Informatyka kwantowa – jak to działa?

Robert von Oliva

naruciakk

2019-09-14

Informatyka kwantowa

1. Klasyczna informatyka – bit
   $(b = 0 \vee b = 1)$
2. Kwantowa informatyka – kubit
   $(|q\rangle = |0\rangle \vee |q\rangle = |1\rangle)$

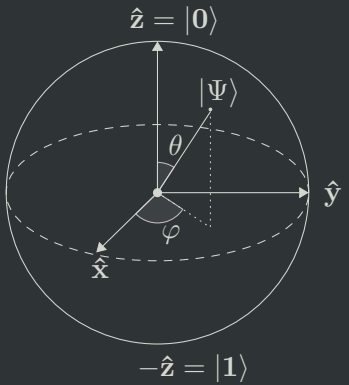

Figure: Glosser.ca, Wikicommons, CC BY-SA 3.0

Superpozycja

Obiekt znajduje się w dwóch stanach jednocześnie

$$|\rho\rangle = c_0 |0\rangle + c_1 |1\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

gdzie $c_0, c_1 \in \mathbb{C}$ oraz ${c_0}^2 + {c_1}^2 = 1$. Stany kwantowe mogą być dodawane i na ich podstawie tworzone nowe stany kwantowe, podczas pomiaru dostajemy 0 albo 1.

Splątanie

Układ jest lepiej opisany niż jego części składowe

$$|\rho\rangle_{12} = c_{00}\,|0\rangle_1|0\rangle_2 + c_{01}\,|0\rangle_1|1\rangle_2 + c_{10}\,|1\rangle_1|0\rangle_2 + c_{11}\,|1\rangle_1|1\rangle_2$$

dla porównania

$$|\psi\rangle_1 \otimes |\phi\rangle_2 = (a|0\rangle_1 + b|1\rangle_1) \otimes (c|0\rangle_2 + d|1\rangle_2)$$

,

$$|\psi\rangle_1 \otimes |\phi\rangle_2 = ac\,|0\rangle_1|0\rangle_2 + ad\,|0\rangle_1|1\rangle_2 + bc\,|1\rangle_1|0\rangle_2 + bd\,|1\rangle_1|1\rangle_2$$

nie jest równe pierwszemu! Dodatkowo ${c_{00}}^2 + {c_{01}}^2 + {c_{10}}^2 + {c_{11}}^2 = 1$. Nie jesteśmy w stanie opisać układu cząstek przy pomocy stanów jego cząstek składowych

Historia dziedziny I

1. Lata 1960, Stephen Wiesner, *Conjugate Coding*, kodowanie kwantowe, kwantowe banknoty
2. 1973, *Holevo's theorem*
3. 1981, Richard Feynman: *nie da się zasymulować wydajnie układu kwantowego na komputerach klasycznych*
4. 1981, Tommaso Toffoli: bramka Toffoli (CCNOT)
5. 1985, David Deutsch: uniwersalny komputer kwantowy (*kwantowa maszyna Turinga*)

Historia dziedziny II

6. 1992, algorytm Deutsch-Jozsa, pierwszy przykład wyższości komputerów kwantowych
7. 1994, Peter Shor: **szybka faktoryzacja**
8. 1995, pierwsza fizyczna realizacja bramki kwantowej (CNOT)
9. 1998, pierwsze wykonanie algorytmu kwantowego (komputer dwukubitowy, algorytm Deutsch-Jozsa)
10. 2001, pierwsze uruchomienie algorytmu Shora (faktoryzowana liczba: 15)

Historia dziedziny III

11. 2005, pierwsza realizacja kwantowego bajtu
12. 2014, pierwsza udana i bezbłędna teleportacja kwantowa na odległość ok. 3 metrów
13. 2016, IBM udostępnia platformę internetową pozwalającą na dokonywanie obliczeń na ich maszynach kwantowych
14. 2016, symulacja molekuły wodoru na 9 kubitach (Google)
15. 2019, IBM Q System One, pierwszy komercyjny komputer kwantowy (20 kubitów)

„Moc operacyjna” komputerów kwantowych

1. 1998, 2 kubity (NMR), 3 kubity | MIT
2. 2000, 5 kubitów | TU München, 7 kubitów | Los Alamos
3. 2006, 12 kubitów | Waterloo, MIT
4. 2007, 28 kubitów | D-Wave Systems (Quantum annealing)
5. 2008, 128 kubitów | D-Wave Systems
6. 2012, 84 kubitowe obliczenia | D-Wave Systems
7. 2017, 2000 kubitów | D-Wave Systems (XD)
8. 2017, 17 kubitów | IBM, 17 kubitów | Intel, 50 kubitów | IBM
9. 2018, 72 kubity | Google, 49 kubitów | Intel

Jak zrobić kubita?

