Kvantové algoritmy a bezpečnost

Václav Potoček

Osnova

- Úvod: Kvantové zpracování informace
- Shorův algoritmus
- Kvantová distribuce klíče
- Post-kvantové zabezpečení

Úvod

Kvantové zpracování informace

- Kvantový počítač: hypotetický stroj využívající kvantovou mechaniku k řešení algoritmických úloh
- R. Feynman 1982: klasické počítače nepostačují k simulacím kvantových systémů, simulátor musí být také kvantový systém
- Kvantové počítače umožňují překonat hranice efektivity klasických počítačů
  - → Kvantové varianty teorie informace a složitosti

Úvod

Kvantové zpracování informace

- Zpracování informace: kvantová mechanika nahrazuje binární logiku
- Nuly a jedničky → stavy fyzikálního systému
- Řízený výpočet → řízený časový vývoj

Úvod

Kvantové zpracování informace

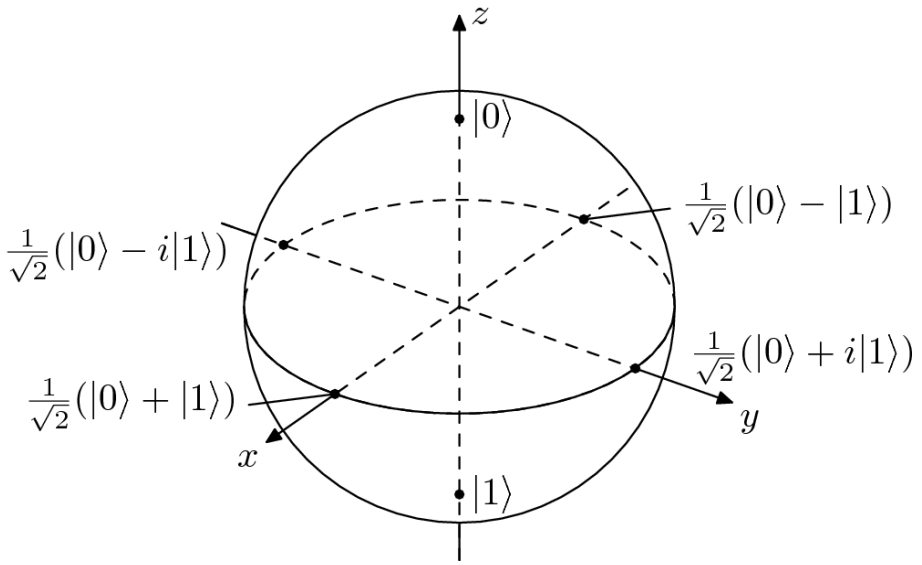
- Základní principy:
  - Stavový prostor: Hilbertův prostor
  - Časový vývoj: libovolná unitární operace

    → princip superpozice
  - Měření: pravděpodobnostní charakter

Úvod

Kvantové zpracování informace

- Jednotka kvantové informace: qubit
  - Systém se dvěma bázovými stavy: $|0\rangle$, $|1\rangle$
  - Libovolné superpozice: stavy „mezi“ 0 a 1
- N qubitů: exponenciálně rostoucí dimenze



Úvod

Kvantové zpracování informace

- Kvantové měření:
  - Výsledkem je klasická informace
  - Příklad: $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
  - Měření ve „výpočetní bázi“ dá výsledky 00, 01, 10 či 11 s pravděpodobnostmi úměrnými $|\alpha_{00}|^2$ až $|\alpha_{11}|^2$
  - Stav se po měření změní a není možné jej „zálohovat“

Úvod

Kvantové zpracování informace

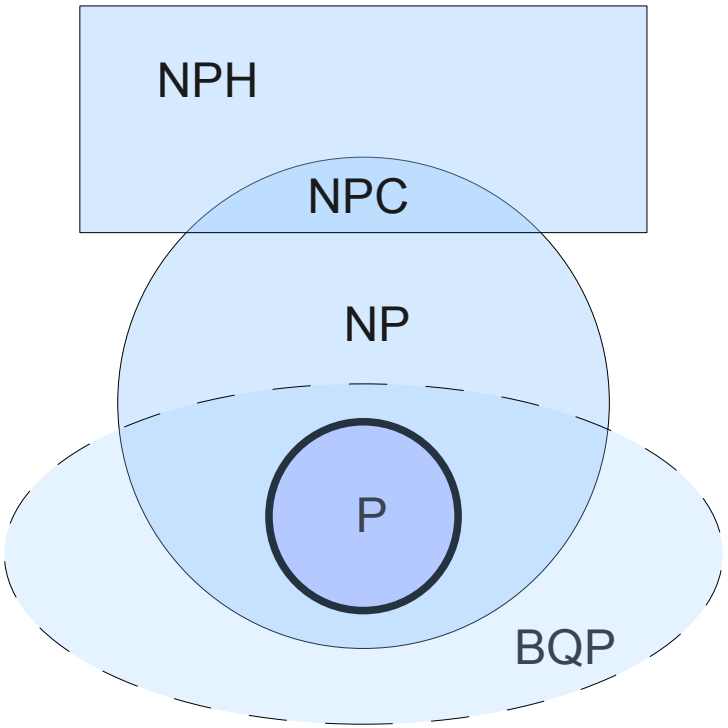
- Obtíže kvantového počítání:
  - Nedává zrychlení oproti klasickému počítání „samo o sobě“
  - Všechny algoritmy musejí být reverzibilní
  - Komplikovaná příprava vstupních stavů
  - Není možné deterministické měření stavu ani jeho opakování pro upřesnění
- I přesto mohou kvantové algoritmy dosahovat efektivity nedosažitelné pro klasické počítače

