Kvantumszámítógépek – miért?

Hagyományos számítógép:

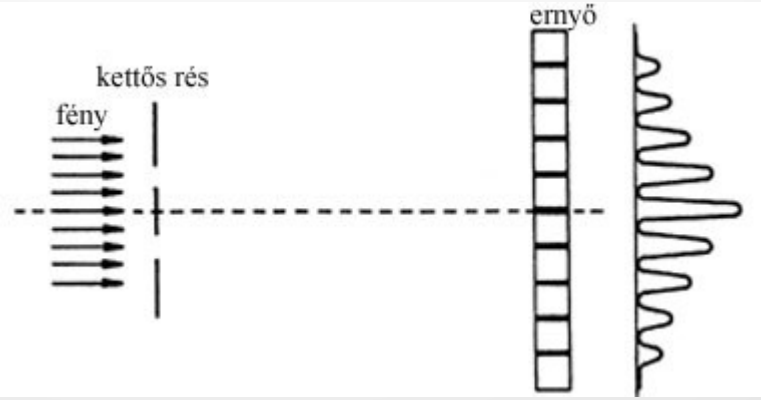
- kétállapotú memória (bit)
- elektronikus jelszinten alapuló logikai kapuk
- órajelre végzett műveletek

Elvileg minden rendben (Moore törvény, szépen nő a teljesítmény)
Kisebb problémákat jeleznek előre (pl. egyre csökkenteni kell a vezető- és félvezető rétegek méretét a nagyobb órajel és integráltság érdekében, 10 mikron, 30 atom, alagútjelenség...)

Kvantumszámítógépek – alapok

Rájöttek, hogy az elemi részecskék kvantumállapotában (hullámfüggvény) információ tárolható és az manipulálható, majd kiolvasható.

Miről is van szó?
- hullámfüggvény (részecske típusú és hullám típusú viselkedés)
- mérés hatására veszi fel a sajátállapotát
- interferencia: valójában hullám
- 1 részecske interferencia – benne van az információ a részecske hullámfüggvényében

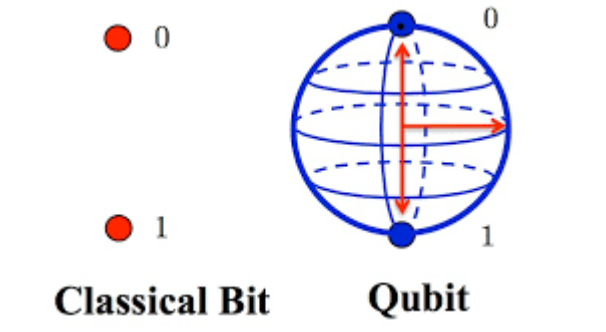


Kvantumszámítógépek – Qubit

A rendszer zavartalan állapota:

Klasszikus bit: 0 kizáró vagy 1

Qubit: A * 1 + B * 0, ahol A és B komplex számok – ez lesz az információtárolás egysége.



Kvantumszámítógépek – mit csinálunk?

Játék a hullámfüggvényekkel:

1. csináljunk egy környezettől kellően elzárt rendszert (alacsony hőmérséklet, elektromágneses szigetelés)
2. állítsuk be a kezdőállapotot
3. időnként piszkáljuk (végezzünk rajta műveleteket)
4. olvassuk ki a végállapotot

A piszkálást bizonyos algoritmusokkal művelve ezzel a rendszerrel műveletek végezhetők: számítógép

Kvantumszámítógépek – implementáció

Hogyan készítsünk el egy ilyet fizikailag?

- Qubit: valami kétállapotú kvantumos mennyiség, pl. magspin (mérés esetén a mágneses tér irányába, vagy azzal ellentétesen áll be, egyébként a két sajátállapot szuperpozíciója)

- Manipuláció változó mágneses térrel

- Csatolt állapot lehetséges: feltételes NEM kapu két Qubit között (ha az egyik 1, akkor a másik átfordul, különben nem)

- Mérés a végén NMR berendezéssel

Kvantumszámítógépek – algoritmusok

Két algoritmust is sikerült erre a furcsa rendszerre alkotni:

Shor: számok törzstényezőkre bontása
Grover: rendezetlen listában keresés

Általában milyen területen érdemes támadni:
- n db azonos típusú elemből álló értelmezési tartomány
- mindegyik n elem azonos valószínűséggel lehet megoldás
- ugyanazt az algoritmust kell minden elemre futtatni, hogy megkapjuk, hogy az adott elem megoldás-e

Hagyományos számítógép: n/2 a várható érték a megoldás idejére
Kvantumszámítógép: gyök n (/2) – de miért?

Kvantumszámítógépek – párhuzamos működés

Mert a Qubit nem egy információs bit, a Qubit-ekből álló „regiszter” nem egy értéket (pl. induló értéket) tárol, hanem ez egy sok dimenziós komplex vektor. A megoldási algoritmus sok induló értékkel egyszerre indítható el! (valójában az értelmezési tartomány egy alterével indítható az algoritmus)

És ezek nem zavarják egymást? Nem

(pl. az egymáson „keresztben” haladó fotonok sem zavarják egymást.)

Kvantumszámítógépek – valószínűségi végeredmény

De a kiolvasott „eredménnyel” van kis probléma:

Valószínűségi eredményt kapunk!
(pl. az 5 92% valószínűséggel osztója a 15-nek, a 7 pedig 4% valószínűséggel...)
Tehát az eredményt „hagyományos” számítógéppel ellenőrizni kell!

Ezért olyan területeken lehet jól bevetni a kvantumszámítógépeket, ahol az eredményt nehéz kiszámolni, de könnyű ellenőrizni.

Kvantumszámítógépek – problémák

Két éve: 10 qubit-es gép, sikerült a 15-öt törzstényezőkre bontani a Shor algoritmus egyszeri futtatásával, azaz „1 lépésben”.

Növelni kellene a Qubit-ek számát! Problémák:
- egyre romlik a jel/zaj viszony, egyre kisebb környezeti zaj lehetséges, egyre hidegebb és jobban árnyékoltabb rendszer kell
- a „szomszédos” Qubit-ek esetében jó a csatolás, nem minden Qubit alkot egymással két Qubit-es kaput, csak kitüntetett párok vannak (az algoritmusok bonyolódnak)

Növelni kell a végezhető műveletek számát! A mostani zavarvédettség mellett pár 100 művelet után szétesik az állapotfgv.

Kvantumszámítógépek – még luxuscikk