Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie

Ewolucja sieci
Techniki kwantowe w teleinformatyce

Piotr Chołda

Instytut Telekomunikacji

16 kwietnia 2024 r.

Plan wykładu

1. Komputery kwantowe
2. Algorytmy kwantowe: wstęp
3. Kwantowe uczenie maszynowe
4. Komunikacja kwantowa: wstęp
5. Obliczenia kwantowe
6. Algorytmy kwantowe: przykład
7. Komunikacja kwantowa: bardziej zaawansowane zagadnienia

Wprowadzenie do wykładu

O CZYM?

Wprowadzenie do wykładu

PO CO?

ZACZYNAMY!

Plan wykładu

Komputer kwantowy

Sprzęt: działalność raczej dla fizyków niż inżynierów

Liderzy: IBM, Google, IonQ, Intel; USTC, Alibaba (Chiny); D-Wave Systems, Xanadu (Kanada) ...

Szybkie zmiany: teraz 133 kubitów (rok temu 127 kubitów) w komputerze ogólnego przeznaczenia (IBM). Ale różne firmy robią różne produkty i różnie to jest liczone (wygląda że obecnie najwięcej to prawie 400 kubitów): ranking ze stycznie 2024 r.

Rysunek: 50-kubitowy komputer IBMa

QC

***Quantum computing*, obliczenia kwantowe**

Przewaga obliczeń kwantowych nad tradycyjnymi:

- **Zrównoleglenie kwantowe**: dzięki użyciu koncepcji superpozycji stanów kwantowych — komputer kwantowy może wykonywać algorytm na wszystkich możliwych wejściach na raz.
- **Wymiar kwantowej przestrzeni Hilberta**: „wymiar" przestrzeni stanów w układzie kwantowym jest wykładniczy w stosunku do odpowiedniego systemu klasycznego.
- **Splątanie**: różne podsystemy (np. kubity) w komputerze mogą być splątane, co wprowadza nieklasyczne korelacje między nimi. Właściwość jest szczególnie przydatna w przypadku transmisji (teleportacja).

Komputer kwantowy

Zalety

Zalety ale nie cuda!

- Komputer kwantowy umożliwia równoczesne operowanie na stanach reprezentujących system (przyspieszenie!).
- Model obliczeń jest nadal zgodny z tezą Turinga–Churcha (równoważność z maszyną Turinga).
- Problemy rozwiązywalne efektywnie przez komputer kwantowy są zaliczane do klasy $\mathcal{BQP}$ (*bounded-error quantum polynomial time*, klasa problemów rozwiązywalnych przez komputer kwantowy w czasie wielomianowym, przy prawdopodobieństwie $< \frac{1}{3}$ że odpowiedź jest błędna w pojedynczym przebiegu): $\mathcal{P} \subseteq \mathcal{BQP} \subseteq \mathcal{NP}$.
- Jeśli coś jest problemem $\mathcal{NP}$-trudnym, to dalej może być kłopotliwe obliczeniowo.

Komputer kwantowy

Zalety

Zalety ale nie cuda (cd.)! A właściwie nawet trochę wady ☺

- Sposób działania jest probabilistyczny: obliczenie kwantowe zwraca losowo tylko jeden stan (z całej superpozycji stanów). Dlatego obliczenia typowo wykonuje się wiele razy (jak w przypadku klasycznych algorytmów probabilistycznych).
- Komputer kwantowy nie ma zastąpić komputera klasycznego, np. trzeba na niego opracować zupełnie nowe algorytmy (a nie po prostu zrekompilować istniejące, żeby działały szybciej ☺).
- Zapewne najbardziej popularny „sukces" komputera kwantowego to faktoryzacja całkowitoliczbowa (na podstawie algorytmu Shora), ale nie ma dowodu, że ten problem jest $\mathcal{NP}$-zupełny.

Komputer kwantowy

Jak fizycznie działa komputer kwantowy?

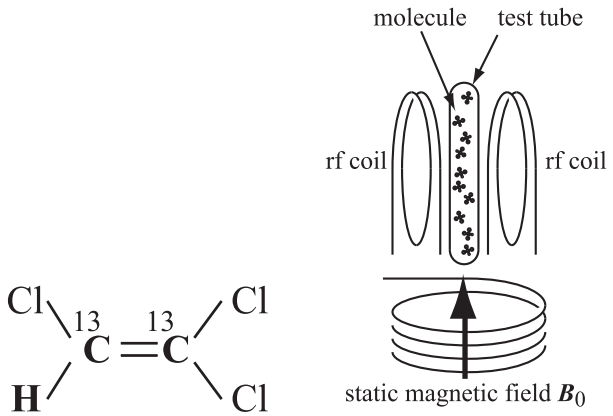
- Jądrowy rezonans magnetyczny...
- Pułapki jonowe...
- Kropki kwantowe...
- Układy nadprzewodzące...

Poza możliwością manipulowania poszczególnymi stanami — ważne jest także, aby można było zaimplementować tzw. bramki kwantowe (w celu manipulowania kubitami).

Kubity

Realizacja fizyczna

Jądrowy rezonans magnetyczny NMR (ang. *nuclear magnetic resonance*): stany są związane ze spinami cząsteczek, a ich zmiany osiąga się przez aplikację częstotliwości radiowej będącej w rezonansie z częstotliwością spinu.



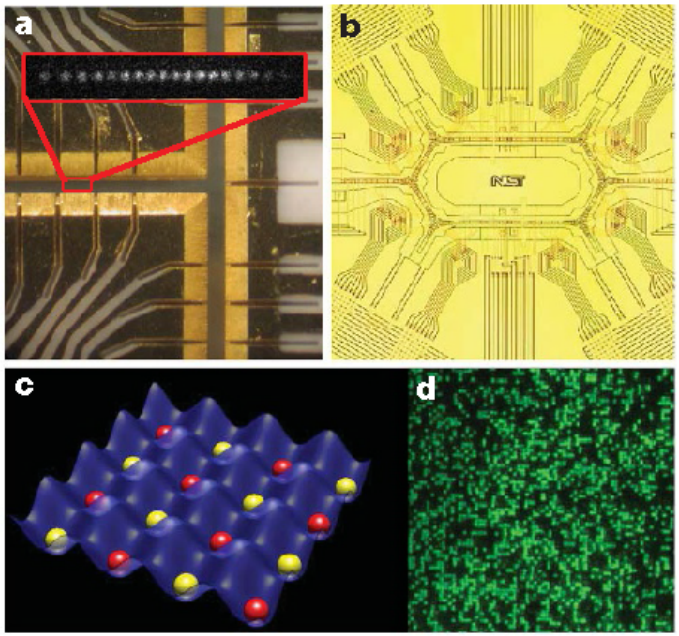
Rysunek: Trichloroetylen. Wszystko w ciekłym helu!

Chłodzenie praktycznie do 0 K.

Kubity

Realizacja fizyczna

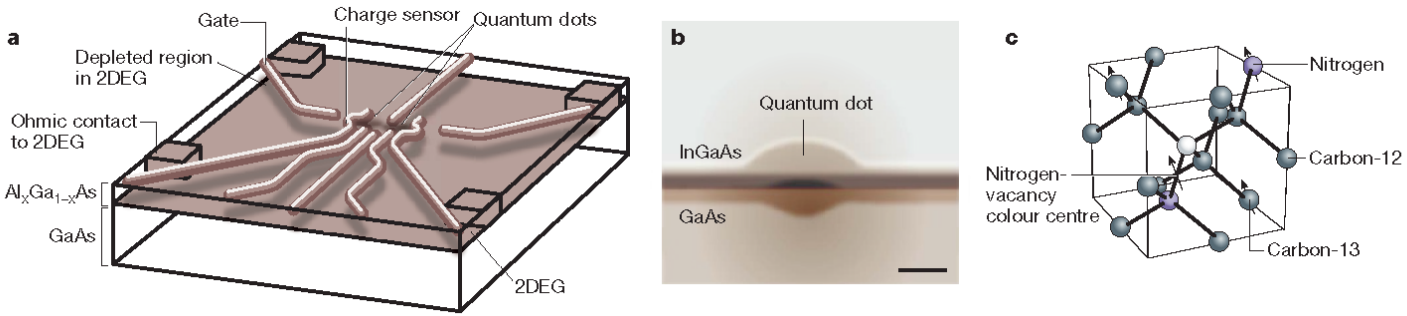
Pułapki jonowe (*cold confined atomic ions*): zmrożone prawie do 0 K atomy / jony — stan kubitu jest związany z określonym poziomem energetycznym (zmiana stanu: pompowanie energii wiązką laserową).



