Kvantové počítače

Radek Rozkošný

Obsah prezentace

- Co je kvantový počítač?
- Kvantové informace
- Kvantový bit
- Kvantový hardware
- Využití

Co je kvantový počítač?

- Klasický počítač
  - Je počítač, který využívá elektrický proud protékající obvody, který lze měřit klasickými postupy
- Kvantový počítač
  - využívá při svojí činnosti fenomény známé z kvantové mechaniky, jako je například superpozice nebo kvantové provázání, k vykonávání operací s daty

Klasické vs. kvantové pojetí informace

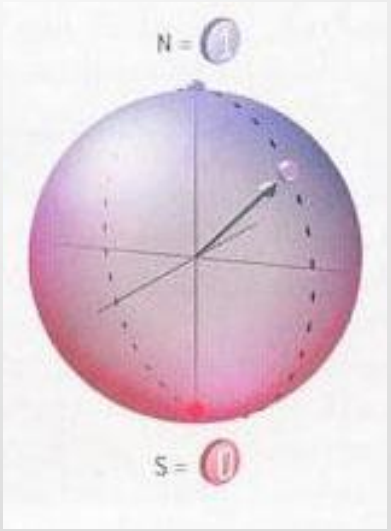
- Klasická informace
  - Lze libovolně kopírovat. Zejména je možné vytvořit zcela identickou kopii dané zprávy.
- Kvantová informace
  - Nelze vytvořit identickou kopii neznámého kvantového stavu.
    - Čtení zprávy zároveň ovlivňuje její obsah.

Kvantový bit - qubit [kju:bit]

- jednotka kvantové informace
- Je reprezentovaný jednoduchým atomovým jádrem
- informace kódována jako jeden ze dvou kvantových stavů kvantového objektu
- jeden qubit může nabývat hodnot 1 nebo 0 anebo superpozice obou
- konkrétní hodnotu 0 či 1 nabývá qubit až ve chvíli měření

Bit vs Qubit

- Bit
  - může mít jeden z dvou stavů: 0 nebo 1.
  - Bit může být reprezentovaný tranzistorem přepnutým ho polohy ZAPNUTO nebo VYPNUTO.
- Qubit
  - má mnohem více možných stavů
  - stavy můžou být reprezentované šipkou ukazující na místo ve sféře
  - Severní pól je rovný 1, jižní 0, ostatní lokace jsou kvantové superpozice 0 a 1čky

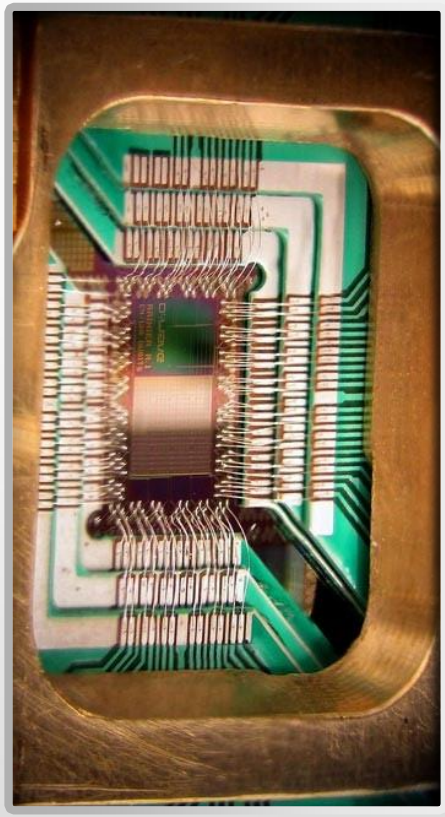


Základní výpočetní jevy kvantových počítačů

- **Kvantová interference qubitů** – vzájemné ovlivňování stavu qubitů, kdy pro některé výpočetní cesty může dojít k vzájemnému vyrušení stavu qubitů, nebo naopak k zesílení pravděpodobnosti jejich stavu
- **Kvantové provázání (propletení) qubitů** – máme dva zapletené qubity a na jednom naměříme hodnotu buď 1 nebo 0. Díky spojení naměříme na druhém qubitu stejnou hodnotu, jako na prvním a vzdálenost mezi quibity je irelevantní, ačkoli rychlost interakcí mezi qbity nemůže přesáhnout rychlost světla

Kvantový hardware

- Problém s citlivostí kvantových stavů
- Nemůžeme provádět měření během procedury
- Jsou vyvíjeny dva typy metod:
  - Lineární pasti podchlazených iontů
  - Spin-molekulární struktury



Praktické využití

- Simulace kvantové mechaniky
  - ve fyzice, chemii, nanotechnologiích, biologii a medicíně.
  - Počítač může vypočítat miliony proměnných najednou.
    - Všechny jsou dnes omezeny pomalou rychlostí kvantových simulací.
- Kryptoanalýza
  - Je schopen prolomit extrémně komplikované kódy
    - RSA šifrování

Ukázka

- http://algassert.com/quirk

Děkuji za pozornost