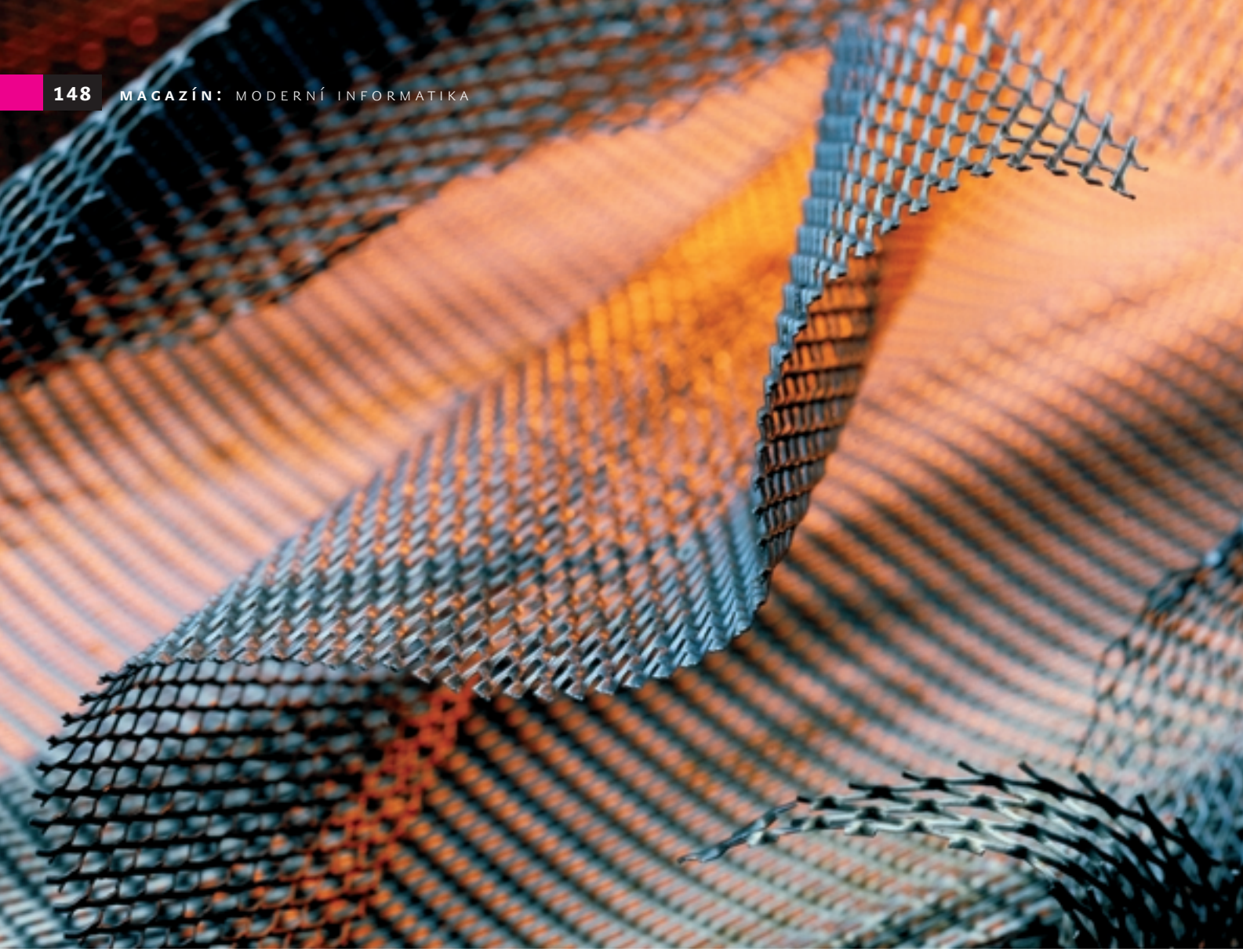


JEMNÝ ÚVOD DO KVANTOVÉHO POČÍTÁNÍ

Od bitů ke qubitům (1)

Dne 19. prosince 2001 oznámila firma IBM první praktickou realizaci kvantového počítače, na kterém už mohla běžet nejjednodušší instance Shorova faktorizačního algoritmu. Hlavní aspekty tohoto počinu, jehož význam možná dnes ještě ani nedokážeme docenit (pokud jej ovšem ukvapeně nepřeceňujeme), se pokusíme objasnit v právě začínajícím dvoudílném příspěvku.

Po téměř sto letech aktivního rozvoje kvantové mechaniky se zdá, že po teoretické i praktické stránce dospěla do stavu, kdy je schopna sloužit jako platforma pro realizaci výpočetních procesů. Potvrzuje to i zmíněná realizace kvantového počítače a provedení ukázkového výpočtu, jímž byla faktorizace čísla 15 ([4]). Právě zvolená úloha, spolu s tušením nevídaného výpočetního výkonu (a novinářskou senzacechtivostí), byla důvodem, proč se kvantový počítač ihned vetřel do povědomí veřejnosti jako tajemná hrozba pro současné kryptografické algoritmy.