Kubity

Realizacja fizyczna

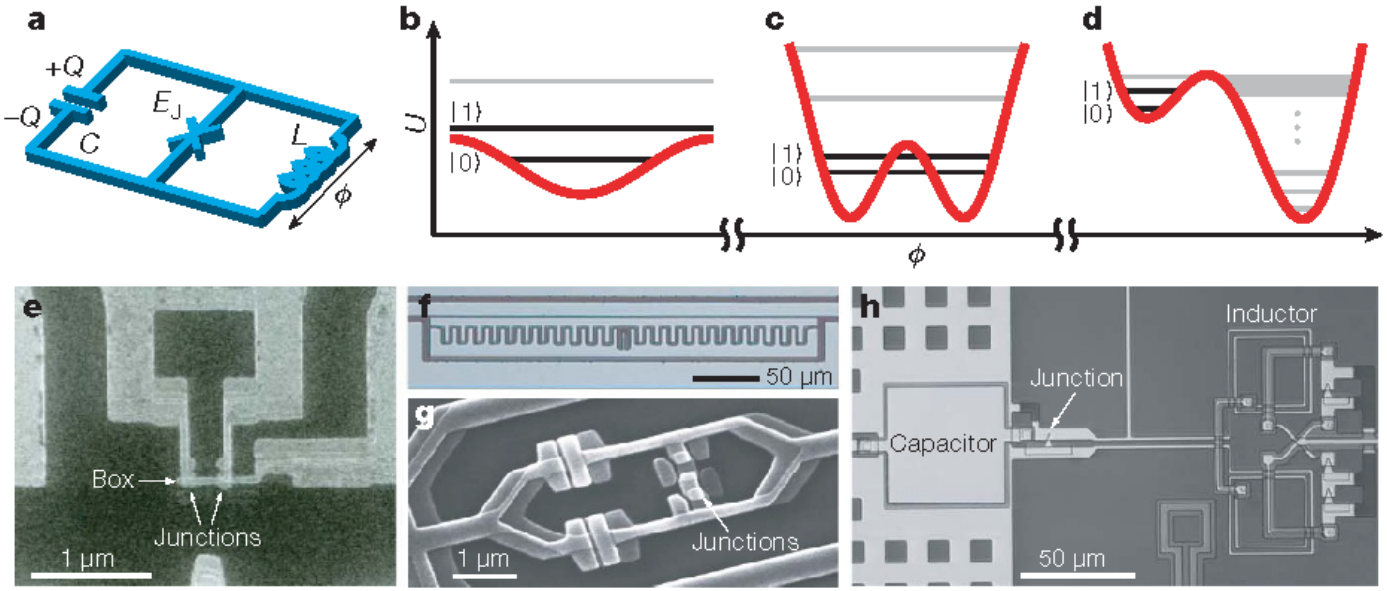
Kropki kwantowe (*quantum dots*): nano-kryształy (rozmiary $\sim 10^{-9}$ m), możliwość reprezentacji stanu albo jako specyficznej energii albo spolaryzowania elektronu uwięzionego w pewnej strukturze półprzewodnikowej.



Kubity

Realizacja fizyczna

Układy nadprzewodzące (*superconductors*): kubity są zapisane za pomocą odmiennych poziomów energii w układach nadprzewodzących (np. złączu Josephsona).



Kryteria DiVincenzo (2000)

Dlaczego tak wolno nam idzie z tym rozwojem tej dziedziny?

- Istnienie skalowalnego systemu z dobrze scharakteryzowanymi kubitami.
- Możliwość inicjalizacji kubitów w rejestrze kwantowym, np. $|00\ldots0\rangle$ („reset" komputera).
- Wystarczająco długi czas koherencji (utrzymanie reżimu kwantowego, tj. czasu życia czyli utrzymania stanu superpozycji). **Kluczowy problem**. W praktyce możemy utrzymać reżim przez ok. milion operacji bramek (np. do praktycznej **faktoryzacji 21** potrzeba było setek tysięcy operacji).
- Istnienie uniwersalnego zestawu bramek kwantowych.
- Możliwość pomiaru stanu kubitów. Problematyczna ze względu na szybką dekoherencję oraz błędy w działaniu bramek kwantowych.

Plan wykładu

Algorytmy kwantowe

Najbardziej znane

- Algorytm Deutscha-Jozsa'y (sprawdza, czy funkcja jest zbalansowana).
- Algorytm przeszukiwania rejestru (Grover). Poszukuje takiej wartości x, że $f(x) = 1$ (poprawa złożoności: z liniowej na pierwiastkową).
- Algorytm znajdowania okresu w funkcjach okresowych (Simon), zaś dla funkcji modulo: Shor, 1994 (od tego czasu zaczęto uważniej przyglądać się koncepcji komputerów kwantowych, wcześniej traktowano je jako ciekawostkę fizyków).

Quantum Algorithm Zoo

Faktoryzacja

Względne bezpieczeństwo kryptosystemu RSA

RSA opiera się na trudności rozkładu na liczby pierwsze (faktoryzacji) modułu systemu — liczby półpierwszej: $N = p \times q$.

- Złożoność najlepszego algorytmu klasycznego: $\mathcal{O}\left(e^{\sqrt[3]{\frac{64}{9} N \log^2 N}}\right)$.
- Złożoność algorytmu kwantowego:
  - Złożoność czasowa: $\mathcal{O}\left(N^3 \log N\right)$.
  - Złożoność „przestrzenna": liczba kubitów: $\mathcal{O}\left(\log N\right) +$ liczba bramek: $\mathcal{O}\left(N^2 \log N \log\log N\right)$.
- 2001: faktoryzacja **15**; 2011: faktoryzacja **21** (rejest 7-kubitowy); 2019: porażka przy **faktoryzacji 35** ☺
- Lepiej radzimy sobie z faktoryzacją z użyciem podejścia optymalizacyjnego (np. za pomocą **kwantowego wyżarzania**): udaje się sfaktoryzować wartości liczb reprezentowanych na kilkuset bitach (względnie nieproblematyczne dla komputera klasycznego).

