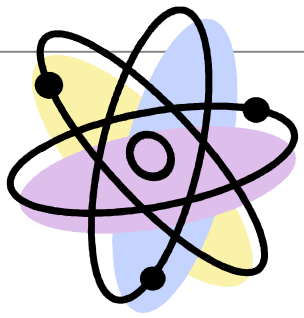
# Kvantové výpočty



I.Kolingerová

Obsah:

1. Hlavní myšlenka
2. Základní vlastnosti kvantové soustavy
3. Kvantová hradla
4. Použití

## 1. Hlavní myšlenka

- Idea kvantových výpočtů: R.Feynman, poč.80.let:
  - Časová náročnost numerické simulace vývoje kvantového systému roste exponenciálně s počtem stupňů volnosti tohoto systému (např. s počtem vzájemně interagujících částic)
  - Spontánní dynamika vhodně sestavené kvantové soustavy tedy může realizovat a podstatně urychlit určité numerické výpočty

2

## 2. Základní vlastnosti kvantové soustavy

- Superpozice stavů
- Změna stavu objektu kvantovým měřením
- Vzájemná provázanost/propletení

3

## Analogie: nákup kvantového auta

- 3 stavové 1b proměnné f,b,s: počet dveří, barva, sedan a-n
- Auto v obchodě pod plachtou, nikdo neví, jaké je (tj. v jakém z 8 možných stavů je)

- Stav např. dán výrazem 0.1[000]+0.2[001] +0.3[010]+0.4[011]+0.3[100]+0.6[101] +0.4[110]+0.3[111]

4

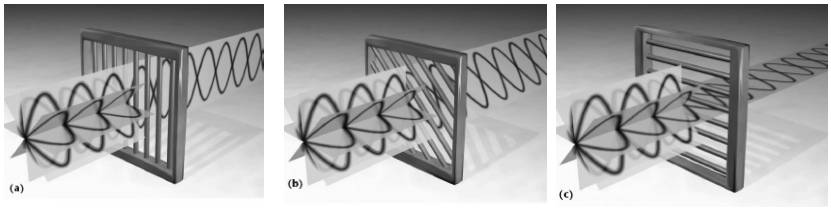
## Nákup kvantového auta

- Smíme auto i s plachtou posunout, ale ne se podívat
- Možnost predikce stavu podle pravděpodobností, pravděp. stavu je váha$^2$, suma pravd.=1
- Kvantové auto: je ve všech stavech najednou, ale když se podíváme pod plachtu, ocitne se jen v jednom stavu, v něm už zůstane - superpozice stavů + kvantové měření

5

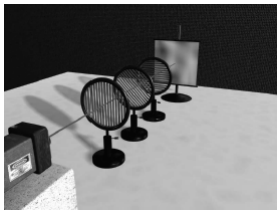
## Kvantové měření

- Experiment 1: pošleme fotony s různou polarizací polarizačním filtrem, projdou jen ty souhlasně orientované




6

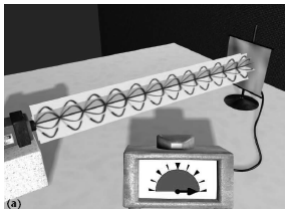
- Experiment 2: pošleme fotony s náhodnou polarizací (rovnoměrná pravděp.) třemi polarizačními filtry, úhel a množství dopadlých fotonů měříme na stínítku
- 5 kroků

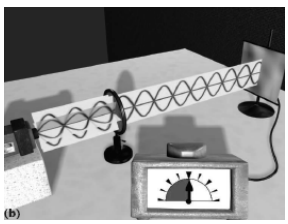




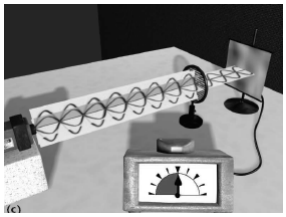


- Krok 1- změříme A jednotek
- Krok 2 - svislý filtr, změříme A/2 jednotek - foton je klasifikován jako svislý s pravděp.p ~ (sin jeho úhlu od svislice)$^2$ nebo jako vodorovný s 1-p
- Foton je měřením změněn (promítnut do jednoho ze stavů) a v nové konfiguraci zůstane