1. Nuclear magnetic resonance
2. Kropka kwantowa (spin elektronów, pozycja elektronów)
3. Uwięzione jony
4. Superconducting quantum computing

Figure: MartinSaunders, Wikicommons, public domain

Jak zrobić kubita? – Kropka kwantowa

1. Kubit oparty o spin elektronów
2. Kropka kwantowa – mały (rzędu nanometrów) półprzewodnik
3. Niska dekoherencja, skalowalność, wysoka dokładność

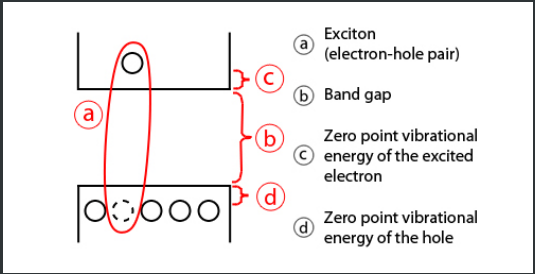

Figure: Jpailee, Wikicommons, CC BY-SA 3.0

Jak zrobić kubita? – Nuclear magnetic resonance

1. Kubit oparty o spin nukleonów
2. Aby zbadać spin używamy techniki spektroskopii NMR
3. Aby operować na kubicie – elektromagnetyczne impulsy
4. Niskie SNR przy większej liczbie
5. Czy to jest komputer kwantowy?

Figure: Mike25, Wikicommons, public domain

Jak zrobić kubita? – Uwięzione jony

1. Kubit oparty o uwięzione w polu elektromagnetycznym jony (duh)
2. Dwa poziomy struktury nadsubtelnej lub stan podstawowy/wzbudzony
3. Rekord: 20 jonów uwięzionych w strukturze
4. Operacje wykonywane przy użyciu laserów
5. Dobre, ale trudne w budowie

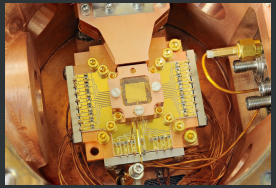

Figure: usnistgov, public domain

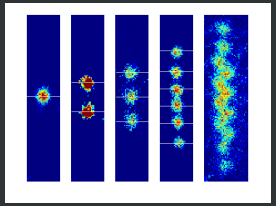

Figure: usnistgov, public domain

Jak zrobić kubita? – Superconducting quantum computing

1. Kubit jest implementowany przy użyciu nadprzewodzących układów elektronicznych
2. Jedna z najpopularniejszych realizacji: Intel, IBM, Google, D-Wave
3. Obwód zachowuje się jak atom posiadający dwa poziomy energetyczne

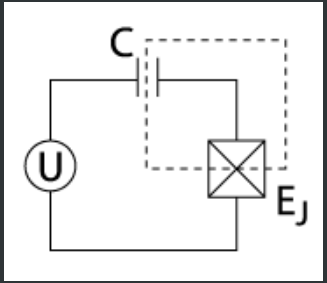

Figure: Bjohnson00, Wikicommons, CC BY-SA 3.0

Trudności w realizacji – Kryteria DiVincenzo

1. Skalowalny system z dobrze określonym kubitem
2. Możliwość zainicjowania stanu kubitu
3. Długie czasy dekoherencji
4. Zbiór uniwersalnych bramek kwantowych
5. Możliwość wykonania pomiaru
6. Możliwość konwersji kubitów na takie, które da się przesłać
7. Możliwość wiarygodnej transmisji kubitów

Problemy

W przypadku informatyki kwantowej istnieją pewne obostrzenia w konstruowaniu rozwiązań, biorące się bezpośrednio z ograniczeń wynikających z mechaniki kwantowej:

1. Odwracalność – operacje kwantowe są odwracalne, wszelkie bramki dają możliwość powrotu do informacji zawartej na wejściu.
2. Zakaz klonowania – nie ma możliwości idealnego skopiowania stanu kwantowego. Można skopiować go częściowo, ale nie całkowicie.
3. Zakaz usuwania – nie ma możliwości usunięcia jednej z dwóch kopii nieznanego stanu kwantowego, dopełnia zakaz klonowania.

