

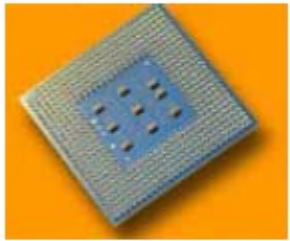
Kvantové počítání

Mooreův zákon: každé dva roky se počet součástek na čipu zdvojnásobí
Dnešní přepínače ... miliarda atomů

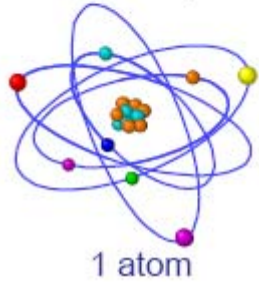
Kolik atomů per bit ?



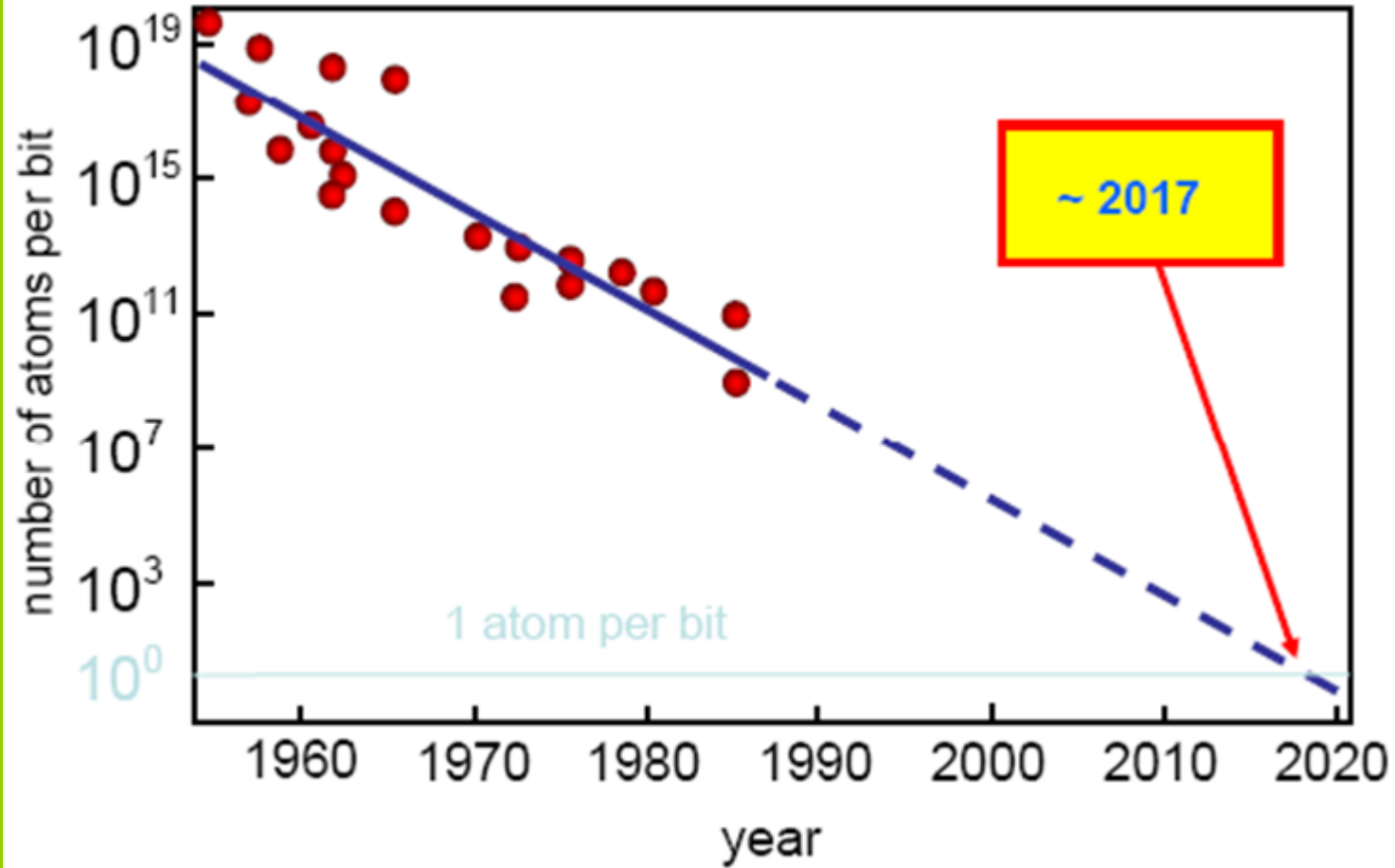
ENIAC (1947)



