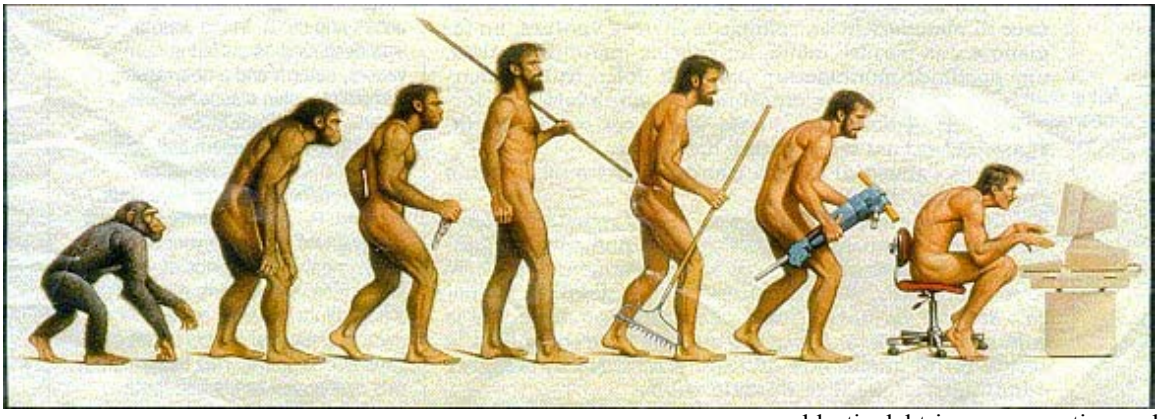
Quark 2004/09, Čo skúmajú mladí

Kvantové spracovanie informácie

V súťaži mladých vedeckých pracovníkov SAV do 35 rokov O najlepšiu publikáciu získal Mgr. MÁRIO ZIMAN, PhD., z Fyzikálneho ústavu SAV v Oddelení vied o neživej prírode prvé miesto. O čo v nej išlo, vám priblíži sám autor.



Prvé použitie nástroja našimi dávnymi predkami bolo veľmi pravdepodobne jedným z najdôležitejších počinov v evolúcii človeka. Od tohto okamihu prešlo veľa tisícročí, počas ktorých človek vyvíjal čoraz účinnejšie a zložitejšie nástroje a zariadenia. No a dnes si život bez niektorých z nich už ani nevieme predstaviť. Prístroje sú všade okolo nás a dokonca podľa nich posudzujeme stupeň ľudského vývoja. Ťažko povedať, ktorý stroj je v tomto rebríčku najvyššie, ale bezpochyby jedným z horúcich favoritov je počítač alebo ešte presnejšie procesor. Ten však nie je iba mozgom každého počítača, ale má ho aj práčka, mobilný telefón, pomáha nám riadiť auto, ale aj skúmať vesmír. Aká je jeho budúcnosť?

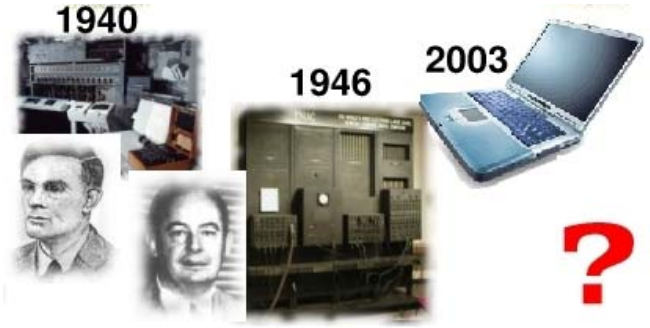
MÁLOKTO VERIL

Zostrojenie prvých počítačov si vyžiadala hlavne matematika. Človek skrátka nie je schopný vykonávať veľké množstvo rôznych aritmetických operácií potrebných, či už na vyriešenie nejakého fyzikálneho problému alebo na prelomenie tajnej šifry. Vskutku prvé prístroje, ktoré počítali namiesto nás, riešili práve úlohy tohto typu. Prvý počítač vyvinutý počas 2.svetovej vojny v USA mal za úlohu riešiť úlohy spojené s atómovou bombou. Angličania v tej dobe používali počítacie stroje na hľadanie šifrovacích kľúčov, ktoré im umožnili odhaliť tajnú nemeckú korešpondenciu. Od vtedy prešlo už vyše 50 rokov a nie každý si dnes vie predstaviť, že prvý počítač (ENIAC) zaberal celú športovú halu a nie každý v tom čase veril, že vôbec bude niekedy fungovať. Dnes máme oveľa výkonnejšie počítače s veľkosťou knihy (notebooky) a o ich funkčnosti (a užitočnosti) nikto nepochybuje. Navyše ENIAC bola schopná ovládať iba skupina vyškolených pracovníkov, kdežto dnešný počítač v princípe ovláda aj dieťa (samozrejme, nie je schopné riešiť fyzikálne úlohy alebo hľadať tajné šifry).

