# Úvod do kvantového počítání

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

10. března 2005

# O přednáškách



# Osnova dnešní přednášky

2 Proč kvantové počítání a počítače
- Problémy a složitosti
- Fyzikálně inspirovaný výpočetní model
- Realizace

3 Další alternativní modely
- DNA počítače

# Osnova dnešní přednášky

2. Proč kvantové počítání a počítače
   - Problémy a složitosti
   - Fyzikálně inspirovaný výpočetní model
   - Realizace

3. Další alternativní modely
   - DNA počítače

# Část I

# Přednášky

# Úvodní slovo k přednáškám

- Nové a zajímavé téma
- Aplikační oblast tvoří základ mé dissertace
- Možnost získání zápočtu z předmětu 36SP

## Čas a místo

- liché čtvrtky
- místnost K4

# Osnova přednášek

1. Proč kvantové počítání a počítače
2. Hilbertovy prostory, qubit, unitární vývoj
3. Kvantové registry
4. Kvantové obvody a reverzibilní brány
5. Deutschův problém
6. Shorův faktorizační algoritmus
7. Teleportace a superdense kódování
8. Kvantová distribuce klíců, protokol BB84

# Část II

# Dnešní přednáška

# Problémy a složitosti

## Klasický výpočetní model

Turingův stroj (TM) - Alan Turing (1912-1954)

form. gramatiky
RAM stroje
atd.
} Polynomiálně ekvivalentní s TM

# Problémy a složitosti

## Churchova teze

Problém je algoritmicky řešitelný, právě když je rekurzivní.
(= řešitelný pomocí TM)

Problémy

- rekurzivní
- nerekurzivní

# Problémy a složitosti

## Churchova teze

Problém je algoritmicky řešitelný, právě když je rekurzivní.
(= řešitelný pomocí TM)

Problémy

- rekurzivní
- nerekurzivní

# Problémy a složitosti

## Silná Churchova teze

Problém je řešitelný v polynomiálním čase, právě tehdy když je v polynomiálním čase řešitelný na TM.

Problémy:

- zvládnutelné (polynomiálně omezené) - P, BPP
- nezvládnutelné - NP

# Problémy a složitosti

## Silná Churchova teze

Problém je řešitelný v polynomiálním čase, právě tehdy když je v polynomiálním čase řešitelný na TM.

Problémy:

- zvládnutelné (polynomiálně omezené) - P, BPP
- nezvládnutelné - NP

# Výpočetní model založený na kvantové mechanice

Kvantová mechanika:

- Fyzika malých částic
- Masivní paralelismus
- Propletení kvantových stavů (entanglement)
- Měření je nedeterministické

# Výpočetní model založený na kvantové mechanice

Applikační oblasti:

- Zrychlení klasických algoritmů
  - Shorův faktorizační algoritmus
  - Groverův vyhledávací algoritmus
- Kvantová kryptografie
  - Kvantová distribuce klíčů
  - Generování náhodných čísel
- Kvantová teleportace

# Výpočetní model založený na kvantové mechanice

Applikační oblasti:

- Zrychlení klasických algoritmů
  - Shorův faktorizační algoritmus
  - Groverův vyhledávací algoritmus
- Kvantová kryptografie
  - Kvantová distribuce klíčů
  - Generování náhodných čísel
- Kvantová teleportace

# Výpočetní model založený na kvantové mechanice

Applikační oblasti:

- Zrychlení klasických algoritmů
  - Shorův faktorizační algoritmus
  - Groverův vyhledávací algoritmus
- Kvantová kryptografie
  - Kvantová distribuce klíčů
  - Generování náhodných čísel
- Kvantová teleportace

# Fyzická realizace

Libovolný 2-dimenzionální kvantový systém

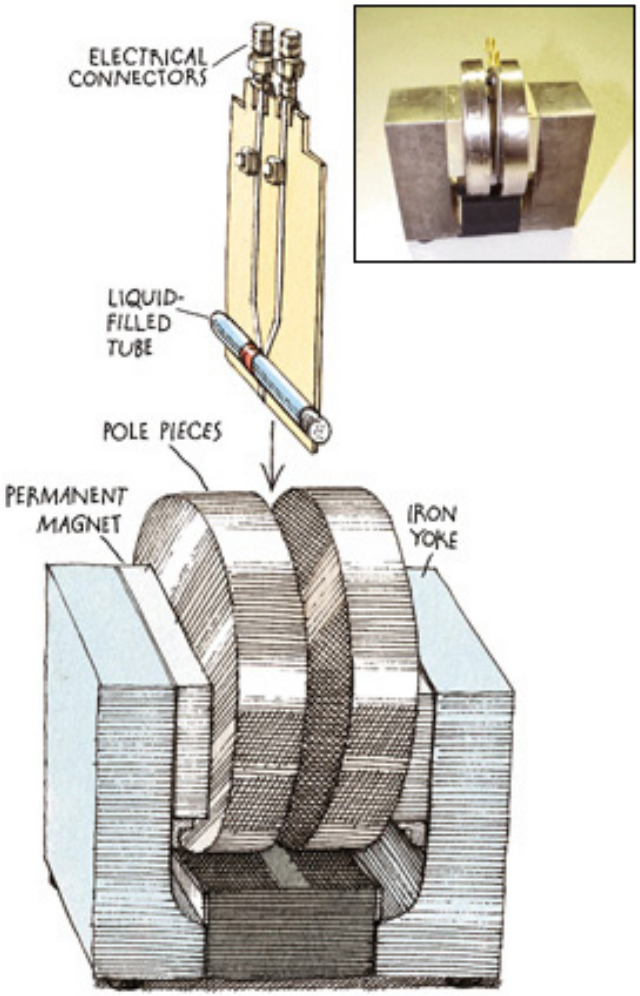
- polarizace fotonu
- 1/2 spinový moment částice