Pentium 4 (2002)



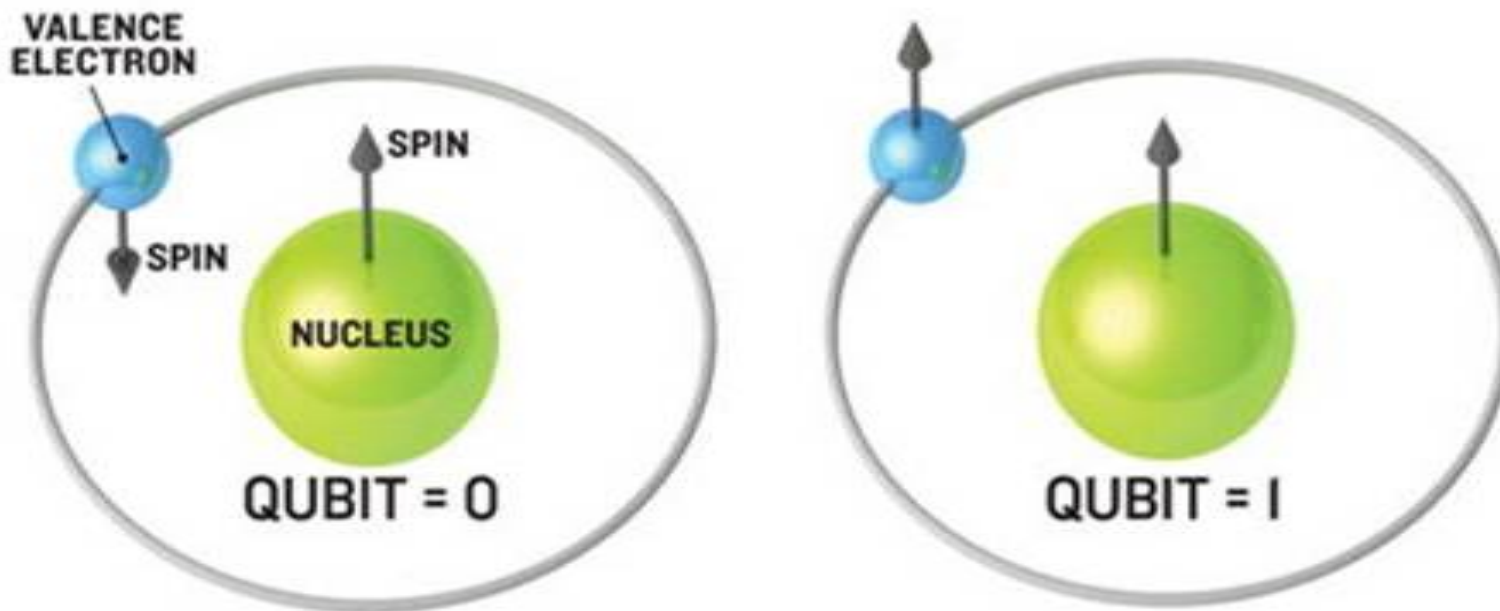
1 atom



- Na tak malých rozměrech přichází ke slovu kvantová mechanika:
- Částice se může nacházet na dvou nebo více místech současně
- Částice může se jednou projevovat jako tvrdý kousek hmoty, jindy jako klubko vlny