OTCOVIA INFORMATIKY

Kým úlohou strojov v minulosti bolo hlavne pomáhať pri fyzickej námahe, tak dnešné zariadenia pomáhajú aj pri „intelektuálnej“ činnosti a zložité matematické úlohy riešia v zlomku sekundy. Počítač je zariadením, ktoré dokáže spracovávať informáciu a manipulovať s ňou. Za vznikom prvého počítača stálo viacero osôb, a za všetky si spomeňme aspoň mená ako *John von Neumann* a *Alan Turing* (**obr.2**), ktorí sa veľkou mierou zaslúžili o model počítača a o odhalenie jeho skrytých možností. Dnes sa pokladajú za „otcov“ vedného odboru *informatika*, ktorý si kladie za cieľ študovať informáciu v tom najširšom zmysle.

Stále však treba mať na pamäti, že každý počítač je vo svojej podstate fyzikálnym prístrojom (ako väčšina strojov), a teda princípy, na ktorých bola vybudovaná informatika, sú v podstate dané zákonmi fyzikálnymi. Súčasné počítače pracujú na základe našich poznatkov z oblasti elektriny a magnetizmu, ktorá sa zaraďuje do tzv. klasickej fyziky. Klasická fyzika je široký pojem zahrnujúci v podstate všetku fyziku, okrem kvantovej fyziky, ktorá je zjednodušene povedané teóriou mikrosveta na úrovni atómov. V mikrosvete platia trochu iné pravidlá, než na aké sme zvyknutí z bežnej skúsenosti. Pravda je taká, že kvantovému svetu stále nerozumieme tak, aby sme mohli byť so sebou spokojní. Aj preto je veľmi ťažké o kvantovej teórii hovoriť na populárnej úrovni a bez použitia potrebnej matematiky. Ak kvantovému svetu celkom nerozumiete, prípadne sa vám jeho vlastnosti nepozdávajú, netrápte sa. „*Myslím, že bezpečne môžem vyhlásiť, že kvantovej teórii nerozumie nikto*“, povedal svojho času Richard Feynman, nositeľ Nobelovej ceny za fyziku.



Obrázok 2. *Vývoj počítačov. Na obrázku vidíme jedny z prvých počítačov: anglický “The Bombe” používaný počas II. svetovej vojny pri rozšifrovávaní nemeckých správ, a americký ENIAC skonštruovaný tesne po vojne. Pri ich vzniku stáli Alan Turing a John von Neumann (na obrázku).*

KVANTOVÝ SVET

Ak si dáme dohromady ustavičné zmenšovanie jednotlivých komponent počítača a hranice platnosti klasickej fyziky, tak celkom prirodzene prídeme k otázke: ***akým spôsobom bude fungovať počítač pracujúci na princípoch kvantovej teórie?*** Kvantový svet otvára pre informatiku a spracovanie informácie úplne nové obzory. Poskytuje viac možností, ktoré nám umožňujú s informáciou narábať efektívnejšie, prináša

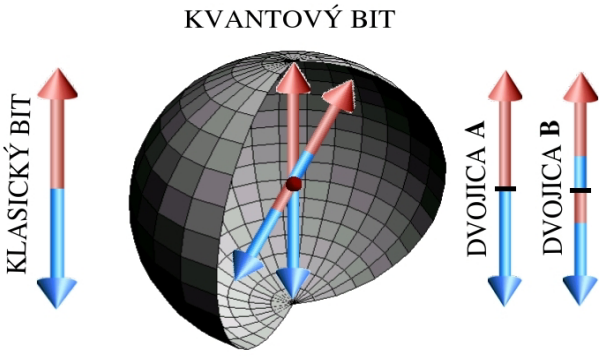
nové úlohy a riešenia, ale definuje aj nové problémy. Napríklad kopírovanie je v kvantovom svete nemožné. ***V čom je základný rozdiel medzi správaním sa informácie na klasickej a kvantovej úrovni?*** Vo vlastnostiach fyzikálnych systémov kódujúcich bit informácie, t.j. *klasického* a *kvantového bitu*, čiže v rozdielnosti dvoch fyzikálnych teórii.