Algorytm Shora

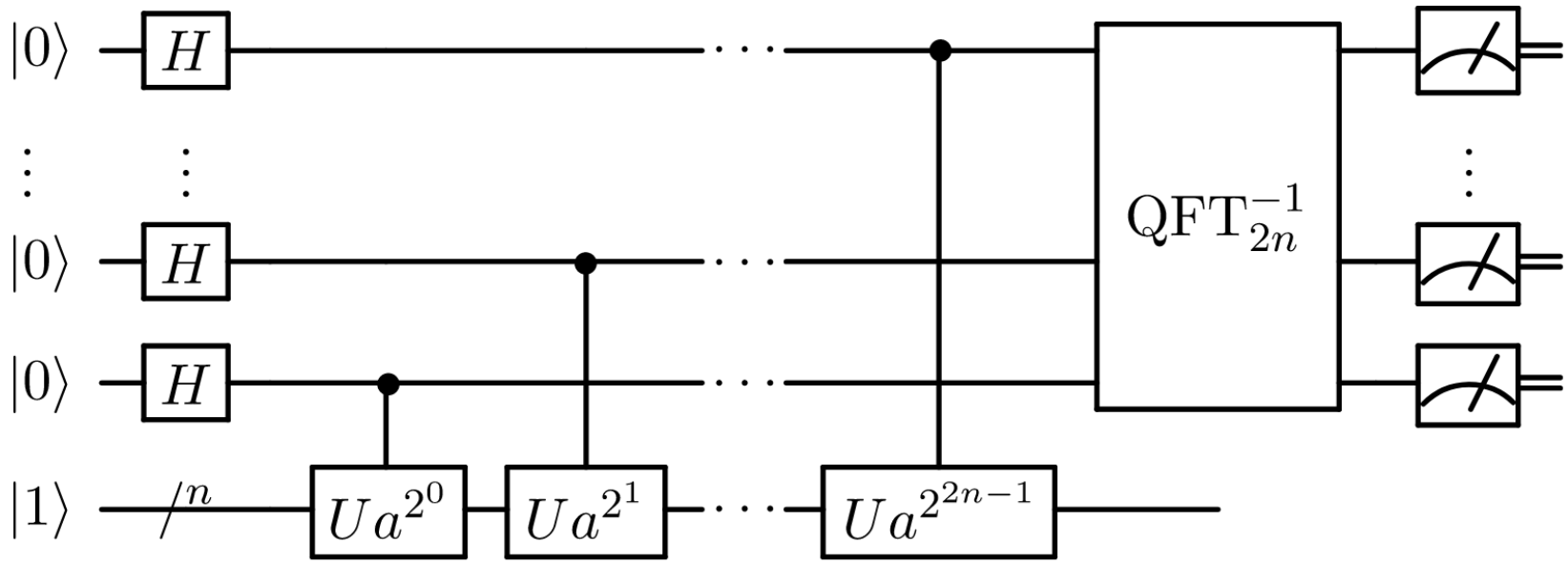
Zupełnie inna logika działania niż dla algorytmu na klasyczny komputer (chociaż wyników używa się potem klasycznie):

- „Kwantowy algorytm faktoryzacji całkowitoliczbowej".
- Ale tak naprawdę to jest algorytm znajdujący **okres pewnej funkcji modulo**. Na tej podstawie można dokonać (w sposób klasyczny) faktoryzacji.
- Okresowość funkcji da się modelować fazą pewnej wartości własnej. Znalezienie odpowiedniej fazy mówi nam coś o okresie.
- Używamy **kwantowej transformaty Fouriera**, która pozwala nam znaleźć okres. We współczesnych aplikacjach teleinformatyki coraz częściej wraca sygnałówka! ☺
- Występują piki amplitud, które są powiązane z okresem — możemy je statystycznie wykryć (algorytm probabilistyczny).

Algorytm Shora

Część kwantowa: poszukiwanie okresu

To jest algorytm na komputer kwantowy ☺



W sumie klasyczny algorytm też da się utożsamić z dużym układem bramek (innych!), ale o tym zwykle nie pamiętamy...

Co potem?

Praktyczne działanie algorytmu Shora = koniec współczesnej kryptografii asymetrycznej!

Post–kwantowe algorytmy szyfrowania (kryptografia post–kwantowa) — podstawowe pomysły:

- Kryptografia oparta na kodach korekcyjnych (system McEliece'a, 1978).
- Kryptografia oparta na kratach (problemy SIS, LWE, CVP; 1996).
- Kryptografia oparta na funkcjach skrótu (jednokrotny podpis Winternitza, 1979).
- Kryptografia oparta na specyficznych (izogenicznych) krzywych eliptycznych (SIDH, 2011). Nie mylić z klasycznym podejściem ECDH!
- Kryptografia wielu zmiennych z układami równań wielomianowych (problem MQ, 1988).

Algorytmy kryptografii post-kwantowej to **algorytmy klasyczne** ☺

Plan wykładu

QML

***Quantum machine learning*, kwantowe uczenie maszynowe**

Dwie opcje:

- Użycie komputerów kwantowych do poprawy szybkości obliczeń z użyciem uczenia maszynowego (w niektórych przypadkach — np. kwantowego wyżarzania, *quantum annealing* — używa się jeszcze jednego fenomenu specyficznego dla mechaniki kwantowej — tunelowania).
- Użycie klasycznych metod uczenia maszynowego w celu poprawy obliczeń związanych z pomiarami kwantowymi (np. uczenie ze wzmocnieniem — agenci kwantowi korzystają z algorytmu Grovera).

W przypadku pierwszego podejścia korzystamy z faktu, że niektóre algorytmy kwantowe działają szybciej niż algorytmy klasyczne.

Przykład

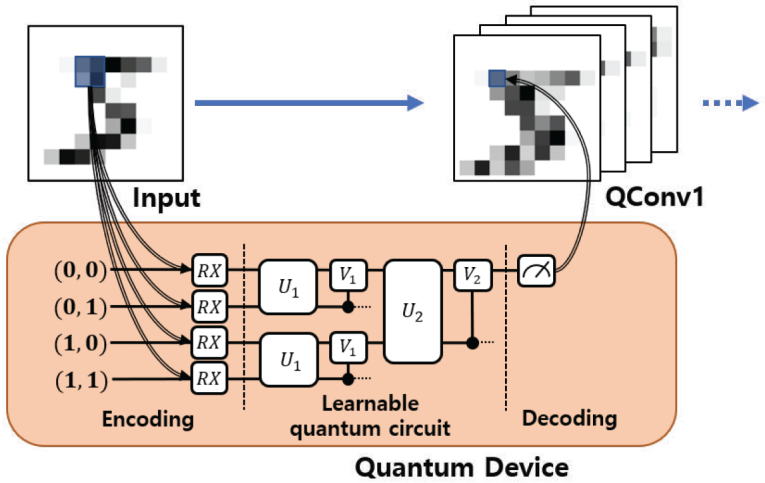
Kwantowa analiza głównych składowych QPCA (*quantum principal component analysis*)

- Klasyczny algorytm: $\mathcal{O}(d^2)$ — redukujemy przestrzeń d-wymiarową cech, gdzie $d = 2^n$.
- Algorytm kwantowy: $\mathcal{O}((\log d)^2)$ — przyspieszenie wykładnicze.
- Podstawa przyspieszenia: kwantowy algorytm rozkładu spektralnego (tj. na wektory i wartości własne).

Przykład

Kwantowe splotowe sieci neuronowe

- Klasyczny algortym: $\mathcal{O}(n^2)$ — dla filtru o rozmiarze n^2.
- Algorytm kwantowy: $\mathcal{O}(\log n)$ — przyspieszenie wykładnicze (dzięki zrównolegleniu obliczeń na pikselach).
- Podstawa przyspieszenia: elementy kwantowe dotyczą splotu (filtru).



Plan wykładu

QComm

***Quantum communications*, komunikacja kwantowa**

- Kanał kwantowy i różne opcje transmitowania danych.
- Kwantowe kody transmisyjne i korekcja błędów.

Potrzeba korekcji błędów

Stany kwantowe są bardzo niestabilne, dlatego należy wprowadzić korektę błędów:

- Nie **tylko w transmisji**! Czasem o tym zapominamy, ale przy przechowywaniu danych lub ich przetwarzaniu też trzeba korygować przekłamania — po prostu w układach klasycznych do przechowywania danych w praktyce nie występuje ten problem.
- Szacuje się, że komputery kwantowe mogą efektywnie działać jeśli występuje do **jednego błędu na miliard bramek**.
  Jakiemu poziomowi BER to by odpowiadało? ☺
- Obecnie w najlepszym przypadku mamy jeden błąd na tysiąc bramek.
- 1995: Shor i Steane — metoda kwantowej korekcji błędów.