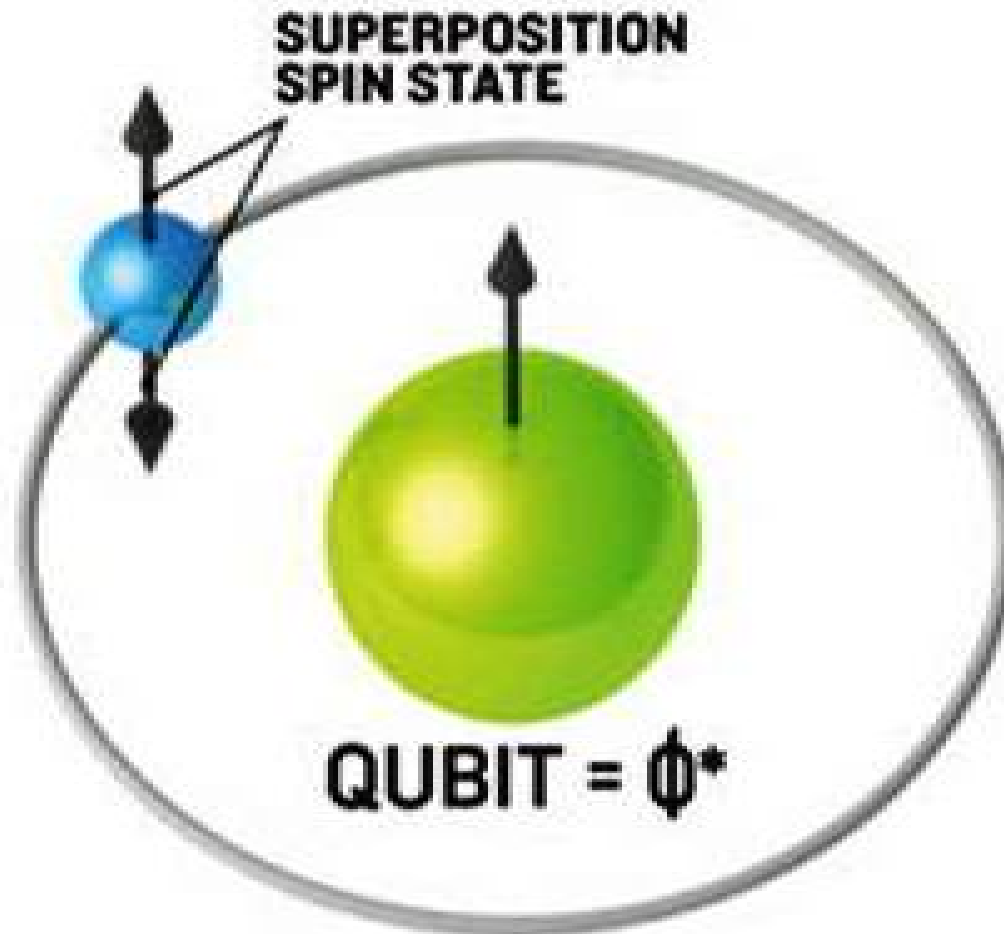
- Co nastane, když se částice (atomy) s takto surrealistickým chováním se stanou elementy počítače ?

- atom rotuje proti směru hodinových ručiček 1
- atom rotuje po směru hodinových ručiček 0



Kdyby byly přípustné pouze tyto dvě možnosti, tak atom by byl nepředstavitelně malým obyčejným přepínačem

Ale kvantová mechanika: atom se může nacházet v obou stavech 1 a 0 současně



V čipu budou binární jedničky a nuly, ale také kvantová kuriozita superpozice dvou stavů 1 a 0

..... kvantová rozmazanost ...
nebude mít stejná příčina vždy stejné
důsledky

.... Neurčitost

.....Kvantový indeterminismus.....

Děsivá představa ???

- Zabránit kvantovým jevům ?
- Richard Feynman, Paul Benioff ... mohla by to být výhoda

Ještě ke kvantové mechanice:

- Kvanta – Max Planck
- Fotoelektrický jev – Albert Einstein

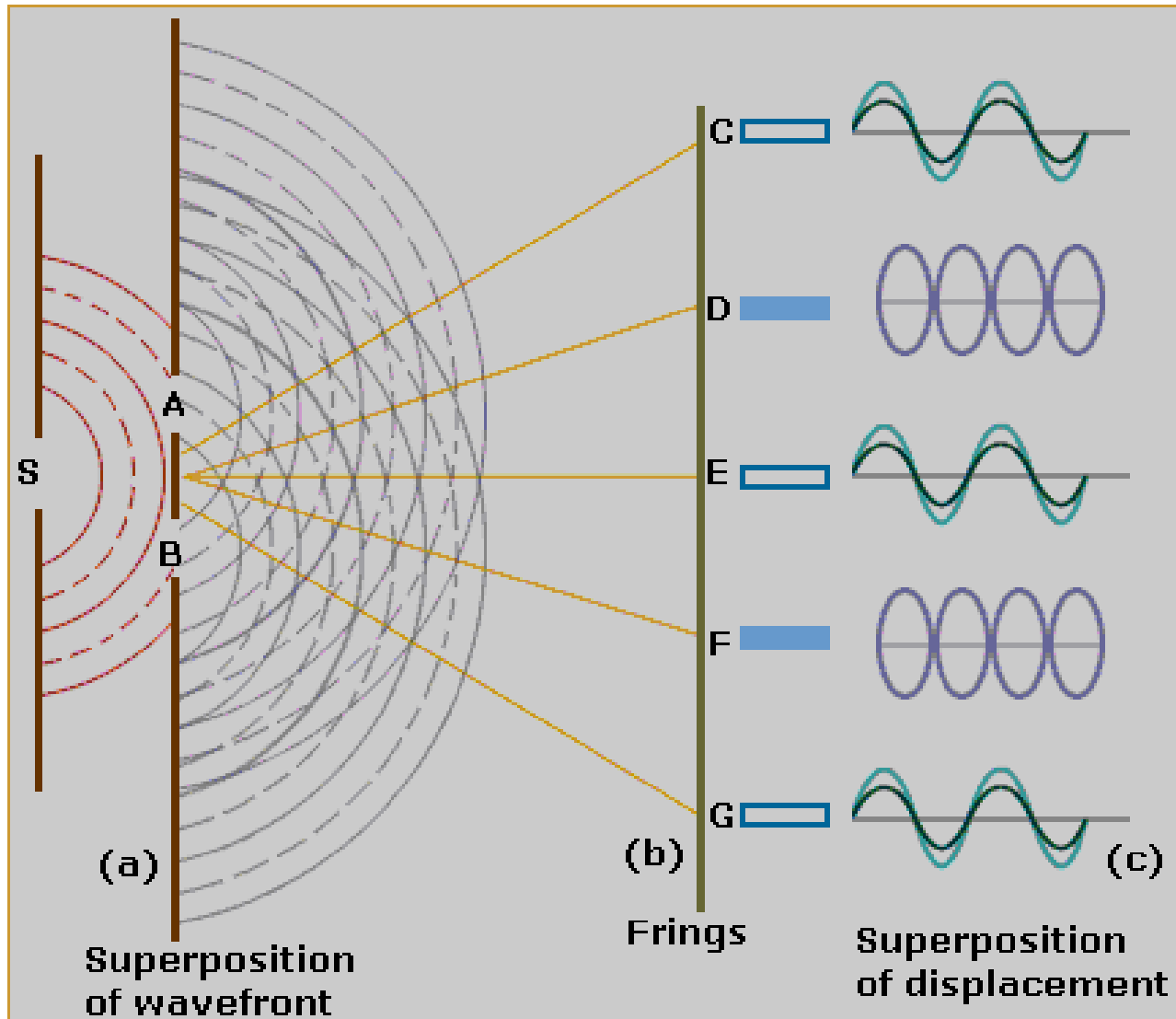
- Co vlastně říká jednotlivému fotonu dopadajícímu na sklo, zda se má odrazit nebo zda má projít ????
- Každý foton činí své rozhodnutí naprosto náhodně

analogie

- Hudba linoucí se z vibrujícího reproduktoru – různé typy vlnek od houslí, klavíru, trubky
- Foton letící ke sklu je soubor vlnek popisující všechny stavy částice ... dosáhne detekční zařízení .. Superpozice se naruší ... přežije jen jediný typ vlnky, všechny ostatní odpovídající jiným stavům zaniknou