KLASICKÝ A KVANTOVÝ BIT

Predpokladám, že ste sa už stretli so základným pojmom informatiky. Je ním *bit informácie*. Ide o abstraktný pojem, ktorý nám slúži na vyjadrenie faktu, že máme k dispozícii dve možnosti, dve rôzne hodnoty informácie. Ak povieme, že máme jeden bit informácie, tak to znamená, že poznáme jednu z dvoch možností, jednu z dvoch hodnôt. Tieto dve hodnoty sa zvyknú štandardne značiť pomocou symbolov „0“ a „1“, pričom ich konkrétny informačný obsah závisí od kontextu. Hodnoty 0/1 môžu znamenať odpovede áno/nie na nejakú otázku, čísla 0/1, farbu bielu/čiernu, stavy zapnuté/vypnuté. My budeme na označenie týchto hodnôt používať symboly „↑“ „↓“, ktoré sa ukážu byť užitočné pri prechode od klasického bitu ku kvantovému.

Jeden bit informácie je pojem čisto abstraktný, a v princípe ľubovoľný fyzikálny systém môže byť použitý ako jeho fyzikálna realizácia. Jediné, čo k tomu potrebujeme, sú dva *perfektne rozlíšiteľné stavy* tohto systému, aby sme vedeli jednoznačne povedať, o ktorú z hodnôt (↑,↓) bitu informácie ide. Tieto stavy zodpovedajú konkrétnym hodnotám nejakej fyzikálnej veličiny, napr. pre žiarovku svieti/nesvieti alebo rôznym hodnotám elektrického napätia a podobne. Perfektná rozlíšiteľnosť sa možno zdá byť samozrejmou a prirodzenou požiadavkou, avšak práve táto vlastnosť bude kľúčovou pri porovnaní klasickej a kvantovej realizácie jedného bitu informácie, t. j. bitu informácie zakódovanej do klasického alebo kvantového objektu.

Klasický aj kvantový bit sa môže nachádzať v dvoch perfektne rozlíšiteľných stavoch. Pre *klasický bit* je týmto počet jeho možných stavov úplný. Avšak pre *kvantový bit* je situácia iná a okrem týchto dvoch stavov ↑,↓ existuje ešte dokonca nekonečne veľa ďalších. Stále však platí, že *maximálne* dva z týchto stavov sú perfektne rozlíšiteľné. Ľubovoľný tretí stav už nevieme od týchto dvoch perfektne odlíšiť. Môžeme si to predstaviť tak, že kvantový bit nachádzajúci sa v tomto stave obsahuje sčasti informácie o oboch hodnotách, ale tieto informácie nie sú úplné. Zvláštnosťou (a v istom zmysle aj charakteristikou) kvantového bitu je, že medzi týmito stavmi existuje nekonečne veľa dvojíc, ktoré sú perfektne rozlíšiteľné. Jednotlivé stavy patriace do rôznych dvojíc však už perfektne rozlíšiteľné nie sú!



Obrázok 3. Klasický a kvantový bit. *Klasický bit sa môže nachádzať iba v dvoch stavoch, zatiaľ čo všetky stavy kvantového bitu tvoria guľu. Stavy z dvojice B ($\uparrow_B,\downarrow_B$) nevieme perfektne odlíšiť od stavov z dvojice A ($\uparrow_A,\downarrow_A$), čo je na obrázku zakreslené pomocou farieb. Každý stav z dvojice B sa nám javí aj ako červený, aj ako modrý.*

