Obliczenia kwantowe

- **Obliczenia kwantowe** = obliczenia wykonywane przez urządzenia wykorzystujące własności mechaniki kwantowej nieobecne na poziomie klasycznym (komputery kwantowe)

- **Oczekiwane korzyści** - (istotne) przyspieszenie obliczeń (redukcja wykładniczej zależności między wielkością danych wejściowych a czasem wykonania obliczenia do zależności wielomianowej, lub istotna redukcja stopnia wielomianu opisującego tę zależność)

Czym różni się mechanika kwantowa od klasycznej?

- Różnice w używanym aparacie formalnym
  - przestrzeń fazowa *vs.* przestrzeń Hilberta stanów
  - stany układu: punkty w przestrzeni fazowej *vs.* wektory w przestrzeni Hilberta (a właściwie punkty w odpowiedniej przestrzeni rzutowej)
  - statystyczne mieszaniny stanów: zbiory mierzalne (wraz z odpowiednią miarą) w przestrzeni fazowej *vs.* nieujemne, śladowe operatory na przestrzeni Hilberta
  - obserwable (wielkości mierzalne) jako funkcje na przestrzeni fazowej *vs.* operatory hermitowskie na przestrzeni Hilberta
- **Różnice "ontologiczne"**
  - liniowa superpozycja stanów układu kwantowego jest również dopuszczalnym stanem (zasada superpozycji), w przeciwieństwie do mechaniki klasycznej, gdzie taka superpozycja nie ma sensu)
  - wielkości fizyczne (pęd, energia, spin) nie są w mechanice kwantowej własnościami układu fizycznego, tzn. nie istnieją "w nim"

Konsekwencje

- pomiar w mechanice kwantowej jest destrukcyjny (pomiar niszczy stan mierzonego układu w sposób nieodwracalny)
- nie można odtworzyć stanu przed pomiarem na podstawie wyniku pomiaru, natomiast stan po pomiarze jest ściśle wyznaczony przez ten wynik
- nie można "sklonować" nieznanego stanu układu kwantowego
- wyniki pomiarów są probabilistyczne (pomiar tej samej wielkości fizycznej w tym samym stanie układu może dać różne wyniki, niezależnie od precyzji przyrządów pomiarowych)
- za pomocą pomiaru można **ściśle** odróżnić dwa stany ortogonalne
- konsekwencją liniowości mechaniki kwantowej jest to, że stan układu złożonego jest wektorem w iloczynie tensorowym przestrzeni Hilberta podukładów
- stany układu złożonego mogą być **separowalne** (tensory proste) lub **splątane** (pozostałe) - te ostatnie mają własności korelacyjne, "paradoksalne" z punktu widzenia mechaniki klasycznej (EPR)

Obliczenia kwantowe

- **obliczenie kwantowe** = przekształcenie stanu początkowego odpowiedniego układu (danych wejściowych) kwantowego w stan końcowy (wynik obliczenia) za pomocą operacji dopuszczalnych przez mechanikę kwantową, takich jak
  - ewolucja kwantowa (zadana równaniem Schrödingera - proces całkowicie deterministyczny)
  - sprzęganie z innym układem kwantowym
  - wykonywanie pomiarów na układzie (lub podukładach)
- **algorytm kwantowy** - sekwencja powyższych elementarnych operacji

Jak (nie)działa komputer kwantowy

- przypuśćmy, że skonstruowaliśmy algorytm kwantowy

$$|\psi\rangle \mapsto |f(\psi)\rangle$$

"obliczający" wartość funkcji f dla dowolnej danej wejściowej $|\psi\rangle$ (reprezentującej np. pewną liczbę x) w postaci wyniku $|f(\psi)\rangle$ (reprezentującego liczbę $f(x)$)

- z liniowości mechaniki kwantowej (zasady superpozycji stanów i liniowości operacji kwantowomechanicznych wynika, że)

$$|\psi_1\rangle + |\psi_2\rangle + \cdots + |\psi_n\rangle \mapsto |f(\psi_1)\rangle + |f(\psi_2)\rangle + \cdots + |f(\psi_n)\rangle$$

po jednym przebiegu otrzymujemy wartości dla dowolnej liczby danych wyjściowych (" kwantowy paralelizm")