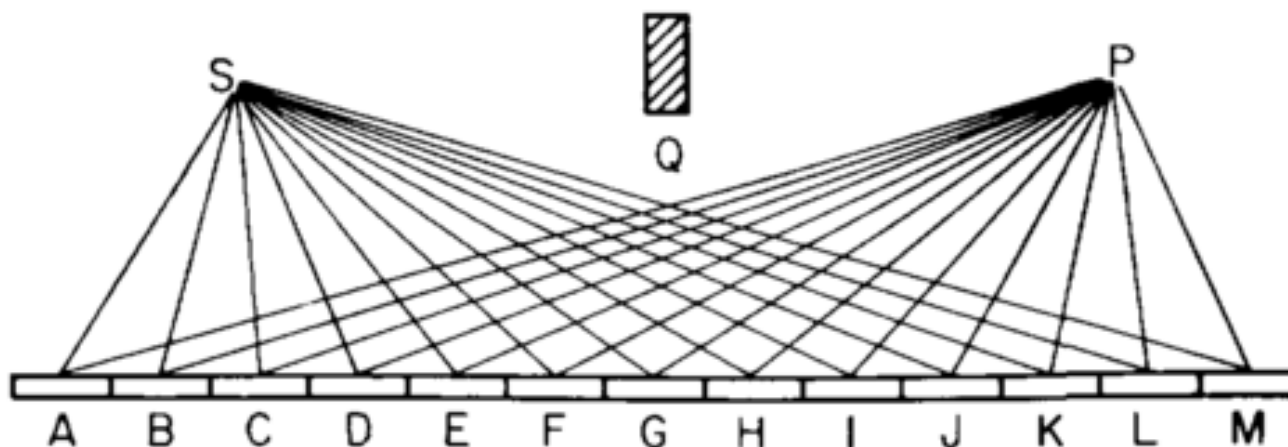
Experiment se dvěma štěrbinami

- Vlny na vodě
- Fotony letící ke dvou štěrbinám ... zakrýt jeden otvor... zakrýt druhý otvor ... nechat odkryté oba dva ... nebudou dvě stopy !!!
- Zmenšit intenzitu ... fotony letí jeden po druhém



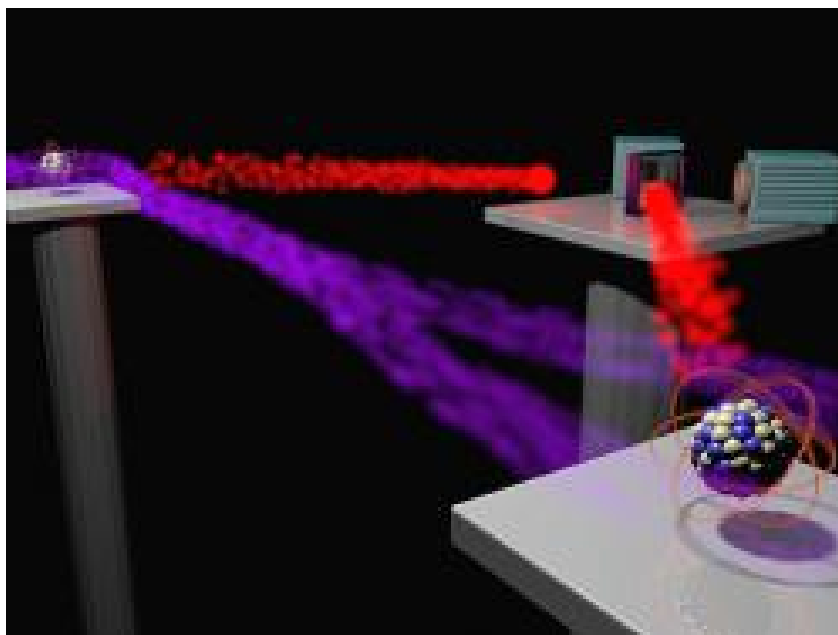
Místo vln:

- Feynman: mnohohrahová interpretace ... foton zkouší současně všechny možnosti svého letu