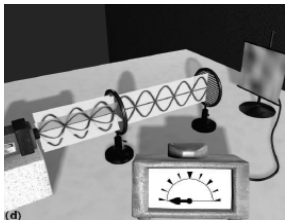


- Krok 3 - vodorovný filtr, opět A/2 jednotek



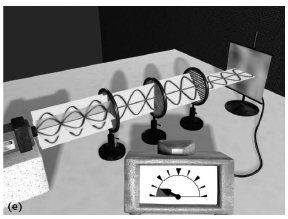
- Krok 4 - svislý, pak vodorovný filtr, 0 jednotek (z 1.filtru jen svislé fotony, neprojdou 2.filtrem)



9



- Krok 5 - mezi svislý a vodorovný vložíme 3.filtr v úhlu -45°, změříme A/8 jednotek !!!!!



1.filtr propustí A/2 svislých, 2. A/4 šikmých, 3. A/8 vodorovných

10

## Shrnutí experimentů

- Kvantová částice existuje zároveň v mnoha nekompatibilních stavech
- Ve stavu superpozice je možné působit na všechny stavy najednou
- Kvantové měření: když měříme kvant.objekt vzhledem k předem vybrané množině stavů, objekt se promítne do jedné z možností
- Když stejné pozorování zopakujeme, aniž jsme na částici nějak jinak působili, zůstane ve stejném stavu
- Částice a měřicí aparát určují možné stavy, které jsou výsledkem měření

11

## Bra-ketová notace

- Ket - sloupcový vektor komplex.čísel $|abc\rangle$
- Bra – řádk.vektor komplexně sdruž.hodnot $\langle abc|$
- Inner (dot) product: $\langle abc||def\rangle = \langle abc|def\rangle =$

  $= \boxed{\bar{a}d + \bar{b}e + \bar{c}f}$
- Outer product: $|def\rangle\langle abc| =$

  $= \boxed{\begin{matrix} d\bar{a} & d\bar{b} & d\bar{c} \\ e\bar{a} & e\bar{b} & e\bar{c} \\ f\bar{a} & f\bar{b} & f\bar{c} \end{matrix}}$

12

## Qubity

- Qubit – základní jednotka kvantových výpočtů, kvantová obdoba bitu, reprezentován ketem
- Základní stavy: $|0\rangle = [1\ 0]^T$ a $|1\rangle = [0\ 1]^T$
- Částice může být v obou stavech najednou, $q = c_0|0\rangle + c_1|1\rangle$, kde $c_0$ , $c_1$ jsou komplex.čísla, $|c_0|^2 + |c_1|^2 = 1$
- Měřením qubit přejde do stavu $|0\rangle$ s pravd. $|c_0|^2$ a $|1\rangle$ s pravd. $|c_1|^2$
- Realizace: 2 směry polarizace fotonů, 2 orientace spinu elektronů …

13

## Vícebitové registry

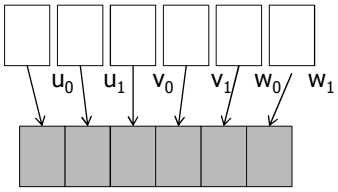
- Klasický registr vytváříme slepením bitů
- Kvantový registr vektorovým součinem bitů (vzniknou všechny kombinace složek v pořadí, v jakém jsou uvedeny)

$$U \otimes V = \{u_0,u_1\} \otimes \{v_0,v_1\} = \{(u_0,v_0),(u_0,v_1),(u_1,v_0),(u_1,v_1)\},$$
$$\dim(U \otimes V) = \dim(U) * \dim(V)$$

$$U \otimes V \otimes W = \{u_0,u_1\} \otimes \{v_0,v_1\} \otimes \{w_0,w_1\} = \{(u_0,u_0,w_0),$$
$$(u_0,u_0,w_1),(u_0,u_1,w_0),(u_0,u_1,w_1),(u_1,u_0,w_0),(u_1,u_0,w_1),$$
$$(u_1,u_1,w_0),(u_1,u_1,w_1)\}$$