Korekcja przekłamań

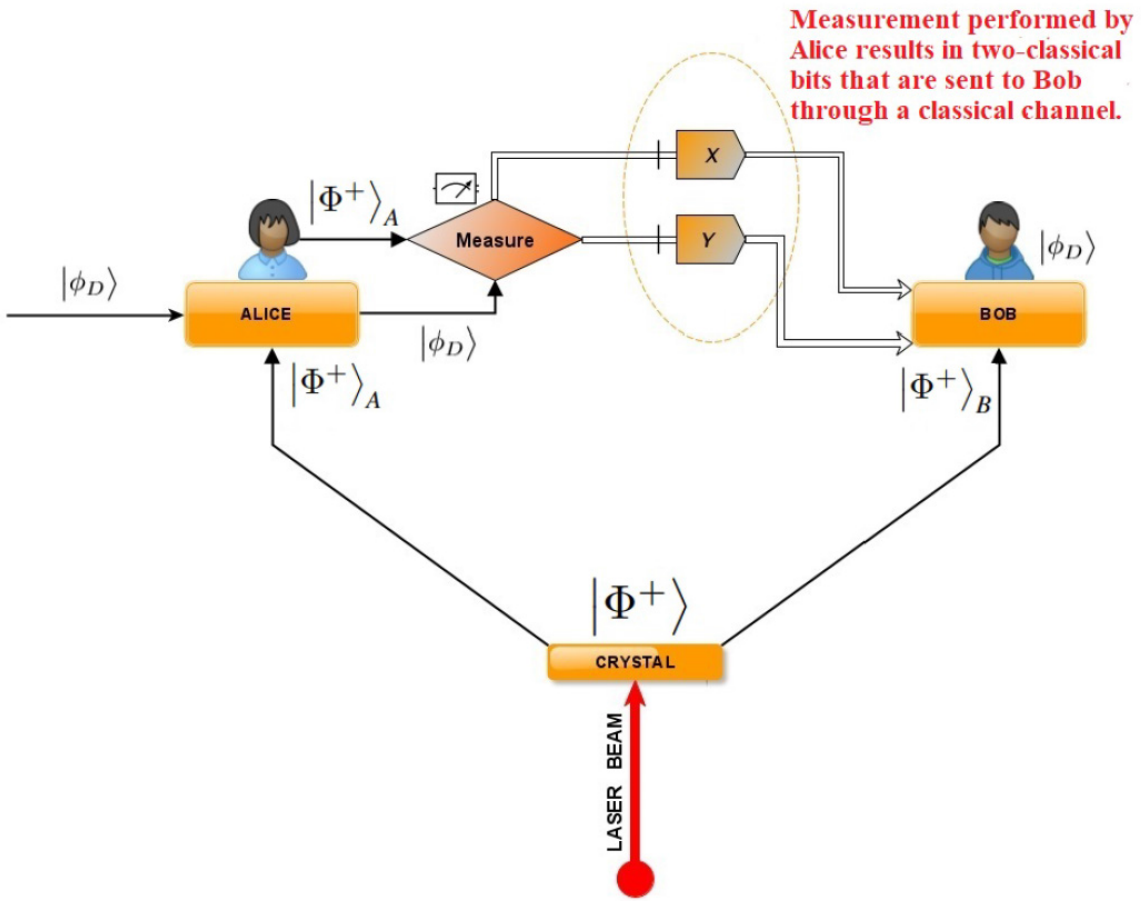
Idea ogólna

- Podobnie jak w przypadku klasycznym opracowujemy kody korekcyjne.
- Kubity informacyjne, kubity nadmiarowe oraz kubity pomocnicze (*ancilla qubits*).
- Nie można mierzyć wprost kubitów informacyjnych, żeby stwierdzić czy zostały przekłamane (zakaz klonowania!). Kubity pomocnicze są nam potrzebne do stwierdzenia, czy wystąpiło przekłamanie — same jednak ulegają kolapsowi.

W części dodatkowej: przykład najprostszego kodu korekcyjnego — trzykubitowy kod chroniący przed odwracaniem (*three-qubit bit-flip code*).

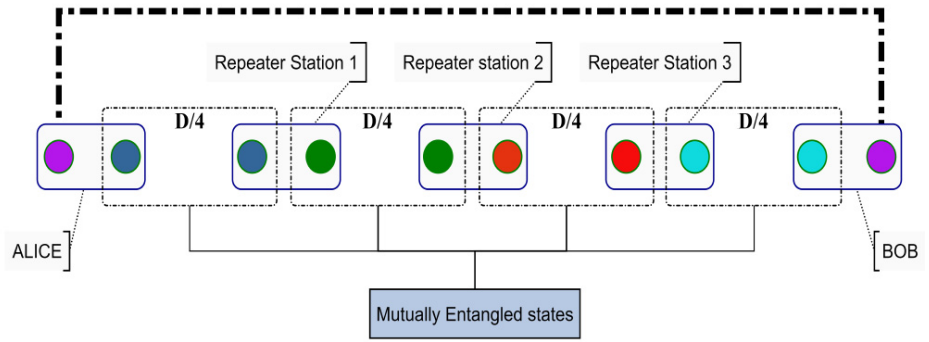
QComm

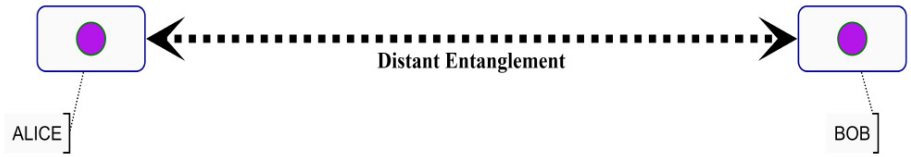
Teleportacja kwantowa



QComm

Kwantowe repeatery („regeneratory”?) używane w celu przekazu splątania





Ze względu na zakaz klonowania nie można wzmacniać poziomu kubitu (więc trudno mówić o regeneracji).

PODSUMOWANIE

Plan wykładu

Fizyka kwantowa

Podstawowe pojęcia z punktu widzenia konstrukcji komputera kwantowego i odpowiednich algorytmów

- Równanie Schrödingera: $\widehat{H}\,|\psi\rangle = i\hbar\frac{\partial}{\partial t}\,|\psi\rangle$.
- Dualizm korpuskularno-falowy. **Doświadczenie ze szczelinami** — pokazujące interferencję pojedynczego elektronu z samym sobą. Mamy rozmycie, np. nie można wprost powiedzieć, że elektron jest w konkretnym miejscu — dopóki nie dokonamy pomiaru. W trakcie pomiaru elektron „decyduje”, gdzie się znajdzie (interferencja zanika).
- Superpozycja kwantowa: dwa stany kwantowe mogą zostać połączone z użyciem superpozycji, tworząc inny stan kwantowy. Dzięki superpozycji możemy teoretycznie dysponować dużo większą mocą obliczeniową.

Cztery postulaty

Ogólne ramy każdej teorii związanej z mechaniką kwantową

- Stany kwantowe opisujemy za pomocą wektorów stanu.
- Dynamika stanów jest opisywana za pomocą ewolucji unitarnej.
- Natura pomiaru polega na rzutowaniu na pewien wektor bazowy.
- Stany systemu złożonego są opisywane z użyciem iloczynu tensorowego.

Postulat 1

Z każdym systemem kwantowym jest związana pewna zespolona przestrzeń wektorowa (tzw. **przestrzeń stanów**, *state space*).

Zamknięty system kwantowy jest reprezentowany przez wektor jednostkowy w przestrzeni stanów (to tzw. przestrzeń Hilberta).

Notacja BRA-KET

Wprowadzona przez Paula Diraca

Notacja Diraca służy do reprezentowania stanów kwantowych.

Ket (wektor kolumnowy):

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Typowo używamy reprezentacji ogólnej $|\psi\rangle$ w bazach ortonormalnych:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2$$

Notacja BRA-KET

Wprowadzona przez Paula Diraca

Bra (wektor wierszowy):

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

Jeśli $|\psi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix}$, to $\langle \psi| = \begin{bmatrix} \psi_1^* & \psi_2^* \end{bmatrix}$.