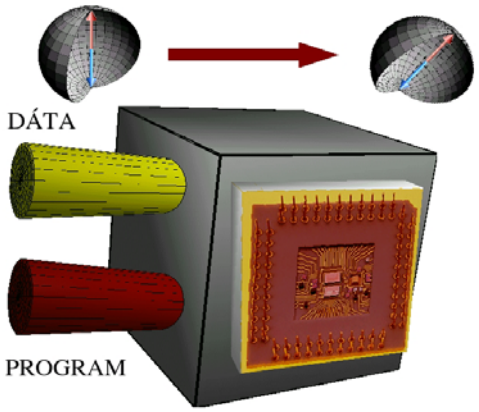
Dvojicu perfektne rozlíšiteľných stavov si označíme ako $\uparrow_A,\downarrow_A$. Symbol „A“ pri tomto značení je akýsi názov tejto dvojice – „dvojica A“. Ak si zoberieme dvojicu A ($\uparrow_A,\downarrow_A$) a dvojicu B ($\uparrow_B,\downarrow_B$), tak stavy $\uparrow_A,\downarrow_B$ alebo $\uparrow_A$, $\uparrow_B$ nevieme perfektne rozlíšiť (**obr.3**). Ako si predstaviť takúto množinu stavov? V prípade klasického bitu išlo o dvojprvkovú množinu – dve šípky smerujúce opačným smerom (hore a dole). Každú dvojicu perfektne rozlíšiteľných kvantových bitov si môžeme predstaviť ako takéto dve opačne orientované šípky. Je viacero možností, ako nekonečne veľa takýchto šípok poskladať dokopy, avšak najjednoduchšou je predstava, že šípky smerujú z toho istého bodu a dvojice sa navzájom líšia iba smerom. Fakt, že dve šípky z rôznych dvojíc nie sú perfektne rozlíšiteľné, je vyjadrený veľkosťou uhla, ktorý tieto šípky zvierajú. Nie je ťažké si predstaviť, že ku každej šípke (stavu) existuje jedna jediná šípka (stav), ktorá s ňou zviera uhol 180 stupňov (ktorý je perfektne rozlíšiteľný). Šípok, ktoré zvierajú iný uhol, je vždy nekonečne veľa. Množinu stavov kvantového bitu si môžeme predstaviť ako guľu (Zem), pričom perfektne rozlíšiteľné stavy tvoria navzájom opačné póly. Presná analýza kvantovej teórie vedie k takému istému výsledku a množinu stavov jedného kvantového bitu si predstavuje ako guľu. Vzájomná rozlíšiteľnosť stavov závisí od uhla. Čím je väčší, tým je väčšia aj rozlíšiteľnosť.

Predpovede kvantovej teórie sú takmer vždy iba pravdepodobnostné. S tým súvisí aj fakt, že stavy nevieme perfektne rozlíšiť. Pri rozlišovaní medzi stavmi $\uparrow_A$ a $\downarrow_A$ existuje meranie, pre ktoré výsledok jednoznačne určuje stav. Ale pri tom istom meraní stavu $\uparrow_B$, nám kvantová teória už predpovedá iba pravdepodobnosti a nikto dopredu nevie, ktorý z výsledkov nameriame. Aby sme odlíšili dva neperfektne rozlíšiteľné stavy, potrebujeme urobiť viac, meraní resp. naše rozlišovanie má iba pravdepodobnostný (štatistický) charakter. Takýto zložitý je kvantový svet obsahujúci jeden bit informácie.

PROCESORY A PROGRAMOVATEĽNOSŤ

Hlavnou súčiastkou každého počítača je jeho procesor, ktorého hlavnou výhodou je jeho *programovateľnosť*. Vďaka tomu nemusíme pri riešení nových úloh vyvíjať a stavať nové špeciálne zariadenia (hardvér). Stačí nám iba vhodne zmeniť program (softvér), ktorý využije zariadenie (procesor), ktoré

už máme. Napríklad taká automatická práčka. Na vstupe máme prádlo („dáta“) a nastavenie gombíkov („program“). Týmto nastavením meníme činnosť, ktorá sa má vykonávať (teplotu vody, rýchlosť otáčok atď.). Nepotrebujeme „bielu“ práčku na biele prádlo a „farebnú“ práčku na prádlo farebné.



Obrázok 4. Kvantový procesor *je zariadenie, ktoré nám umožňuje realizovať kvantové programy, t.j. otočenia. Na obrázku vidno otočenie množiny stavov kvantového bitu (gule) reprezentujúceho vstupné dáta, ktoré je špecifikované voľbou programu.*

Procesor si podobne môžeme predstaviť ako krabicu (**obr.4**), ktorá má dva vstupy a výstupy. Jeden z týchto vstupov obsahuje informáciu o dátach (vstupných parametroch programu) a druhý vstup prinesie informáciu o samom programe, ktorý sa má uskutočniť. Vstupujúca informácia je zakódovaná do stavu vstupujúcich bitov. Program sám osebe je iba transformáciou vstupných parametrov programu na výstupné, t. j. transformáciou vstupujúceho stavu na výstupný. Typ tejto transformácie nie je ľubovoľný, a závisí od fyzikálnej realizácie. Prirodzenou je požiadavka, aby transformácia (program) nemenila perfektnú rozlíšiteľnosť stavov. Inými slovami, aby sa množstvo informácie nemenilo, a menil sa iba informačný obsah. Napríklad pre jeden klasický bit existujú dva programy: IDENTITA (nezmení šípku) a NEGÁCIA (otočí šípku na opačnú).