Jak (nie)działa komputer kwantowy

- **Niestety, to nie działa**
  - musimy odczytać wynik (dokonać pomiaru na stanie końcowym)
  - pomiar taki daje jeden wynik, niszczy przy tym tak "chytrze" otrzymany stan końcowy, bez możliwości jego odtworzenia
  - "kwantowy paralelizm" okazuje się nieprzydatny
  - co gorzej, w porównaniu z mechanika klasyczną tracimy - otrzymany pojedynczy wynik jest jedynie probabilistyczny
- **Wnioski**
  - zdajemy niemądre pytania
  - trzeba wymyślać algorytmy kwantowe, które unikają opisanych wyżej trudności

Przykład: algorytm Deutcha-Jozsy

- chcemy stwierdzić, czy funkcja boolowska $f : \{0, 1\} \to \{0, 1\}$ jest stała $f(0) = f(1)$, czy nie $f(0) \neq f(1)$
- klasycznie musimy dokonać dwukrotnego przebiegu: dla wartości wejściowej 0 i 1
- kwantowo można znaleźć odpowiedź za pomocą jednego przebiegu

Przykład: algorytm Deutcha-Jozsy

- Potrzebujemy
  - dwóch układów kwantowych w dwuwymiarowych przestrzeniach Hilberta (kubitów), w każdej z nich kodujemy 0 i 1 za pomocą dwóch ortogonalnych wektorów $|0\rangle$ i $|1\rangle$
  - kwantowego algorytmu $|\psi\rangle \mapsto |f(\psi)\rangle$
  - urządzenia wykonującego (dopuszczalną) przez mechanikę kwantową operację $H : |0\rangle \mapsto |0\rangle + |1\rangle, \quad H : |0\rangle \mapsto |0\rangle - |1\rangle$
- Przygotowujemy nasz układ złożony w stanie $|0\rangle \otimes (|1\rangle)$
- Wykonujemy operację H na obu podukładach, otrzymujemy $(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$
- Wykonujemy na całym układzie (dopuszczalną) operację $U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |(x+y) \mathrm{mod}\, 2\rangle$
- Otrzymujemy $((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)$
- Za pomocą **pojedynczego** pomiaru w pierwszym podukładzie dokonujemy rozróżnienia między ortogonalnymi stanami $|0\rangle + |1\rangle$ (otrzymanym, gdy $f(0) = f(1)$) i $|0\rangle - |1\rangle$ (gdy $f(0) \neq f(1)$)

Co jeszcze?

- **Algorytm Shora**: faktoryzacja (część kwantowa dotyczy szybkiego znajdowania okresu funkcji)
  - redukcja czasu wykonywania $O(\exp(N) \to O(N)$
  - potencjalne zastosowania: łamanie publicznych kluczy kryptograficznych (RSA)
- **Szybka transformacja Fouriera** (j.w.)
- **Algorytm Grovera**
  - redukcja czasu wykonywania $O(N) \to O\sqrt{N}$
- **"Wykrywanie fałszywych monet"** (N - monet, k - fałszywych - np. o innej masie, możemy porównywać parami na wadze szalkowej)
  - redukcja czasu wykonywania $O(k \log(N/k)) \to O(k^{1/4})$
- **Sprawdzanie przemienności macierzy** (k macierzy $n \times n$ - sprawdzić, czy komutują)
  - redukcja czasu wykonywania $O(kn^2) \to O(k^{4/5} n^{9/5})$
- **Sprawdzanie czy liczba n jest liczbą pierwszą**
  - redukcja czasu wykonywania $O(n^4 2) \to O(n^2 (\log n)^3)$
- ~ 100 algorytmów (przybliżone rozwiązanie układów r-nań liniowych, algorytmy optymalizacyjne w uczeniu maszynowym, specyficzne algorytmy teorii grup...)