Sprzężenie zespolone: $(a + bi)^* = a - bi$

Iloczyn skalarny: $\langle \psi|\phi\rangle = \begin{bmatrix} \psi_1^* & \psi_2^* \end{bmatrix} \begin{bmatrix} \phi_1 \\ \phi_2 \end{bmatrix} = \psi_1^*\phi_1 + \psi_2^*\phi_2 \in \mathbb{C}$

Kubit (bit kwantowy)

Po angielsku: *qubit*

- Kubit reprezentuje, **podobnie jak w przypadku klasycznym**, informację dwustanową.
- W **przeciwieństwie** do klasycznego bitu, kubit może być w dwóch stanach na raz. W chwili obserwacji/pomiaru następuje „kolaps" do jednego z dwóch stanów.
- Pomiar rzutuje stan kwantowy na jeden z wektorów bazowych z prawdopodobieństwem będącym kwadratem modułu odpowiedniej amplitudy.

Kubit jest reprezentowany przez dwuwymiarowy wektor uzyskiwany jako liniowa kombinacja stanów bazowych (superpozycja):

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

Kubit (bit kwantowy)

Po angielsku: *qubit*

Interpretacja fizyczna:

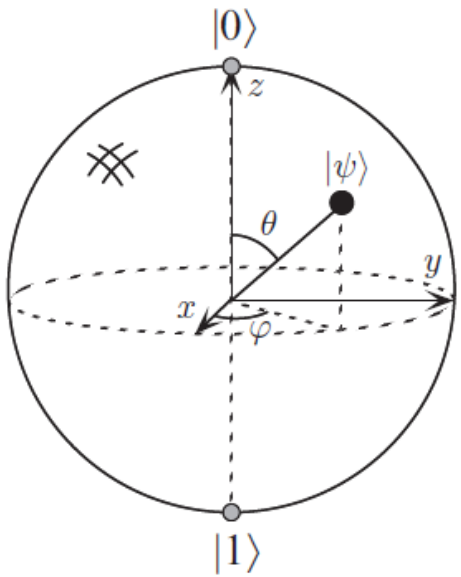
- np. $|0\rangle$: spin górny,
- np. $|1\rangle$: spin dolny,
- $\alpha, \beta \in \mathbb{C}$: amplituda,
- $|\alpha|^2 + |\beta|^2 = 1$,
- $|\alpha| = \sqrt{\alpha\alpha^*}$: moduł liczby zespolonej (dla liczby rzeczywistej: wartość bezwzględna).

Podczas pomiaru:

- z prawdopodobieństwem $|\alpha|^2$ obserwujemy stan bazowy $|0\rangle$,
- zaś z prawdopodobieństwem $|\beta|^2$ — stan $|1\rangle$.

Bity kwantowe (kubity)

Kubity są reprezentowane w tzw. sferze Blocha (zespolonej):



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \alpha = \cos\left(\frac{\theta}{2}\right) \quad \beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$$

Postulat 2

Ewolucja zamkniętego systemu kwantowego jest opisywana za pomocą **transformacji unitarnych**:

$$\left|\psi'\right\rangle = U\left|\psi\right\rangle$$

- Operatory kwantowe są reprezentowane w postaci kwadratowych macierzy unitarnych (utożsamianych z bramkami kwantowymi).
- Rozmiar macierzy musi być taki sam jak wektora reprezentującego stan, na którym zachodzi operacja, a wynik musi być znormalizowany.

Bramka kwantowa NOT Gate

Tzw. bramka X Pauliego, σ_x lub σ_1

Ekwiwalent klasycznej bramki NOT.

Odwzorowuje $|0\rangle \to |1\rangle$ oraz $|1\rangle \to |0\rangle$, czyli:

$$\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \beta\,|0\rangle + \alpha\,|1\rangle$$

Reprezentacja macierzowa:

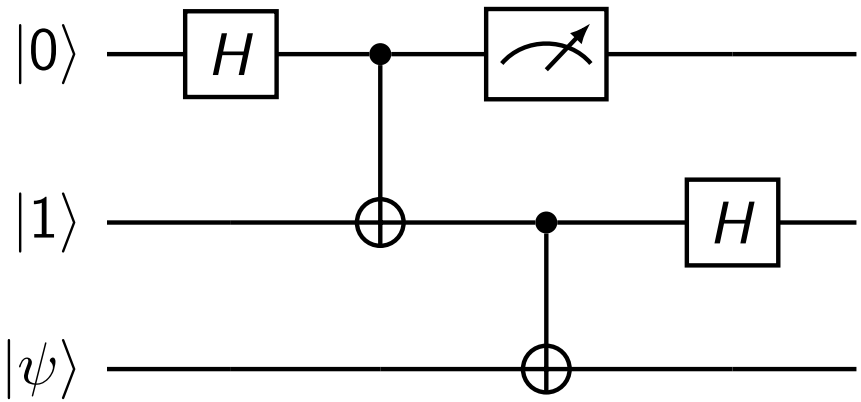
$$\boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Sprawdźmy $\boldsymbol{X}\,|\psi\rangle\ldots$

Bramki kwantowe

Klasyczne obliczenia na bitach mogą być wykonywane z użyciem **bramek logicznych** (AND, OR, XOR,...). W przypadku komputerów kwantowych posługujemy się bramkami kwantowymi.

Algorytmy przedstawiamy za pomocą obwodów kwantowych, które nawet są modelowane z użyciem narzędzi graficznych:



Macierz unitarna

Reprezentacja tzw. przekształcenia unitarnego

Macierz sprzężona hermitowsko (macierz hermitowska) do $\boldsymbol{U}$: $\boldsymbol{U}^\dagger = (\boldsymbol{U}^*)^T$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

Mówimy, że macierz $\boldsymbol{U}$ jest unitarna, gdy jej odwrotnością jest jej macierz hermitowska:

$$\boldsymbol{U}^{-1} = \boldsymbol{U}^\dagger \Leftrightarrow \boldsymbol{U}\,(\boldsymbol{U}^*)^T = \boldsymbol{I}$$

Zatem wszystkie operacje kwantowe są liniowe. Są też odwracalne, w przeciwieństwie do klasycznych obwodów (złożonych z AND...). Tylko pomiar jest nieodwracalny.

Bramki kwantowe

Nowy stan:

$$\boldsymbol{U}(\alpha\,|0\rangle + \beta\,|1\rangle) = \boldsymbol{U}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

Zagadka — co robią następujące bramki?

$$\boldsymbol{Z} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \quad \boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Bramka Hadamarda

Nazywana też bramką Walsha lub Hadamarda-Walsha

Operator jest określony macierzą:

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \boldsymbol{H}^{-1} = \boldsymbol{H}^{\dagger} = \boldsymbol{H}$$

Bramka kreuje superpozycję dwóch stanów bazowych (z dowolnego kubitu!).

Bramka Hadamarda

Właściwości

Działanie macierzy Hadamarda na pojedynczym stanie bazowym:

$$\boldsymbol{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\boldsymbol{H}\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Ten efekt nie jest możliwy w przypadku stanów probabilistycznych!

Po dwukrotnym zastosowaniu wracamy do stanu początkowego (też niemożliwe dla stanów probabilistycznych), ponieważ $\boldsymbol{HH} = \boldsymbol{I}$:

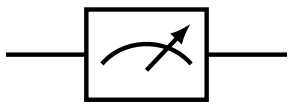
$$\boldsymbol{HH}\,|0\rangle = \boldsymbol{I}\,|0\rangle = |0\rangle$$

$$\boldsymbol{HH}\,|1\rangle = |1\rangle$$

Postulat 3

Jeśli dokonujemy pomiaru/obserwacji $|\psi\rangle$ w ortonormalnej bazie $|e_1\rangle, |e_2\rangle, \ldots, |e_d\rangle$, to uzyskamy wynik pomiaru j (tj. $|e_j\rangle$) z prawdopodobieństwem:

$$\Pr\{j\} = |\langle e_j|\psi\rangle|^2$$



Pomiar zaburza stan — wada **oraz** zaleta (nie można kopiować: tw. o nieklonowaniu) — zwiększa bezpieczeństwo ale też wprowadza niemożliwość wzmacniania „sygnału kwantowego”.