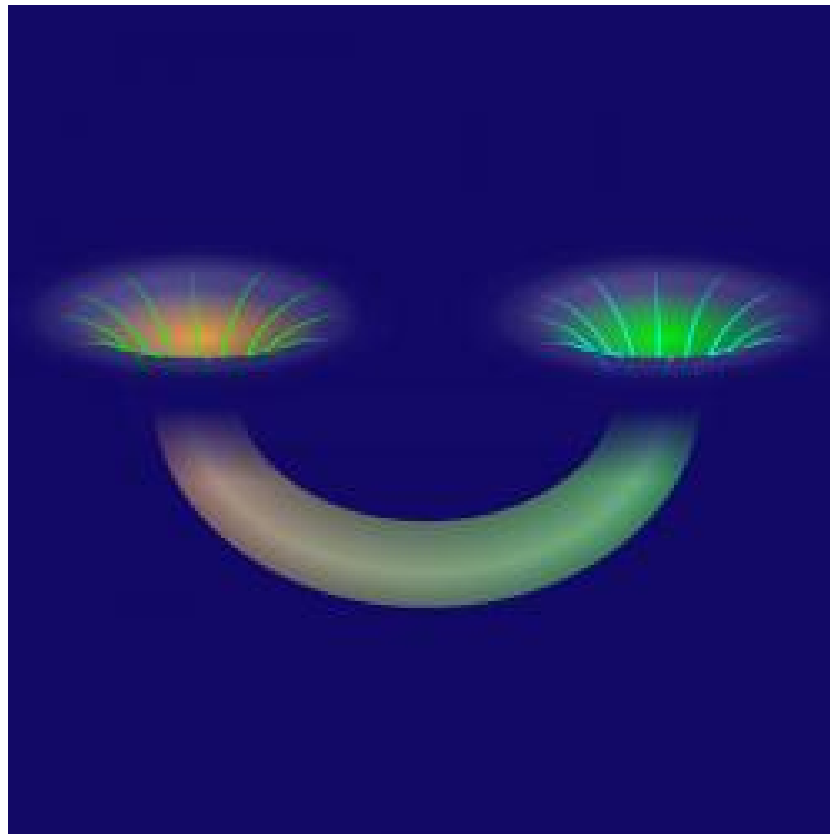


Einsteinův útok na kvantovou mechaniku:

- Einsteinův-Podolského-Rosenův paradox:
- Částice rozpadající se v EPR experimentu má nulový spin – oba vzniklé fotony se musí otáčet opačně
- Komunikace mezi fotony by musela být okamžitá rychlejší než světlo



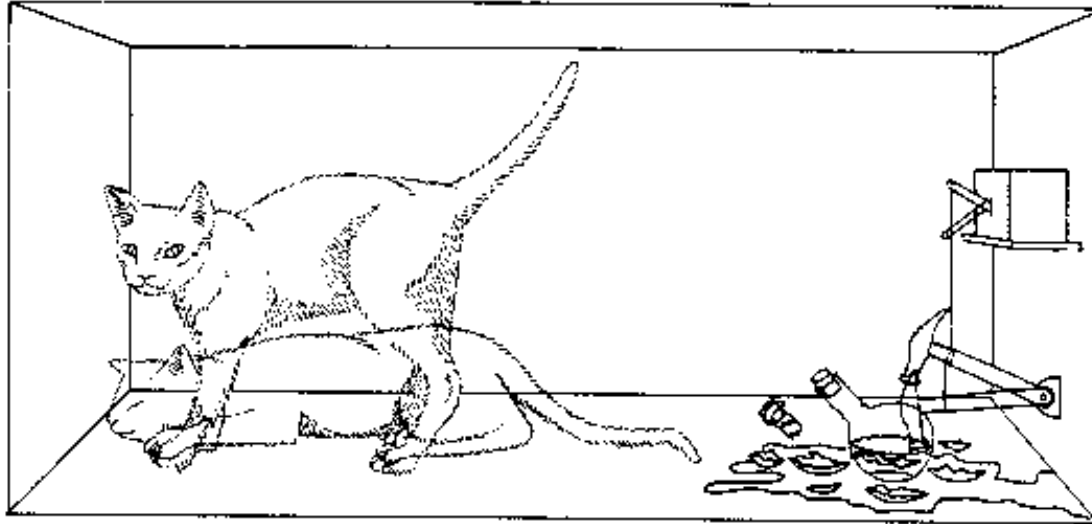
kvantové provázání jde o stav, kdy se změna jednoho systému okamžitě projeví na druhém systému, bez ohledu na jejich vzdálenost dvojici entanglovaných částic



Kvantové počítání

Kvantová superpozice.....

