Kvantové počítače

Michal Čermák – SPŠ Jihlava (MisaCermak@seznam.cz)
Kamil Kos – Arcibiskupské gym. Praha 2 (kamilkos@email.cz)
Jan Olšina – gym. Kroměříž (irigi@centrum.cz)
Zbyněk Sopuch – Masarykovo gym. Příbor (jarpen@centrum.cz)
Václav Uher – gym. Břeclav (wexx@seznam.cz)

Abstrakt:

Práce se snaží přiblížit problematiku kvantových počítačů. Na srovnání s klasickými počítači ukážeme rozdíly a podobnosti v jejich filosofiích. Pomocí jednoduchých příkladů objasníme základní principy kvantové mechaniky, na nichž je postavena jejich funkce.

1 Úvod

První nápady sestrojit kvantový počítač se objevily na počátku 80. let (Richard Feynman), ale zvýšený zájem se datuje od roku 1994, kdy Peter Shor z Bellových laboratoří přišel s kvantovým algoritmem pro faktorizaci velkých čísel na prvočísla. Největším úspechem na tomto poli je zatím sestrojení pětiqubitového kvantového počítače firmou IBM (2000).

Co stojí v pozadí snahy realizovat kvantový počítač? Co se slibujeme od jeho sestrojení? Hlavní výhodu tvoří kratší doba výpočtu některých matematických úloh, neboť se ukazuje, že při jejich řešení klasickými algoritmy roste časová náročnost exponenciálně s velikostí vstupu, zatímco u kvantových algoritmů jen polynomiálně.

2 Odlišnosti kvantového počítání

Pokusme se nejdříve sjednotit naše představy o tom, jakým způsobem fungují se realizují matematické algortimy na počítačích. Na počatku každého počítání stojí příprava předem určeného výchozího stavu (v případě klasických počítačů je to inicializace registru), na kterém se poté provádí logické operace. Po ukončení algoritmu je možno odečíst výsledek.

Kvantový počítač se v tomto ohledu od výše zmíněného schematu nijak neliší. Hlavní rozdíl spočívá v použití kvantových systémů. Oproti klasickým počítačům, které informace kódují pomocí bitů (stavy mající hodnotu 0 nebo 1), používají kvantové počítače tzv. kvantové bity – qubity. Jak může vypadat kokrétní fyzikální realizace qubitu? Je nutné vybrat fyzikální systém charakterizovaný dvěma stavy. Příkladem takového systému může být foton se dvěma navzájem kolmými polarizacemi, elektron se dvěma možnými hodnotami spinu nebo atom se základním a excitovaným stavem elektronu. Kvantový registr potom můžeme definovat jako soubor rozlišitelných qubitů.

3 Základní principy

Podívejme se, v čem se tyto stavy liší od klasických.

(I) *Superpozice*: Z naší běžné zkušenosti jsme zvyklí, že objekt nacházející se v daném místě se nemůže současně vyskytovat na místě jiném. Toto tvrzení je opřeno o naše pozorování makroskopických objektů a není v souladu s tím, co měříme, přesuneme-li svou pozornost na objekty podstatně menší. Tyto mikroskopické objekty se řídí principy kvantové mechaniky, která popisuje částici vlnovou funkcí ψ. Tato vlnová funkce vyjadřuje pravděpodobnost výskytu částice v daném intervalu <x,x+dx>×<y,y+dy>×<z,z+dz> vztahem:

$$p(x,y,z) = |\psi(x,y,z)|^2 \, dxdydz$$

Jinými slovy to znamená, že se částice nachází v tzv. superpozici polohových stavů. (V jistém smyslu se částice nachází na více místech současně). Principem superpozice se však řídí všechny měřitelné veličiny (hybnost, spin).

Co to tedy znamená pro kvantovou obdobou klasického bitu – qubit? Tento se může nacházet nejen ve stavech |1> nebo |0>, ale i v jejich libovolné superpozici.

$$|u\rangle = \alpha\,|1\rangle + \beta\,|0\rangle,$$

kde α, β jsou komplexní konstanty splňující normovací podmínku $\alpha^2 + \beta^2 = 1$.

V čem vlastně spočívá hlavní význam superpozice pro kvantové počítání? Chceme-li provést výpočet pro různé nastavení registru, musíme u klasického počítače zopakovat výpočet pro každé nastavení. Naproti tomu kvantový registr nám umožňuje uvést jej do superpozice těchto nastavení, a provést tento výpočet pro všechna nastavení najednou.