Procesor je zafixovanou transformáciou toho istého typu, ale je definovaný okrem dát aj na programovej časti vstupu. Pomocou vstupného stavu programových bitov určujeme program, ktorý sa má vykonať. Prinajmenšom akademickou otázkou je existencia univerzálneho procesora, t. j. takého, ktorý by vedel uskutočniť všetky možné programy.
V prípade N klasických bitov je počet stavov ako aj počet programov vždy konečný. Ako o chvíľu uvidíme, v prípade aj jediného kvantového bitu je množina programov nekonečne veľká. Našťastie pre kvantový bit nemusíme zachádzať do detailov kvantovej teórie, aby sme vedeli, čo vlastne sú kvantové programy. Povedali sme si, že nerozlíšiteľnosť stavov priamo súvisí s uhlom, ktorý zvierajú príslušné šípky. Zachovanie nerozlíšiteľnosti teda znamená zachovanie tohto uhla. Ľubovoľná rotácia okolo stredu tento uhol zachováva a kvantová fyzika vedie presne k takémuto výsledku. Programy uskutočniteľné na kvantovom bite majú teda veľmi peknú geometrickú ilustráciu ako rotácie gule (stavového priestoru), ktorých je, samozrejme, nekonečne (dokonca nespočítateľne) veľa.

Programovateľnosť v klasickom prípade znamená schopnosť pripraviť konečný počet programov, t. j. konečný počet stavov programových bitov. Tieto stavy sú, samozrejme, všetky perfektne rozlíšiteľné, keďže pre klasický systém sú všetky stavy navzájom perfektne rozlíšiteľné. V kvantovom prípade je programov síce nekonečne veľa, ale aj stavov je nekonečne veľa. Každý program však predstavuje inú informáciu a navzájom sú tieto informácie perfektne rozlíšiteľné. Vieme presne určiť, o ktorý program ide. Preto aj stavy programových kvantových bitov kódujúce tieto programy musia byť podobne ako programy v klasickom prípade navzájom perfektne rozlíšiteľné. Avšak počet perfektne rozlíšiteľných stavov N klasických a N kvantových bitov je vždy ten istý a rovný 2^N. Pre P programov teda treba $M = \log_2 P$ programových kvantových bitov. Keďže aj pre jediný kvantový bit existuje nespočítateľne veľa rôznych programov, tak ani *univerzálny kvantový procesor* realizujúci všetky programy na jedinom kvantovom bite *neexistuje*.
Pre úplnosť si povedzme ako sme na tom v klasickom prípade. Pre N klasických dátových bitov je celkový počet možných programov rovný počtu permutácií všetkých stavov, t.j. $P=2^N!$. Počet potrebných programových bitov M dostaneme riešením rovnice $2^N! = 2^M$, t.j. $M = \log_2 2^N! \approx 2^N\ (N-1)$. Potrebujeme teda exponenciálne veľa (vzhľadom k počtu dátových bitov) programových bitov, aby sme boli schopní uskutočniť akýkoľvek program. Napriek tejto komplikácii však *univerzálny klasický procesor* v princípe *existuje*.

UNIVERZALITA

Zdá sa, že klasicky sme na tom lepšie. Avšak treba mať na pamäti, že počet klasických a kvantových programov je diametrálne odlišný. A navyše, kvantovým procesorom možno predsa len vrátiť ich „stratenú“ univerzalitu. Existujú procesory, ktoré dané programy vykonávajú iba s istou pravdepodobnosťou, pričom situáciu, keď procesor neuspeje, je veľmi jednoduché odhaliť. Univerzalita je teda „zaplatená“ stratou deterministickosti výpočtu. Napríklad, aby sme vedeli uskutočniť ľubovoľnú rotáciu (program) jedného kvantového bitu, tak potrebujeme program zakódovať do stavu dvoch kvantových bitov. Pravdepodobnosť s akou uskutočníme želaný kvantový program je potom ¼.

BUDÚCNOSŤ POČÍTAČOV

V úvode sme si položili otázku, aká je budúcnosť počítačov. Skôr alebo neskôr kvantové efekty bude treba vziať do úvahy. *Mooreov zákon*, ktorý popisuje ustavičné zmenšovanie procesorov, hovorí o roku 2015, a preto sa treba sa na túto dobu pripraviť skúmaním rôznych aspektov týchto „strojov budúcnosti“. Dnes vieme, že kvantové analógy niektorých klasických programov sú na kvantových počítačoch neuskutočniteľné. Aby sme boli presní, tak tieto analógy nie sú kvantovými programami, a preto nie sú zrealizovateľné. V tomto článku sme do zoznamu výsledkov v tejto rýchlo sa rozrastajúcej oblasti pridali neexistenciu univerzálneho kvantového procesora. Napriek týmto „negatívnym“ vlastnostiam však kvantové počítanie teoreticky v sebe skrýva veľký potenciál. Otázkou (experimentálnou a technologickou) zostáva, či ho budeme vedieť využiť alebo nie.

MÁRIO ZIMAN