Používané technologie

- Ion trap
- Cavity QED
- NMR

# Nukleárná magnetická rezonance (NMR)

## Obecné schéma kvantového počítače s NMR technologií



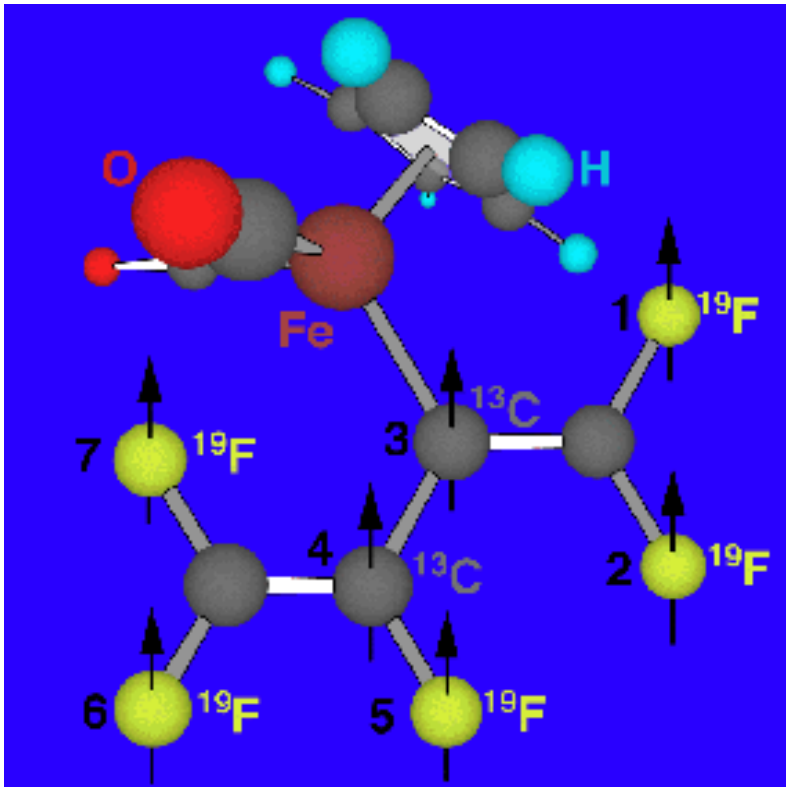



# 7-qubitový systém od IBM

Na tomto 7-qubitovém systému bylo faktorizováno číslo 15


# pentafluorobutadienyl cyclopentadienyldicarbonyl-iron complex

- 1 molekula $\rightarrow$ 1 počítač
- přibližně použito $10^{20}$ molekul



2 Proč kvantové počítání a počítače
- Problémy a složitosti
- Fyzikálně inspirovaný výpočetní model
- Realizace

3 Další alternativní modely
- DNA počítače

# DNA počítače

## Deoxyribonukleová kyselina - DNA

- dva řetězce prostorově uspořádané do šroubovice
- složená z nukleotidů obsahujících dusíkovou bázi
  - adenin - A
  - thymin - T
  - cytosin - C
  - guanin - G
- spojení možné pouze mezi A-T a C-G
- nukleotidy jsou orientované

# DNA počítače

## Deoxyribonukleová kyselina - DNA

- dva řetězce prostorově uspořádané do šroubovice
- složená z nukleotidů obsahujících dusíkovou bázi
  - adenin - A
  - thymin - T
  - cytosin - C
  - guanin - G
- spojení možné pouze mezi A-T a C-G
- nukleotidy jsou orientované

# DNA počítače

## Deoxyribonukleová kyselina - DNA

- dva řetězce prostorově uspořádané do šroubovice
- složená z nukleotidů obsahujících dusíkovou bázi
  - adenin - A
  - thymin - T
  - cytosin - C
  - guanin - G
- spojení možné pouze mezi A-T a C-G
- nukleotidy jsou orientované

# DNA počítače

## Deoxyribonukleová kyselina - DNA

- dva řetězce prostorově uspořádané do šroubovice
- složená z nukleotidů obsahujících dusíkovou bázi
  - adenin - A
  - thymin - T
  - cytosin - C
  - guanin - G
- spojení možné pouze mezi A-T a C-G
- nukleotidy jsou orientované

# DNA počítače

## Adlemanův experiment

Existence Hamiltonovské cesty v orientovaném grafu
! NP-úplný problém !

Algoritmus (nedeterministicky polynomiální):

1. generuj náhodně cesty v grafu
2. zjisti zda nějaká cesta začíná a končí v požadovaném bodě grafu
3. zjisti zda je délky požadované délky
4. zjisti zda obsahuje všechny vrcholy
5. výstup ano/ne