Pomiar kubitu

Nieodwracalna operacja w której uzyskujemy operację o kubicie. Rezultatem takiego pomiaru będzie jeden z dwóch stanów ($|0\rangle$ albo $|1\rangle$), odpowiednio z prawdopodobieństwem $|\alpha|^2$ lub $|\beta|^2$.

$$P_0 = |0\rangle \langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$P_1 = |1\rangle \langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Fajne zastosowanie – Symulacje procesów kwantowych

Symulowanie pewnych zjawisk fizycznych związanych z mechaniką kwantową na komputerze klasycznym jest trudne.
Można więc wykorzystać układy fizyczne, które jesteśmy w stanie kontrolować (np. komputery kwantowe) do symulacji pewnych cięższych do kontrolowania zjawisk, np. zjawisk fizyki molekularnej.

Fajne zastosowanie – Kryptografia

1. Algorytm Shora – ukrócenie działania (niektórych) klasycznych algorytmów klucza publicznego (np. RSA).
2. Kryptografia kwantowa – metody niezależne od urządzenia (Device Independent i Semidevice Independent), kwantowa dystrybucja klucza itp.
3. Kwantowa wymiana klucza (QKD) – do klasycznej komunikacji potrzebujemy klucza, który można ustalić przy użyciu technik kwantowych.

Fajne zastosowanie – Realizacja problemów obliczeniowych

1. Faktoryzacja dużych liczb – Algorytm Shora (klasycznie: subwykładniczy, kwantowo: logarytmiczny)
2. Przeszukiwanie losowych zbiorów – Algorytm Grovera (klasycznie: liniowy, kwantowo: $O(\sqrt{n})$)
3. Rozwiązywanie układów równań liniowych – algorytm HHL (klasycznie: *sort of* liniowy, kwantowo: *sort of* logarytmiczny)

Algorytm Shora – OwO what's this

Weźmy pewną liczbę naturalną N. Celem jest znalezienie dzielnika tej liczby (w praktyce rozkład na czynniki pierwsze iloczynu dwóch dużych liczb pierwszych)

Klasycznie: nie ma algorytmów klasy P, najmniej $O(e^{\sqrt[3]{\frac{64}{9}b(\log b)^2}})$.

Algorytm Shora – Jak on działa – Część klasyczna

1. Wybierz losowy numer $a < N$.
2. Oblicz najwyższy wspólny dzielnik liczb a i N.
3. Jeżeli najwyższy wspólny dzielnik tych obu liczb jest różny od 1 to a jest odpowiedzią.
4. W innym wypadku, korzystając z algorytmu kwantowego, należy znaleźć okres funkcji $f(x) = a^x \mod n$

Algorytm Shora – Jak on działa – Część kwantowa

Działanie algorytmu opiera się na tym samym co algorytm Grovera – zwiększamy amplitudę na pożądanej odpowiedzi, jednocześnie zmniejszając na reszcie. Pierwszym krokiem jest utworzenie dwóch kwantowych rejestrów i nadanie superpozycji kubitom w tych rejestrach (bramki Hadamarda)

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle = \left(|x_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(|x_q\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

Algorytm Shora – Jak on działa – Część kwantowa

Aplikujemy funkcję $f(x) = a^x \mod n$ do otrzymanego stanu przy użyciu odpowiedniego układu kwantowego, uzyskując

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle.$$

Algorytm Shora – Jak on działa – Część kwantowa

Używamy odwróconej kwantowej transformaty Fouriera. Przekształca ona każdy możliwy do uzyskania stan w taki sposób, że wygasza się on z innymi stanami o takim samym okresie, powodując, że stan zzawierający potrzebny nam okres funkcjima bardzo wysoką amplitudę.
Następnie możemy dokonać pomiaru i uzyskać okres funkcji.

1. Jeżeli odnaleziony okres jest nieparzysty zaczynamy procedurę od nowa
2. Jeżeli $a^{r/2} \pm 1 = 0 \mod n$ zaczynamy procedurę od nowa
3. Poszukiwanym dzielnikiem jest $NWD(a^{r/2}+1, N)$ lub $NWD(a^{r/2}-1, N)$.

Literatura i dodatkowe czytanie

1. An Introduction to Quantum Algorithm, Emma Strubell, 2011, dostęp 2019-09-14
2. Learn Quantum Computing with the Quantum Katas, Mariia Mykhailova, 2018, dostęp 2019-09-14
3. Wstęp do informatyki kwantowej, Michel Le Bellac, Wydawnictwo Naukowe PWN, Warszawa 2011, ISBN 9788301165703
4. Fundamentals of Quantum Information Theory, Michael Keyl, 2002, dostęp 2019-09-14
5. Quantum Country, ciekawy zbiór artykułów z gatunku *jak to działa*, dostęp 2019-09-14
6. Wstęp do informatyki i kryptografii kwantowej, Oficyna Wydawnicza Politechniki Wrocławskiej, dostęp 2019-09-14