosowaniem splątania kwantowego jest teleportacja kwantowa. Ten teoretyczny proces pozwala na transfer informacji za pośrednictwem splątanych cząstek. W tym procesie dwie strony – znajdujące się w dowolnej odległości od siebie – wykorzystują wspólny splątany stan do przekazania informacji o danym stanie kwantowym z jednej lokalizacji do drugiej. Proces ten nazywany jest teleportacją stanu kwantowego.

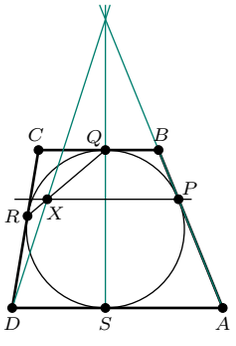
W 2012 roku naukowcom udało się osiągnąć teleportację kwantową na odległość 143 km, z La Palmy do Teneryfy, *arXiv:1205.3909 [quant-ph]*.

Obecna technologia kwantowa

Technologia kwantowa jest wciąż w fazie początkowej, ale dokonano już znaczących postępów. Duże firmy technologiczne, takie jak Google, IBM i Intel, budują komputery z coraz większą liczbą kubitów, jednak wciąż zmagają się z redukcją błędów. Obecnie dysponujemy urządzeniami NISQ (Noisy Intermediate-Scale Quantum), które mają wystarczającą liczbę kubitów do pewnych obliczeń kwantowych, ale są podatne na błędy i dekoherencję. Naukowcy pracują nad technikami korekcji błędów i kodami korekcji kwantowej, by zmniejszyć dekoherencję. Długoterminowym celem jest budowa odpornych na błędy komputerów kwantowych, które znajdą zastosowanie w różnych branżach.

Największy komputer kwantowy na świecie to system 1180 kubitów opracowany przez Atom Computing. Każdy kubit jest neutralnym atomem, uwięzionym i kontrolowanym przez układ laserów.

Zadania



Przygotował Dominik BUREK

M 1813. Niech $ABCD$ będzie trapezem $(DA \| CB)$ opisanym na okręgu, który jest styczny do boków AB, BC, CD i AD odpowiednio w punktach P, Q, R, S. Prosta przechodząca przez P i równoległa do podstaw trapezu przecina prostą QR w punkcie X. Udowodnić, że proste AB, QS i DX przecinają się w jednym punkcie.

M 1814. Dane są liczby a, $b > 1$, dla których

$$a + \frac{1}{a^2} \geqslant 5b - \frac{3}{b^2}.$$

Udowodnić, że $a > 5b - \dfrac{4}{b^2}$.

M 1815. Dane są liczby całkowite $n > 20$ i $k > 1$ takie, że $k^2 \mid n$. Udowodnić, że istnieją dodatnie liczby całkowite a, b, c, dla których

$$n = ab + bc + ca.$$

Przygotował Andrzej MAJHOFER

F 1117. W szczelnie zamkniętm cylindrze, pod tłokiem znajduje się $m = 10$ g ciekłej wody. Bardzo szybkie przesunięcie tłoka powoduje spadek ciśnienia w cylindrze do wartości bliskiej zeru. Temperatura otoczenia i cylindra z wodą wynosi 0°C. Ile lodu wytworzy się w wyniku tego procesu? Można przyjąć, że początkowo pod tłokiem była wyłącznie ciekła woda. Ciepło topnienia wody $L_f \approx 334$ J/g, a ciepło parowania $L_v \approx 2260$ J/g.

F 1118. W szczelnym pojemniku znajduje się mieszanina helu i neonu. Mieszanina jest w równowadze termodynamicznej, przy czym liczby moli neonu i helu są takie same. W sciance pojemnika zrobiono bardzo mały otwór. Jaki będzie skład wiązki gazu uchodzącego z pojemnika tuż po wykonaniu otworu? W jednostkach masy atomowej masy atomowe wynoszą: helu $\mu_{\mathrm{He}} = 4$, a neonu $\mu_{\mathrm{Ne}} = 20$.

Rozwiązania na str. 24