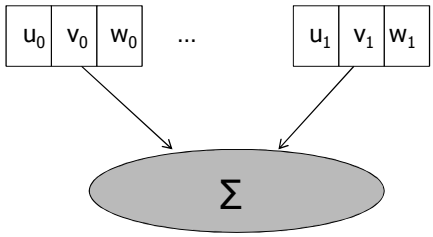
## Vícebitové registry

Klasický registr




Hodnoty $u_0$ .. $w_1$ mohou mít nezávislé váhy

3-qubitový register




Váhu může mít jen každá kombinace, všechny jsou najednou v jednom 3b registru

15

- Příprava qubitu: qubit dán do požad.stavu, pak registr místo vektor.součinu vytvořen jen slepením bitů
- Kopie qubitu-částice bez předchozího měření není možná;
- je možná v případě, že původní částice při kopírování zahyne

  => klonování ne, teleportace ano

16

## Propletení (entanglement)

- Př.: 2x2bit.registry
  $b_0$=|00>, $b_1$=|11>,β=w|00>+w|11>,w=1/√2
  Změříme jen 2.qubit, asi v 50% je 0, jinak 1
  Pokud zjistíme |0>, pak víme jistě, že v 1.qubitu také |0>
  Vlastně je stav neprohlédnutého bitu také promítnut, i když jsme si ho neprohlédli – tzv. propletení 2 qubitů registru β

17

## Překvapivé praktické aplikace

- Není časové omezené - částice jednou propletené tak zůstanou navždy
- Propletené bity nemusí ležet fyzicky blízko – klidně ve vzdálenosti celého vesmíru
- Změřením jedné částice změříme i ostatní s ní propletené – zároveň kolapsují do příslušného stavu
- Experiment Einstein-Podolsky-Rosen (EPR) –q0 z β si necháme, $q_1$ pošleme pryč rychlostí světla, po 10 mil. let se podíváme na $q_0$ a promítne se tím i $q_1$

18

## 3. Kvantová hradla

- Vhodná hradla pro kvant. výpočty musí být reverzibilní (vstup určitelný z výstupu) – většina existujících klasických není
- Př. reverzibilních hradel: $C_{not}$, Toffoli
- $C_{not}$:

| a (source) | b (target) | x | y |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

- a prochází nezměněno, b je XOR

19

Kvantová hradla

- Toffoli (3 drátové hradlo):

  x=a, y=b, z=c xor (a and b)
  (tj. **if** (x=1 and y=1) z=not c ; **else** z=c)

20

## Kvantové hradlo $C_{not}$

- 2-qubit. register α=0.5(|00>+ |01>+|10>+|11>), váhy stavů mohou obecně být různé
- $C_{not}$ změní váhy stavů vstupů, jako by je pronásobilo maticí

|00>->|00>
$C_{not}$: |01>->|01> =
|10>->|11>
|11>->(10>

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

21

## Kvantové hradlo Toffoli

|000>->|000>
|001>->|001>
|010>->|010>
T: |011>->|011>=
|100>->|100>
|101>->|101>
|110>->|111>
|111>->|110>

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

- Univerzální hradlo - lze sestavit lib. logiku pro kvantové výpočty

22

## Čistě kvantové hradlo

√NOT:

|0> -> 1/√2(|0>-|1>)
|1> -> 1/√2(|0>-|1>)

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

- Pokud na vstupu hradla qubit v čistém stavu, dostaneme zpět superpozici obou bází (čistá náhodnost)
- Pokud hradlo použijeme 2x, dostaneme inverzi původního qubitu $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

23

## 4. Použití

- Kvantový paralelismus: Kvantový stav je vlastně superpozice všech hodnot - výpočet se všemi hodnotami najednou!
- Obecně nelze oddělit dílčí stavy součástí kvantového systému
- Kvantový počítač - soustava určitého počtu qubitů, zvolenou posloupností fyzikál.operací se dostávají do superponovaných a provázaných kvantových stavů
- Tato posloupnost operací - hlavní součást kvantového algoritmu