Schrödingerova kočka

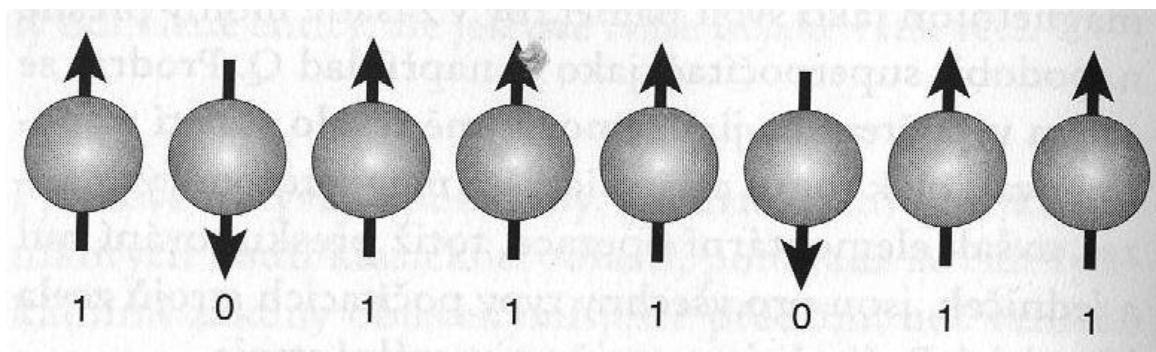


$$|\Psi\rangle = |\Psi_{alive}\rangle + |\Psi_{dead}\rangle$$

**Jestliže stav změříme víme
jedno nebo druhé**

Počet všech možných stavů deseti
kvantových částic:

Počet všech možných stavů deseti kvantových částic:



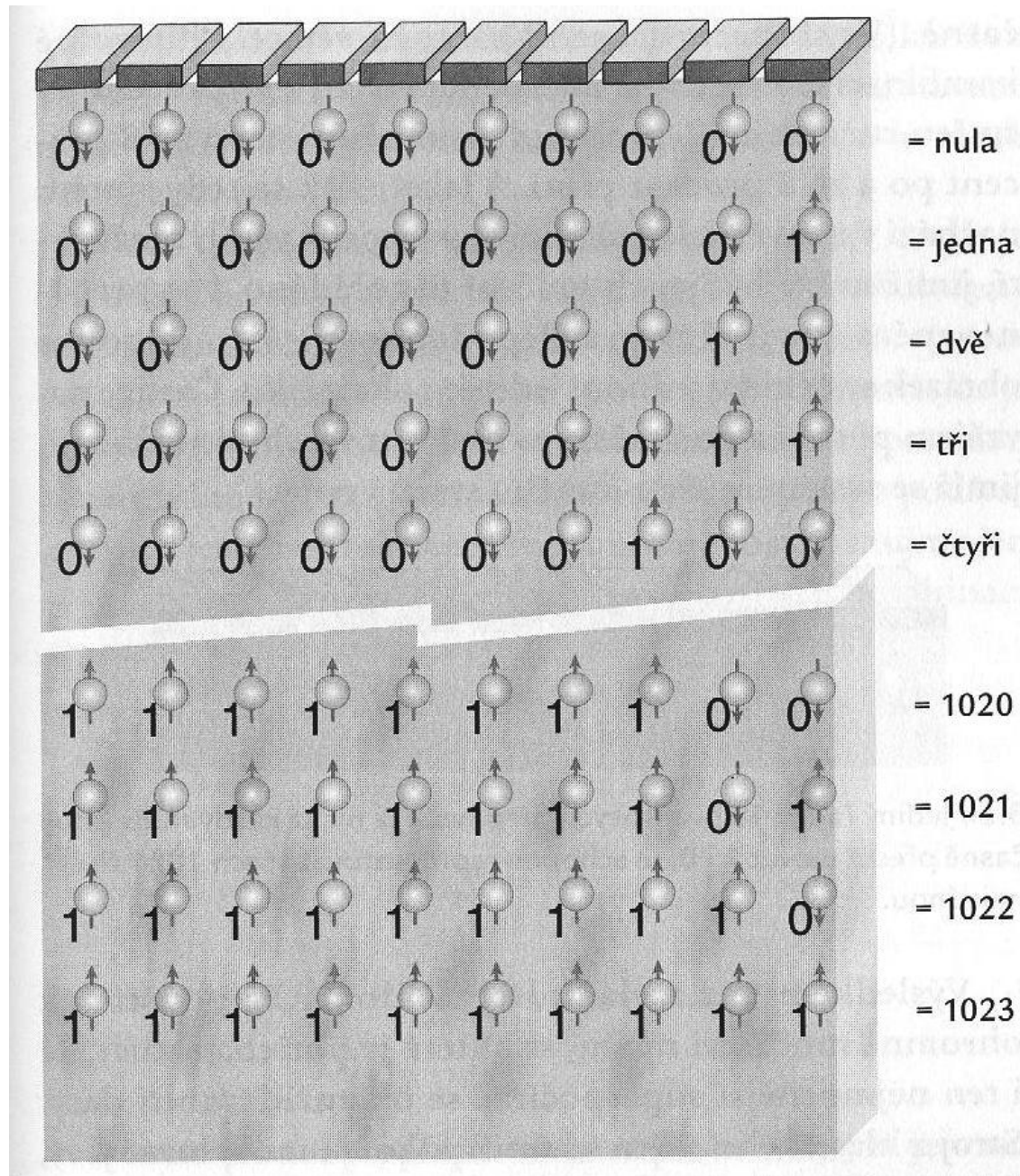
Ve dvou stavech: $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{10} = 1024$