Co powoduje "quantum speed-up"?

- splątanie? (nie, *viz.* algorytm Deutcha-Jozsy, chociaż w niektórych algorytmach może grac rolę, w szczególności w tzw. *one-way quantum computing*)

- zasada kwantowej superpozycji? (zasadniczo tak, w sumie więc rolę gra "kwantowy paralelizm" odpowiednio wykorzystany)

Implementacje i przeszkody

- Proponowane fizyczne architektury komputerów kwantowych
  - Zimne atomy i jony w pułapkach magneto-optycznych sterowane polami laserowymi
  - Układy nadprzewodzące
  - Elektrony w kropkach kwantowych
  - Jądrowy rezonans magnetyczny
  - Pola elektromagnetyczne we wnękach rezonansowych
- Przeszkody
  - Dekoherencja - utrata własności kwantowych na skutek oddziaływania z otoczeniem

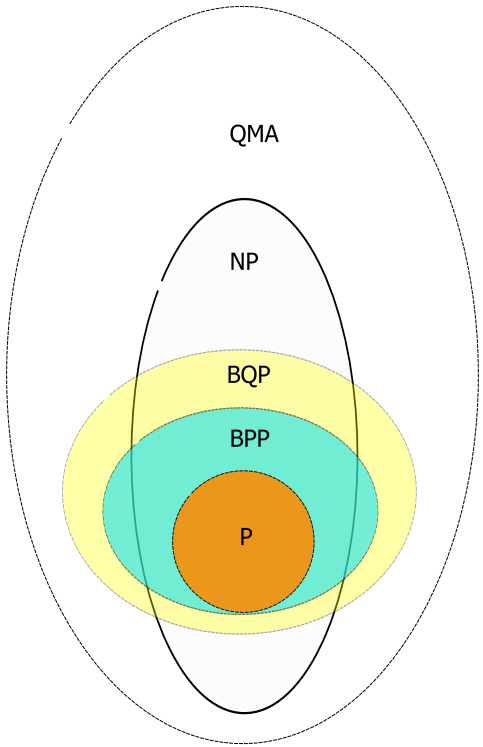
Problemy fundamentalne. Klasy złożoności

P - rozwiązywalne przez deterministyczny komputer klasyczny w czasie wielomianowym

BPP - rozwiązywalne przez probabilistyczny komputer klasyczny w czasie wielomianowym

BQP - rozwiązywalne przez komputer kwantowy w czasie wielomianowym
NP rozwiązanie może być sprawdzone przez deterministyczny komputer klasyczny w czasie wielomianowym

QMA - rozwiązanie może być sprawdzone przez komputer kwantowy w czasie wielomianowym



Problemy fundamentalne. Komputery kwantowe i Teza Churcha

- Teza Churcha "Co może być efektywnie policzone, może być policzone przez maszynę Turinga
- Dla fizyka: "efektywnie policzalne"="policzalne przez rzeczywisty układ fizyczny" (obiekty matematyczne, niezależnie od poglądów jakie mamy na temat ich ontologii, są poznawalne za pomocą zjawisk fizycznych - dynamiki cząstek i pól, przebiegów elektrycznych w mózgu...)
- **Mechanika kwantowa nie narzuca dodatkowych ograniczeń na obliczalność w sensie fizycznym**

Problemy fundamentalne. Dowody komputerowe

- Dowód komputerowy problemu czterech barw
- Podobieństwa: "ufamy" komputerowi, nie jesteśmy w stanie przeprowadzić dowodu w krótkim czasie
- Różnice: w klasycznym wypadku możemy, w zasadzie, sprawdzić stan komputera w dowolnym momencie, w kwantowym jest to niemożliwe - pomiar niszczy "kwantowość"
- Znane algorytmy kwantowe dają rezultaty sprawdzalne na komputerze klasycznym w wielomianowym czasie, jednak nie wyklucza to istnienia (i przydatności) algorytmów niespełniających tego warunku