Pomiar

Pomiar pewnego systemu dokonuje się zawsze przez inny system, co powoduje zaburzenie i system pozostaje w wyniku pomiaru w stanie czystym (np. $|0\rangle$ lub $|1\rangle$).

Nie możemy wprost wyznaczyć amplitud w stanie kwantowym: $\alpha|0\rangle + \beta|1\rangle$. Ale możemy to zrobić pośrednio w wyniku wykonania pomiaru (tzn. można byłoby to robić wielokrotnie, żeby wyestymować α i β):

$$\Pr\{0\} = |\alpha|^2 \quad \Pr\{1\} = |\beta|^2$$

Pomiar

Przyjęcie bazy pomiarowej jest dowolne i umowne, byleby wektory bazy były ortonormalne, inna popularna baza:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Np. w przypadku kwantowej dystrybucji klucza (QKD) stosuje się różne bazy, dzięki czemu można wykrywać podsłuch.

Postulat 4

Mieszany stan kwantowy jest reprezentowany jako **iloczyn tensorowy** stanów, które się na niego składają.

W ogóle mamy tutaj kilka iloczynów wektorowych i wszystkie są stosowane...

Przestrzeń Hilberta

Iloczyn wewnętrzny/skalarny, *inner product*, *dot product*

- Wektory: $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$.
- Iloczyn wewnętrzny:
$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \cdot \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1^* & \alpha_2^* & \ldots & \alpha_n^* \end{bmatrix} \times \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}, \text{ czyli...}$$
- $\ldots \boldsymbol{u} \cdot \boldsymbol{v} = \langle \boldsymbol{u} | \boldsymbol{v} \rangle = \left(\boldsymbol{u}^T \right)^* \times \boldsymbol{v}$.
- Norma wektora: $|\boldsymbol{u}| = \sqrt{\langle \boldsymbol{u} | \boldsymbol{u} \rangle}$.

Iloczyn tensorowy

Iloczyn Kroneckera, iloczyn zewnętrzny, *outer product*

$$|\boldsymbol{u}\rangle \otimes |\boldsymbol{v}\rangle = |\boldsymbol{uv}\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \otimes \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 \boldsymbol{v} \\ \alpha_2 \boldsymbol{v} \\ \vdots \\ \alpha_n \boldsymbol{v} \end{bmatrix} = \begin{bmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \vdots \\ \alpha_1\beta_n \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \\ \vdots \\ \alpha_2\beta_n \\ \vdots \\ \alpha_n\beta_1 \\ \alpha_n\beta_2 \\ \vdots \\ \alpha_n\beta_n \end{bmatrix}$$

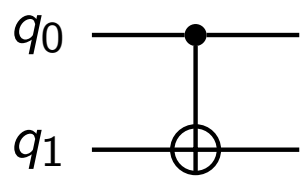
Czym jest zatem $|0\rangle \otimes |1\rangle$ albo $|1\rangle \otimes |1\rangle \otimes |0\rangle$?

Bramka sterowanej negacji CNOT

Controlled NOT

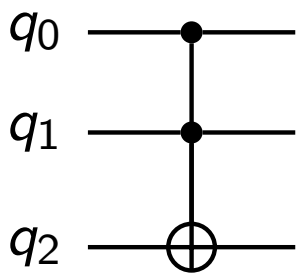
Reprezentacja macierzowa:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



Bramka Toffoli'ego

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$



Używając jedynie bramek Hadamarda i Toffoli'ego można zbudować dowolny obwód kwantowy.

Rejestry kwantowe

- Rejestr kwantowy o długości m (zestaw kubitów) — dla systemu złożonego z wielu kubitów określamy wektor opisujący go z użyciem iloczynu tensorowego:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_m\rangle$$

- Kubajt (ang. *qubyte*): rejestr złożony z ośmiu kubitów.

Wiele kubitów

Przyspieszenie kwantowe

Jeśli dokonujemy pomiaru na stanie:

$$\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

to w wyniku pomiaru uzyskamy jeden stan czysty $|xy\rangle$ z prawdopodobieństwem $\Pr\{xy\} = |\alpha_{xy}|^2$.

Tutaj widać moc obliczeniową superpozycji: możemy operować na ciągach bitowych, gdzie ogólny stan m kubitów to:

$$\sum_{\ell \in \{0,1\}^m} \alpha_\ell\,|\ell\rangle$$

Na takim stanie możemy dokonywać obliczeń (jak gdyby na 2^m ciągach na raz) — to zapewnia nam przyspieszenie kwantowe i przewagę nad systemami klasycznymi.

Stan rozkładalny

Jeśli mamy złożenie dwóch stanów:

$$\alpha\,|0\rangle + \beta\,|1\rangle \quad \text{oraz} \quad \gamma\,|0\rangle + \delta\,|1\rangle$$

w stan mieszany i rozkładalny, to uzyskamy:

$$\alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle$$

Ale mogą być stany wielokubitowe i nierozkładalne...

Splątanie kwantowe: specyficzne dla fizyki kwantowej zjawisko polegające na tym, że para (lub większa grupa) cząstek jest generowana w specjalny sposób (albo tak ze sobą oddziaływuje), że stan jednej z nich nie może być opisany oddzielnie od stanu innej (innych).

Splątanie kwantowe

Quantum entanglement

Przykład splątania — jeden z tzw. stanów Bella:

$$\left|\Phi^{+}\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

nie da się rozłożyć na $\alpha\,|0\rangle + \beta\,|1\rangle$ oraz $\gamma\,|0\rangle + \delta\,|1\rangle$ (dlaczego?).

Konsekwencja: nie wiemy z góry, co zaobserwujemy, ale jeśli zaobserwujemy stan pierwszego z kubitów jako $|x\rangle$, to na pewno drugi kubit zostanie zaobserwowany także jako $|x\rangle$ — choćby obiekt, który reprezentuje ten kubit był na drugim końcu wszechświata! Obiekty, w przypadku których wystąpiło splątanie można rozdzielić i przemieszczać — opieramy na tym **transmisję kwantową**.

Można się pobawić

Mamy biblioteki do obliczeń z użyciem algorytmów kwantowych

- IBM: Qiskit,
- Fraunhofer: Qrisp,
- Google: TensorFlow Quantum, OpenFermion, Circ
- ...

Plan wykładu

Algorytmy kwantowe

Prosty przykład: alg. Deutscha-Jozsa'y

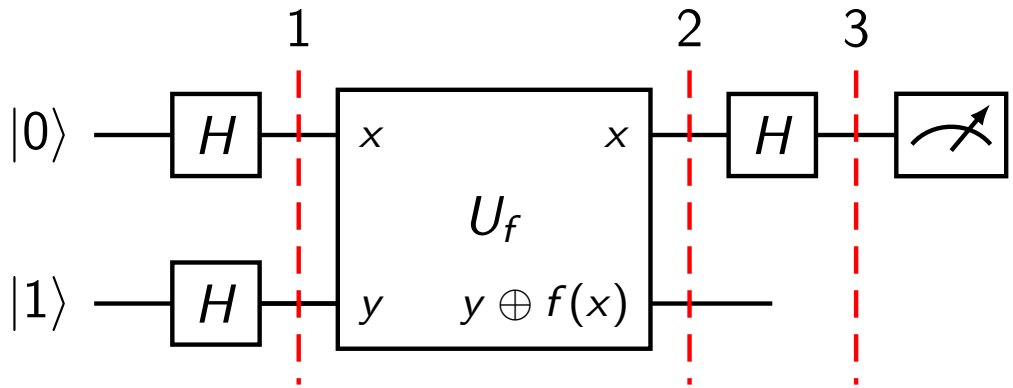
- Pojęcie funkcji stałej i funkcji zrównoważonej.
- Potrzeba jednorazowego sprawdzenia wartości (zamiast dwukrotnego, jak w przypadku klasycznym) — wynalazek Deutscha.
- Potem rozszerzenie przez Jozsa na układy n-elementowe.