1024 řádků procesoru

Dvanáct částic ... 4096 řádků

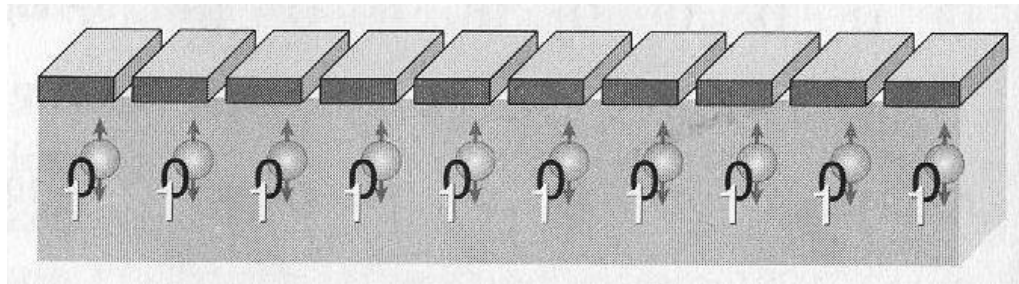
Dvacet částic ... 1 048 576

Čtyřicet částic ... zhruba bilion řádků



Unicorn College, Z. Zeinger:
Kvantové počítání

Ale kvantové částice Superpozice 0 a 1
..... Navzájem na sebe působí



Nezvladnutelná úloha i pro nejmocnější superpočítač

Ale co počítač, který by sám fungoval kvantově mechanicky ?
10 kvantových přepínačů – jeden pro každou částici

Řádek složený z n atomů může vyjadřovat 2^n čísel současně

Uvažujme jen 3 kvantové přepínače:

Existuje 8 možných kombinací tří bitů:

Nechť pouze přepínač zcela napravo v trojici je v superpozici, první dva jsou na nule,pak řádek představuje současně čísla 000 a 001.

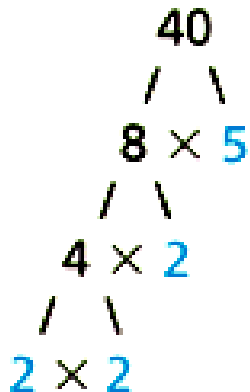
Je-li i prostřední přepínač v superpozici ... představuje současně 000, 001, 010 a 011.

Všechny tři v superpozici pak všech osm možností

000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

Klasický faktorizační algoritm

What is the prime factorization of 40?



So, $40 = 2 \times 2 \times 2 \times 5$.

Počet kroků 2^n

Kvantová faktorizace

Počet bitů: $N=2^n$

Počet kroků: n^2

příklad $n=10$

Kvantových kroků: 100

Klasických kroků: 10.000