(II) *Interference*: Fyzikálně je výpočet realizován určitou soustavou částic, které mají vlnové vlastnosti – mohou tedy spolu interferovat. Pro některé výpočetní cesty tedy může dojít k vzájemnému vyrušení částic, nebo naopak jejich zesílení (což se dá využít v některých kvantových algoritmech).

(III) *Provázání*: Dalším důležitým rysem kvantových systémů je tzv. provázání. Jedná se o velice zvláštní typ korelace mezi částicemi, který nemá v klasickém světě analog. Navzdory tomu jde skutečně o efekt, který se dá prokázat.

(IV) *Princip neurčitosti*: Máme-li systém v neznámém stavu, nemůžeme jej bez narušení změřit. V klasickém počítači můžeme změřit stav určité části registru a zkopírovat jej do určité jiné části registru. V případě kvantového registru reprezentovaného kvantovým stavem však platí věta, podle níž nelze tento registr zkopírovat. Navíc do systému nelze nijak zasahovat, protože jakékoliv měření průběh výpočtu naruší (každý qubit získá konkrétní stav a superpozice se zruší). Proto při technické realizaci je třeba zabezpečit izolaci proti působení vnějších vlivů.

4 Reprezentace logických operací na stavech kvantového registru

Vytváříme-li v klasickém počítači libovolné algoritmy, využíváme k tomu dílčích logických operací s bity (NOT, AND, OR, ...) Tento princip je zachován i pro kvantové počítače. Logické operace jsou představovány určitými operátory působícími na skupiny qubitů. Z principů kvantové mechaniky plyne, že operátory musí být unitární (tzn. mají-li vstupující qubity jednotkovou normu – splňují $\alpha^2 + \beta^2 = 1$, mají vystupující qubity také jednotkovou normu), tedy jsou i reverzibilní (tzn. z vystupujících qubitů musí být možné určit, jaké byly vstupní qubity). Proto je reprezentace logických operací u kvantových počítačů složitější než u klasických.

Příklad:

Klasická operace NAND (not AND) je definována jako:

00 – 1

01 – 1

10 – 1

11 – 0

Vidíme, že tato operace není reverzibilní (z výsledku nemůžeme určit vstup, neboť pro výstup 1 existují 3 možné vstupy). Proto tato operace nemůže být definována unitárním operátorem na qubitech. Proto se tato operace definuje tzv. Toffoliho bránou:

000 – 000

001 – 00**1**

010 – 010

011 – 01**1**

100 – 100

101 – 10**1**

110 – 111

111 – 11**0**

Na vstupu do Toffoliho brány vložíme dva qubity, jejichž operaci NAND počítáme a na třetí qubit vložíme hodnotu 1 (zajímají nás tedy jen ty trojice qubitů, které mají třetí qubit roven 1). Ve výstupu určí třetí qubit hodnotu NAND. Snadno se přesvědčíme, že je operace reverzibilní – dá se ukázat, že je i unitární.

5 Shrnutí

Kvantové počítání je v současnosti již značně rozvinutým vědním oborem. Problém spočívá ve velmi složité technické realizaci kvantových počítačů a také ve faktu, že pro každý algoritmus je nutné sestavit jiný kvantový počítač. Zatímco nejsložitější kvantový počítač má v současnosti velikost registru 5 qubitů, pro praktickou použitelnost by bylo třeba dosáhnout alespoň hranice 100 qubitů

Poděkování

Děkujeme především Ing. Jaroslavu Novotnému za uvedení do problematiky, cenné rady, neuvěřitelnou trpělivost a poskytnutý čas.

Rovněž děkujeme doc. Ing. Igoru Jexovi, DrSc. za poskytnutí literatury a konzultaci v dané problematice.

Děkujeme FJFI CVUT za zajištění materiálního zázemí.

Reference:

[1] BENETT, CHARLES H.: *Quantum Information and Computation* Physics Today october 1995, pp. 24–25

[2] EKERT, ARTHUR: *Quantum Interferometers as Quantum Computers* Physica Scripta, 1998, pp. 218–222

[3] MOTL, LUBOŠ: *Nejvýkonnější kvantový počítač od IBM,* www.scienceworld.cz,2001