Przypadek dla dwóch wartości argumentów ($n = 2$):

x	f_0	f_1	f_x	$f_{\overline{x}}$
0	0	1	0	1
1	0	1	1	0

Algorytmy kwantowe

Prosty przykład: alg. Deutscha-Jozsa'y



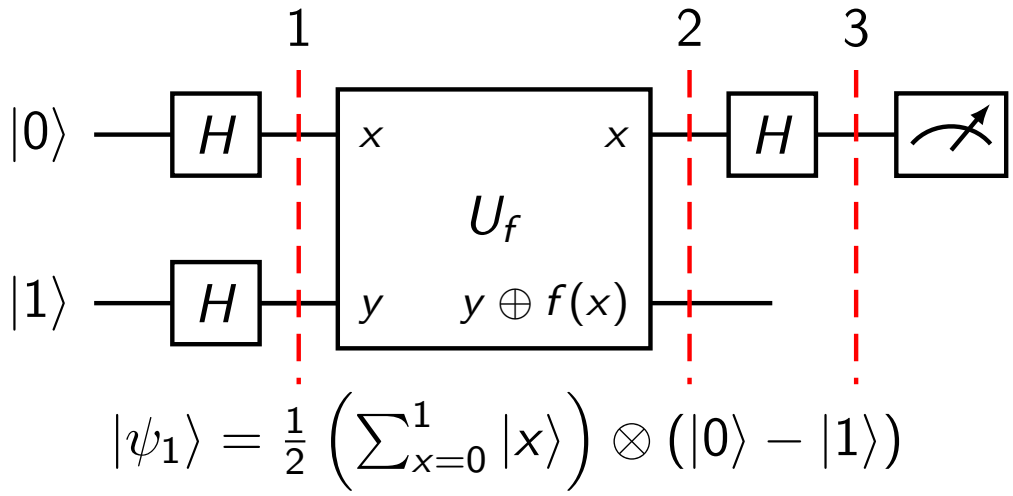
- W ogólności wnioskujemy na podstawie pomiaru $|\psi_3\rangle = (H \otimes I) U_f (H \otimes H) |01\rangle$ ☺
- Najpierw uzyskujemy stan mieszany:

$$|\psi_1\rangle = (H \otimes H) |01\rangle = H|0\rangle \otimes H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}\left(\sum_{x=0}^{1} |x\rangle\right) \otimes (|0\rangle - |1\rangle)$$

Algorytmy kwantowe

Prosty przykład: alg. Deutscha-Jozsa'y



- Obliczmy $|\psi_2\rangle = U_f |\psi_1\rangle$.
- Jeśli $f(x) = 0$:

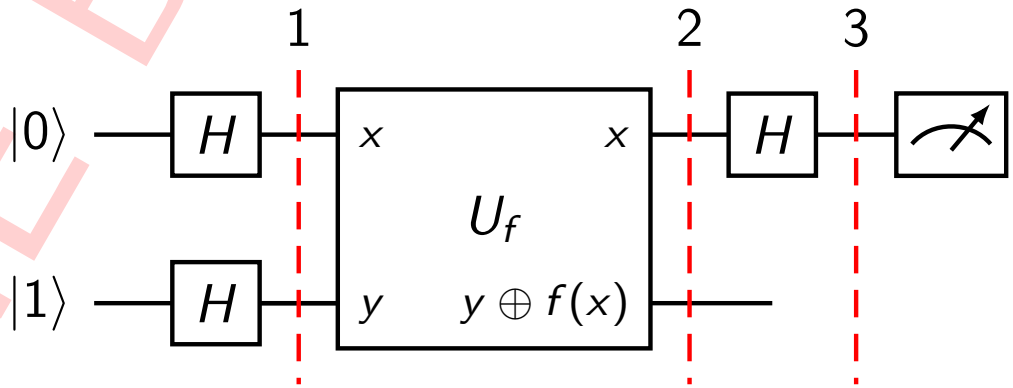
$$U_f(|x\rangle \otimes (|0\rangle - |1\rangle)) = |x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = |x, 0 \oplus 0\rangle - |x, 1 \oplus 0\rangle = |x\rangle \otimes (|0\rangle - |1\rangle)$$

- Jeśli $f(x) = 1$:

$$U_f(|x\rangle \otimes (|0\rangle - |1\rangle)) = |x, 0 \oplus 1\rangle - |x, 1 \oplus 1\rangle = -|x\rangle \otimes (|0\rangle - |1\rangle)$$

Algorytmy kwantowe

Prosty przykład: alg. Deutscha-Jozsa'y



- Zatem kompaktowo możemy zapisać $|\psi_2\rangle = U_f |\psi_1\rangle$:

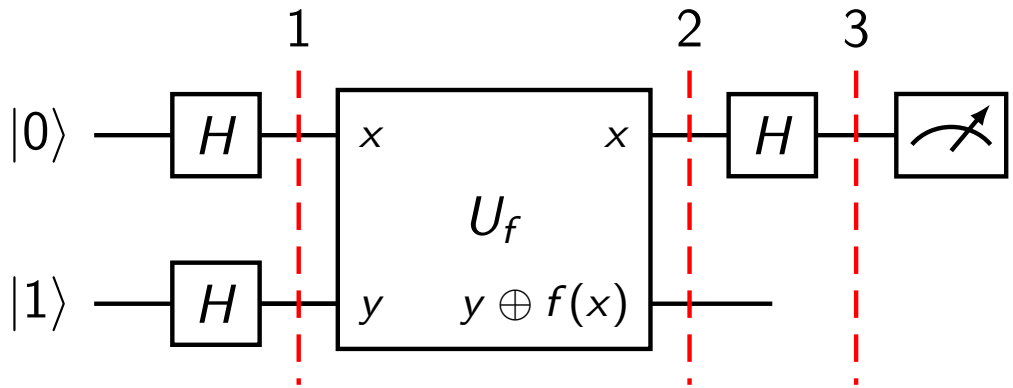
$$|\psi_2\rangle = \frac{1}{2}\left(\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle\right)\otimes(|0\rangle-|1\rangle) = |\phi_2\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

- Gdzie mamy do czynienia ze stanem:

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$$

Algorytmy kwantowe

Prosty przykład: alg. Deutscha-Jozsa'y



$$|\phi_2\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$$

- Finalnie dokonujemy pomiaru na $H|\phi_2\rangle$:

$$|\psi_3\rangle = H|\phi_2\rangle = \frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \frac{1}{2}\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle$$

- Interpretacja wyniku jednokrotnego pomiaru:
  - $|0\rangle$: czynnik przy $|1\rangle$ musiał się wyzerować, czyli było $f(0) = f(1)$ — funkcja jest stała;
  - $|1\rangle$: czynnik przy $|0\rangle$ musiał się wyzerować, czyli...

Plan wykładu

Kanały kwantowe

- ρ: ogólna reprezentacja stanu kwantowego transmitowanego przez kanał;
- E: reprezentacja kanału (funkcja przejścia).

- Idealny: $E(\rho) = \rho$.
- Kanały z błędami: ogólnie $E(\rho) = (1 - p)\rho + pA\rho A^{\dagger}$.