Úvod

Kvantové zpracování informace

- Třídy složitosti pro rozhodovací problémy:

(Hypotéza: BQP ∩ NPC = ∅)



Shorův algoritmus

aneb Jak kvantová informace pomáhá dešifrovat

- P. Shor, 1994: polynomiální kvantový algoritmus (časová složitost $O((\log N)^3)$) pro faktorizaci celých čísel a pro diskrétní logaritmus
- Dosud známé algoritmy: exponenciální složitost
- Bezprostřední ohrožení většiny současných kryptosystémů s veřejným klíčem, jakmile by kvantové počítače byly dostupné
- 2001: experimentální realizace se 7 qubity – umožňuje faktorizovat čísla do 2^4

Shorův algoritmus

aneb Jak kvantová informace pomáhá dešifrovat

- Princip: faktorizujme N
  1. Zvolíme náhodné $a < N$
  2. Spočítáme gcd(a, N) – pokud je ≠ 1, máme dělitel
  3. Sestavíme posloupnost (a^x mod N) a nalezneme její periodu r
  4. Pokud je r liché nebo $a^{r/2} = -1 \pmod{N}$, opakujeme
  5. Jinak: gcd($a^{r/2} - 1$, N) je netriviální dělitel N

Shorův algoritmus

aneb Jak kvantová informace pomáhá dešifrovat

- Shor: kvantový počítač umí najít periodu posloupnosti pomocí diskrétní Fourierovy transformace v kvadratickém čase
  (z hlediska počtu použitých atomárních operací)
- Po přičtení času potřebného k přípravě stavu, včetně opakování algoritmu v případě neužitečného výsledku, stále polynomiální
- Faktorizace čísel $\in$ BQP
- Další důsledek: Diskrétní logaritmus $\in$ BQP

Kvantová distribuce klíče

aneb Jak kvantová informace pomáhá šifrovat

- Myšlenka distribuce klíče: přeneseme pouze jednorázový náhodný klíč, který neobsahuje žádnou informaci
- Když klíč znají obě strany, použije se Vernamova šifra ($c = m \oplus k \;\rightleftarrows\; m = c \oplus k$)
- Jestliže je bezpečnost přenosu klíče ohrožena, zahodíme jej a opakujeme v jiných podmínkách

Kvantová distribuce klíče

aneb Jak kvantová informace pomáhá šifrovat

- Jak zajistit bezpečnost přenosu klíče: využít vlastností kvantového měření
- Bennett, Brassard 1984: protokol QKD nenapadnutelný díky samotným fyzikálním zákonům
- 2004: první komerciální využití pro komunikaci mezi bankami, 2007: elektronické volby

Kvantová distribuce klíče

aneb Jak kvantová informace pomáhá šifrovat

- Alice generuje dvě náhodné posloupnosti a vysílá qubit v jednom ze čtyř stavů:
  - 00 ... $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$
  - 01 ... $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$
  - 10 ... $(|0\rangle + |1\rangle)/\sqrt{2} = |+\rangle$
  - 11 ... $(|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle$
- Bob si vybírá náhodně jednu z těchto bází, ve které měří
  - Stejná báze – získá bit, který Alice vyslala
  - Odlišná báze – získá náhodný výsledek (50:50)

Kvantová distribuce klíče

aneb Jak kvantová informace pomáhá šifrovat

- A a B si po měření sdělí (veřejně) báze: kde se shodovali, takové „datové“ bity použijí
- Na vzorku vyzkouší spolehlivost přenosu
- Případný odposlouchávač nenávratně způsobuje ztrátu informace – projeví se nárůstem chybovosti o 25%
- Pokud je chybovost menší než 25%, A a B mají jistotu, že nikdo jiný zaručeně jejich klíč nezná

