

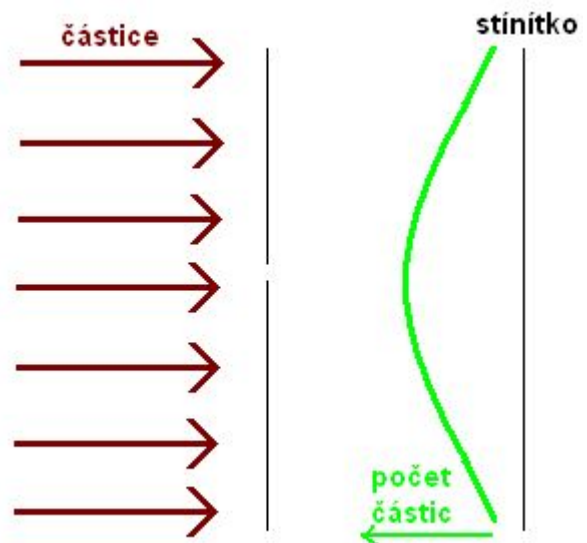
Kvantové počítače

Jeden z nejznámějších zákonů informatiky tzv. Mooreův zákon se v příštích 20 letech dostane do velkých potíží. Předpovídá totiž, že se každých 18 měsíců zdvojnásobí výpočetní síla počítačů. Zatím toho dnešní firmy dosahují stálou miniaturizací součástek použitých na stavbu počítače. Tímto směrem nebude moci jít stále, protože architektura počítačů podle Johna von Neumanna je stará padesát let a jistě do 20 let narazí na velmi tvrdou hranici - fyzikální zákony. Výpočetní součástka nemůže být menší než molekula a zákony makrosvěta, o které se současná architektura opírá, při dalším zmenšování brzy přestanou platit.

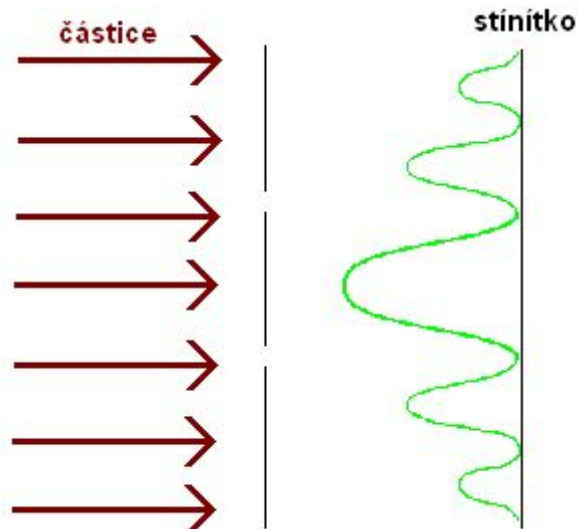
Proto se hledají jiné alternativy. Totální změna architektury bude velmi obtížná, protože má spojitě nahradit tu současnou. Několika variantami jsou například DNA počítače a počítače kvantové. První zmiňované se o něco více podobají těm současným, protože stále využívají plný determinismus avšak na jiném stavebním materiálu.

Druhé zmiňované, o kterém bych se chtěla hlavně zmínit, mají úplně jinou filosofii.

Tuto filosofii bych chtěla přiblížit na příkladu z kvantové fyziky. Máme desku se štěrbinou, na kterou dopadají fotony, a za ní stínítko (např. fotografický papír). Provedeme experiment s jednou štěrbinou a vše dopadne podle našich představ, pod štěrbinou fotonů dopadlo nejvíce. Stejně by dopadla situace v makrosvětě.



Problém nastane pokud uděláme do desky štěrbinu dvě. Pak nastane něco, co nemá v makrosvětě vhodnou analogii. Pro foton se vžila velmi laická představa kuličky, která je velmi zavádějící. Můžeme si jí ale nahradit kuličkou hozenou do vody, má totiž vlnový charakter. Částice vlastně interferuje sama se sebou, prochází



oběma štěrbinami zároveň. Tento jev se nazývá kvantový paralelismus.