Kanały kwantowe

Kanał z odwracaniem wartości, *bit-flip channel*

$$E(\rho) = (1-p)\rho + pX\rho X^\dagger$$

Dla pojedynczego kubitu:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{p} \beta|0\rangle + \alpha|1\rangle$$

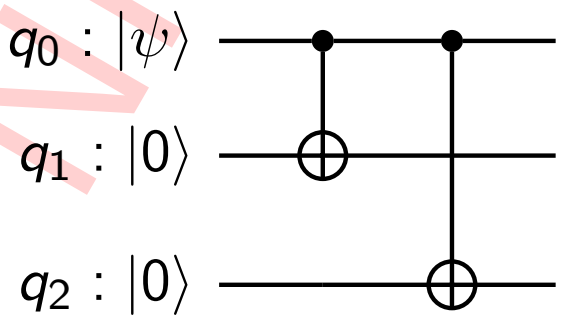
Mamy inne modele kanałów, już nieodpowiadające intuicjom związanym z kanałami klasycznymi, np. kanał zmieniający fazę, kanał z depolaryzacją...

Korekcja przekłamań

Kodowanie stanów

Zobaczmy przykład najprostszego kodu korekcyjnego — trzykubitowy kod chroniący przed odwracaniem (*three-qubit bit-flip code*).

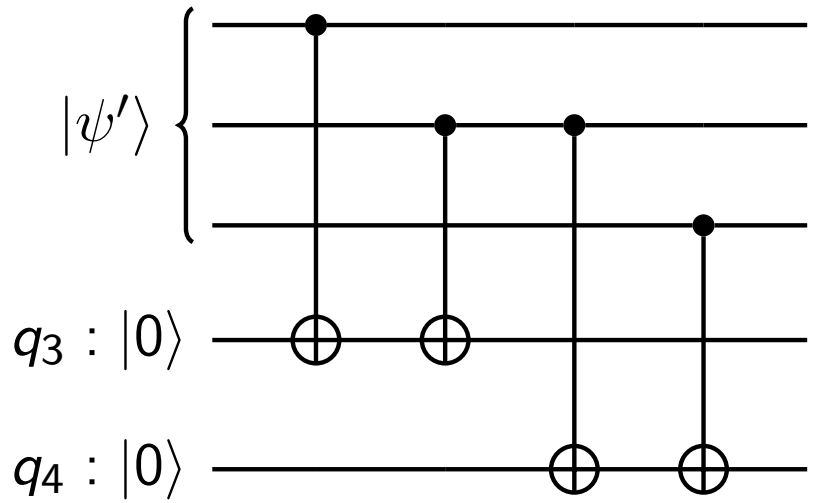
- Chcemy przesłać $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.
- Kodujemy jako (por. klasyczny kod z powtarzaniem): $|\psi'\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$. Do kodowania używamy bramek CNOT (kontrolowanej negacji).



Korekcja przekłamań

Pomiar syndromu

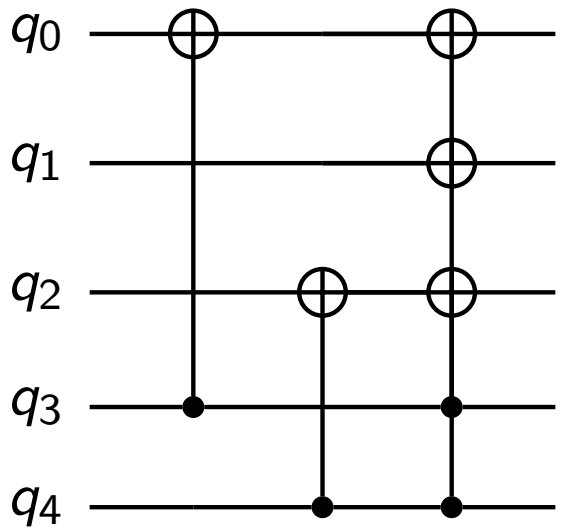
Syndrom jest mierzony za pomocą kubitów pomocniczych.



Korekcja przekłamań

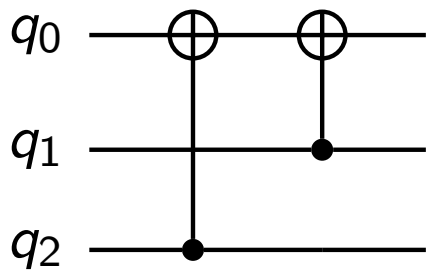
Korekcja przekłamań

Używamy bramek CNOT, ale też bramki Toffoli'ego:



Korekcja przekłamań

Dekodowanie



QComm

Teleportacja kwantowa

- Alice przesyła: $|\phi_D\rangle = \alpha|0\rangle + \beta|1\rangle$, używając stanu splątanego $|\Psi^+\rangle$, czyli:

$$|\psi_D\rangle = |\phi_D\rangle \otimes |\Psi^+\rangle$$

- Zatem stan mieszany, którym dysponuje Alice:

$$\begin{aligned} |\psi_D\rangle &= \alpha|0\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta|1\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ &= \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}} \end{aligned}$$

- Alice używa bramki CNOT do dwóch kubitów, którymi dysponuje (czyli zmienia $|10\rangle$ na $|11\rangle$ oraz $|11\rangle$ na $|10\rangle$):

$$|\psi_D\rangle = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle}{\sqrt{2}}$$

QComm

Teleportacja kwantowa

- Alice używa bramki Hadamarda H do $|\psi_D\rangle$ (czyli zmienia $|0\rangle$ na $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ oraz $|1\rangle$ na $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$), uzyskując stan mieszany:

$$|\psi_D\rangle = \frac{\alpha|000\rangle+\alpha|100\rangle+\alpha|011\rangle+\alpha|111\rangle+\beta|010\rangle-\beta|110\rangle+\beta|001\rangle-\beta|101\rangle}{2}$$

- Można przedstawić rozkład $|\psi_D\rangle$:

$$|\psi_D\rangle = \frac{|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle)+|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)}{2}$$

- Teraz Alice dokonuje pomiaru na swoich dwóch kubitach i z prawdopodobieństwem $\frac{1}{4}$ odczyta $|00\rangle$, $|01\rangle$, $|10\rangle$ albo $|11\rangle$. Jednakże jej pomiar wpływa na to, co da wynik pomiaru u Boba (ze względu na splątanie).
- Alice wysyła wynik pomiaru w sposób klasyczny do Boba.

QComm

Teleportacja kwantowa

$$|\psi_D\rangle = \frac{|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle)+|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)}{2}$$

W zależności od tego, co zmierzy Alice, Bob wie:

- Jeśli Alice poda $|00\rangle$, to stan kubitu Boba to po prostu: $\alpha\,|0\rangle + \beta\,|1\rangle$ — czyli Bob dysponuje wprost ϕ_D.
- Jeśli Alice poda $|01\rangle$, to stan kubitu Boba to: $\alpha\,|1\rangle + \beta\,|0\rangle$ — Bob uzyska kubit Alice jeśli zastosuje bramkę X (NOT).
- Jeśli Alice poda $|10\rangle$, to stan kubitu Boba to: $\alpha\,|0\rangle - \beta\,|1\rangle$ — Bob uzyska kubit Alice jeśli zastosuje bramkę Z.
- Jeśli Alice poda $|11\rangle$, to stan kubitu Boba to: $\alpha\,|1\rangle - \beta\,|0\rangle$ — Bob uzyska kubit Alice jeśli zastosuje bramki X oraz Z.

Podsumowanie

- Przyspieszenie kwantowe dzięki superpozycji. Teleportacja dzięki splątaniu.
- Realizacja sprzętu: w rękach fizyków.
- Wymyślenie algorytmów: jak najbardziej dla teleinformatyków (można też symulować działanie w celu sprawdzenia poprawności).
- Z punktu widzenia teleinformatycznego: opis algebraiczny i probabilistyczny.
- Konstrukcja zupełnie nowych algorytmów: obliczeniowych i transmisyjnych.
- Problematyka: kryptografia, korekcja przekłamań, uczenie maszynowe, telekomunikacja...

OBLICZENIA

Dziękuję za uwagę