24

## Použití

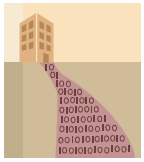
- Kvantové algoritmy složeny z elementárních operací, ovlivňují stav 1-2 qubitů
- Přečtení výsledku: formou měření, odhalí pouze nepatrnou řást kvant. informace a navíc stav nevratně zničí (z qubitu přečte jen Ano nebo Ne)
- Výsledky se nedají přesně předvídat - kvantová mechanika určuje pouze jejich pravděpodobnosti, nutno výpočet několikrát opakovat, výsledek z celkové statistiky
- I tak kvantové algoritmy někdy výrazně předčí klasické algoritmy

25

## Slavná aplikace

Faktorizace (tj. najít prvočísla, jejichž součinem je dané číslo), Shor, Bellovy laboratoře, 1994

- užitečné pro šifrování
- exponenciální problém
- kvant. výpočet vede k zásadnímu urychlení



26

## Kryptografie – kvantové posílání klíče (QKD)

- Potřebujeme mít jednorázový klíč stejný pro obě strany, kódovanou zprávu pak lze poslat veřejně
- Kódování a dekódování - XOR s klíčem
- QKD – vytvoření jednorázového klíče bezpečným způsobem, např. mějme polarizační filtr fotonů a dekodér
- Stejná polarizace filtru a dekodéru – bezpečně odlišíme ⟶ ↑
- Odlišná – náhodně cca 50% ⟶ a 50% ↑

27

## QKD

- A vygeneruje náhodný klíč (1), chce ho B bezpečně poslat
- Pro každý bit A náhodně vybere S nebo D orientaci polarizátoru (2), tím polarizuje klíč a veřejně pošle (3)
- B pro každý bit klíče náhodně nastaví dekodér (4)
- B s tímto nastavením změří klíč, dostane (5), pošle své nastavení (4) veřejně A
- A srovná s (2) a pošle veřejně info, kde uhodl (6)
- A a B zahodí bity, kde B neuhodl (7), zbytek bude klíč (8)

28

QKD

| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | S | S | D | S | D | D | D | S | D | D | S | S | D | S |
| 3 | → | → | ↖ | → | ↖ | ↖ | ↗ | ↑ | ↗ | ↗ | ↑ | ↑ | ↗ | ↑ |
| 4 | D | S | S | S | D | D | S | D | S | D | S | D | D | D |
| 5 | ↖ | → | → | → | ↖ | ↖ | ↑ | ↖ | ↑ | ↗ | ↑ | ↖ | ↗ | ↗ |
| 6 | x | o | x | o | o | o | x | x | x | o | o | x | o | x |
| 7 | | → | | → | ↖ | ↖ | | | | ↗ | ↑ | | ↗ | ↗ |
| 8 | | 0 | | 0 | 1 | 1 | | | | 0 | 1 | | 0 | 1 |

29

QKD

- Dá se čekat tak 50% úspěch
- Pak mohou A a B zkusit na krátké zprávě, zda OK a zda někdo neposlouchá (asi 25 % by bylo špatně)

- Špión chce zjistit řádek 3, přečíst a poslat B, aby A a B nic nepoznali
- Klonování nemožné, musí foton chytit, změřit, okopírovat do dalšího a poslat dál
- Špión nezná nastavení detektoru, takže asi 50% přečte a odešle špatně, úspěch B klesne na polovinu a špionáž se prozradí

30

## Fyzikální realizace kvant. počítače

- Zatím nic moc
- Př.: 1995 - teoreticky popsána soustava nabitých atomů v silně ochlazeném stavu držená ve vzáj, vzdálenosti několika mikronů silným elmg.polem, řízeno laser. impulsy
- Problém: udržet kvant.počítač po celou dobu výpočtu v naprosté izolaci anebo opravovat průběžně škody vzniklé interakcí
- 2001: Chuang, IBM, na bázi magnet.rezonance,
  7 qbitů, Shorův algoritmus, zatím velmi pomalé, pro praktické úlohy ještě nepoužitelné

31