V klasických počítačích je nějaká součástka ve stavu logické 1 nebo (=exclusive or) logické 0 a můžeme tuto hodnotu vždy přečíst a znovu použít. V kvantových počítačích se používá jako nosič hodnoty nějaká částice a hodnota 0 a 1 může být třeba spin (nebo normální a excitovaný stav). Tato částice se nachází ve stavu tzv. superpozice, ve stavu 1 i 0 a všech jejich lineárních kombinacích. Pro tyto jednotky se vžil název kvantový bit, tzv. qubit. V čem vlastně tkví ta výhoda? Pokud v klasickém algoritmu potřebujeme pro řešení úlohy projít všechny možnosti a pro ty něco zjistit. Musíme postupně (sériově) projít jednu po druhé. Složitost tohoto problému je 2^n , kde n je délka slova z množiny $\{0,1\}$. Již pro relativně malá n je to reálně neproveditelné. A právě pro takovou úlohu je kvantový počítač výborný. Má totiž paralelismus zabudovaný ve své podstatě. A takováto úloha se stává řešitelnou.

Zní to pro laika velmi jednoduše, ale s konstrukcí takového počítače je spojeno tolik problémů, které se mohou ukázat nepřekonatelnými. Kvantový počítač je velmi citlivý na vnější podmínky. Jen například přečtením hodnoty se stav superpozice úplně zborší a musí se znovu reinitializovat.

V praxi se zatím podařilo zapojit pouze pět qubitů. Počítač sestrojila firma IBM ve spolupráci s Stanfordovou univerzitou v Kalifornii a s Univerzitou v Calgary. Tato zpráva byla oznámena v polovině srpna roku 2000.

Největším úspěchem kvantového počítače je zatím faktorizace čísla 15 na $5 \cdot 3$, což počítači trvalo půl minuty. To dokazuje, že tento vývoj je stále ve svých počátcích.

Co zapříčinilo takový zájem o kvantové počítače? V roce 1994 přišel Peter Shor z Bellových laboratoří s algoritmem pro rozklad čísel na prvočísla v polynomiálním čase (pro neexistující kvantový počítač). Existence takového algoritmu pro klasické PC by otřásla celým světem. Snad většina používaných šifrovacích metod (RSA, Diffie-Hellman) používá tzv. jednocestné algoritmy. Jednocestný znamená, že průchod z první na druhou stranu (zakódování) je polynomiální a dekodování (bez dalších znalostí) je otázkou času exponenciálního. Taková úloha je právě vynásobení prvočísel na jedné straně a faktorizace velkého čísla na straně druhé.

Konstrukcí dostatečně výkonného kvantového počítače (stovky qubitů) sice padnou snad všechny dnes používané šifry, ale na druhou stranu by umožnil vyvinutí metod proti těmto počítačům odolných. První návrh pochází od Ch. Bennetta a G. Brassarda z roku 1982, kteří v roce 1989 zkonstruovali i první prototyp používající metodu tzv. kvantové distribuce klíče. Ohromnou výhodou této metody je, že zůstane odolná bez ohledu na další technický pokrok. Touto metodou se zabývá také česká vědecká skupina okolo prof. Jana Peřiny ve výzkumném centru pro optiku v Olomouci.

Dalším zajímavým použitím kvantové technologie je generátor náhodných čísel, tento generátor má velkou míru náhodnosti a lze připojit k PC přes paralelní port.



Podle mého názoru mají kvantové počítače budoucnost, ale nestanou se dalšími PCčky, budou to počítače v pozadí, které možná nahradí dnešní serverové počítače. A velmi mě zajímá, jak se návrháři hardwaru vyrovnají s další nemožností zmenšovat součástky.

ZDROJE

<http://akademon.cz/source/qcom.htm>

http://www.inzine.cz/clanok.asp?id_clanok=1226

<http://hron.fei.tuke.sk/~matak/zfiles/frame.htm>

<http://cml.fsv.cvut.cz/~kupca/qc/node4.html>

<http://fyztyd.fjfi.cvut.cz/cd/prispevky/sbpdf/kvanpoc.pdf>

<http://artax.karlin.mff.cuni.cz/~zivns9am/download/kv.doc>

http://www.aldebaran.cz/bulletin/2003_21_qua.html

<http://rco.upol.cz/>

<http://www.scienceworld.cz/> -rozcestník Kvantové počítače
přednáška Principy počítačů doc. Jirovského