Post-kvantové zabezpečení

aneb Jak se kvantovému dešifrování bránit na PC

- Existují i klasické kryptosystémy odolné kvantovým algoritmům
- Příklad: McEliece 1978 – algoritmus založený na NPH problému, odolný (Dinh et al. 2010) vůči variantám Shorova algoritmus

Post-kvantové zabezpečení

aneb Jak se kvantovému dešifrování bránit na PC

- Princip: obecný korekční kód
- Přenos informace chybovým kanálem: kódy korigující chyby
- Jestliže daný jednoduchý kód „promícháme“, je obecně NP-těžkou úlohou jej dekódovat
- Lepší bezpečnost než u ostatních současných systémů za cenu většího sdíleného klíče
- Podle hypotézy: $BQP \cap NPH = \emptyset$

Post-kvantové zabezpečení

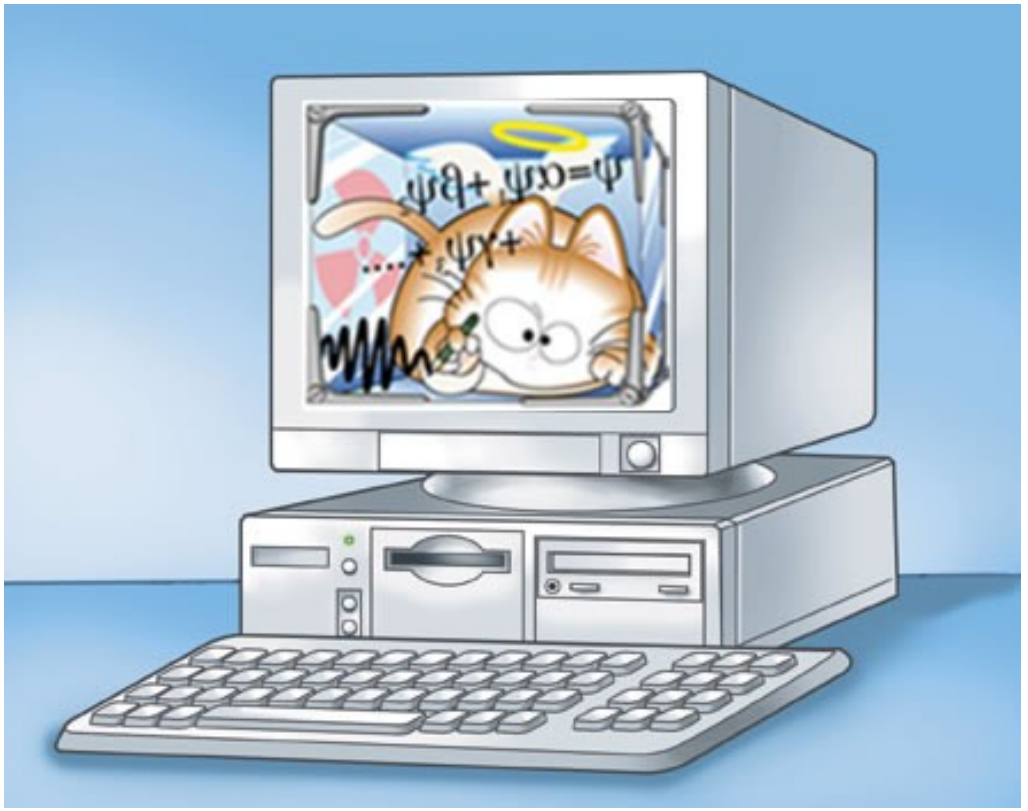
aneb Jak se kvantovému dešifrování bránit na PC

- Kód generovaný maticí G: řádky = kódová slova vzdálená o d bitů, snadné dekódování ze znalosti nulového prostoru, korekce t chyb
- McEliece: sestaví matici $G' = SGP$, kde S je invertibilní, P permutační matice
- A: veřejný klíč: (G', t), soukromý klíč: (S, G, P)
- B: k zakódování použije G' a ještě uměle přidá t náhodných chyb
- A: aplikuje P^{-1}, dekódování, opravu a S^{-1}

Shrnutí

- Kvantové počítače dovedou některé úlohy řešit efektivněji než klasické (až exponenciální urychlení)
- Běžné využití dosud nerealistické, pokud však ano, RSA není bezpečné
- Kvantová distribuce klíče však již dostupná i komerčně
- I klasické šifrování může být vůči kvantovému dešifrování odolné

Děkuji za pozornost.



[1] Shor, P.W., Proc. 35th Annual Symposium on Foundations of Computer Science (1994), dostupné na arXiv:quant-ph/9508027v2 (1995)
[2] Bennett, C.H. and Brassard, G., Proc. IEEE Int. Conf. On Computers, Systems, and Signal Processing (1984)
[3] McEliece,R.J., DSN Progress Report 42-44: 114 (1978)

Václav Potoček, vaclav.potocek@fjfi.cvut.cz