BEZ TEORIE SE NEOBEJDEME...

Úvod do problematiky kvantových počítačů lze asi nejlépe začít právě v duchu nadpisu tohoto článku. Má-li pro nás jakýkoliv stroj rozumně pracovat, musíme se s ním v první řadě domluvit na tom, co po něm vlastně chceme. Musíme tedy zavést způsob kódování informace o zadání úlohy a rovněž tak způsob kódování příslušné odpovědi. U klasických počítačů k tomu používáme staré známé **bity** (tedy vlastně dvojkové číslice, ***bi**nary digit*), které chápeme jako prostředníky pro přenos informace a zároveň také jako základní informační jednotku. V roli „přenašeče" je tedy jeden bit schopen nést informaci o velikosti (nejvýše) jednoho bitu – toto významové přetížení slova bit není možná nejšťastnější, ale z informatického žargonu už je asi nikdo nevymýtí.

Při praktické realizaci počítače tuto matematickou představu bitu „mapujeme" na konkrétní fyzikální objekt – dnes pro reprezentaci bitů nejčastěji používáme napěťové úrovně v určitém místě elektrického

obvodu. Konstrukcí obvodu se snažíme zaručit, aby se v daném bodě vyskytovaly jen dvě možné (a dostatečně odlišné) napěťové úrovně – jedna odpovídající bitové hodnotě 0, druhá reprezentující hodnotu 1.

Kromě obvodů pro uložení informace máme k dispozici i obvody pro její zpracování. Ty převádějí vstupní bitové hodnoty podle daných pravidel na výstupní bitové hodnoty, čímž nad vstupními daty realizují různé matematické operace (opět tedy „mapujeme" abstraktní informační transformace na reálné fyzikální procesy). Systematickým propojováním takových obvodů nakonec dospějeme až k použitelnému počítači, který máme na pracovním stole.

Vznik kvantových počítačů lze v tomto kontextu chápat jako přirozený důsledek snahy zmenšovat rozměry fyzikálních reprezentantů bitů až na atomární, či dokonce subatomární úroveň. I zde je možné nalézt takové fyzikální veličiny, které umožňují zakódovat bitovou informaci. K takovému kroku nás dokonce přímo vybízí základní poznatek kvantové mechaniky, který říká, že **na kvantové úrovni jsou obory hodnot fyzikálních veličin diskrétní, a nikoliv spojité** (jak bychom se na základě smyslového poznání naší reality mohli domnívat).

Pojďme si tedy jako reprezentanta jednoho bitu zvolit přímo nějakou částici (například elektron) a hodnotu bitové informace kódovat konkrétní hodnotou pozorovatelné fyzikální veličiny označované jako *spin* této částice. Elektron je takzvaná *spin-1/2 částice*, takže hodnota spinu (její průmět do zvolené osy) zde může nabývat právě dvou různých čísel, které symbolicky označujeme jako *spin-up* (+1/2) a *spin-down* (-1/2), což se nám skvěle hodí pro vyjádření dvou možných hodnot bitu!

Bohužel, tak jednoduché to nebude. Na této úrovni je již nutné popisovat jevy jinou fyzikální teorií, než na jakou jsme z našeho okolí zvyklí. Nelze proto očekávat, že takový elektron se, pokud jde o jeho spin, bude chovat jako nějaký maličký rotující tenisák. Elektron totiž nemá nic společného s běžným hmotným tělesem, ani veličina spinu s jeho rotací. (Záměrně přeháním, aby bylo jasné, na jakou zeď zde klasický přístup ke konstrukci počítačů narazil.)

Žádná zeď však není tak vysoká, aby se přes ni nepokoušel někdo z vědců přelézt (čas od času se to někomu i podaří). První krok byl nasnadě. Bity realizované na kvantové úrovni se chovají jinak než jejich klasické předobrazy – nazveme je proto ***qubity*** *(quantum bits)* a budeme pokračovat dále v jejich zkoumání. Základní rozdíl mezi bitem a jeho kvantovým kolegou spočívá v tom, že qubit se – jako nějaký uličník – chová **jinak, když jej pozorujeme, a jinak, když jej necháme „bez dozoru"**. Tato rozdvojenost má své kořeny hluboko v teorii kvantové mechaniky a dosud není uspokojivě vysvětleno, odkud se vlastně bere. Zdůvodňuje ji jen matematický popis, pochopit ji rozumově však zatím neumíme. Také z tohoto důvodu se v dalším výkladu uchýlíme k **matematickým prostředkům** (samozřejmě jen pro nejnutnější ilustraci – například pro skutečné analytické řešení dále uvedené Schrödingerovy rovnice by bylo třeba uvést mnohem více, než nám prostor článku dovoluje).

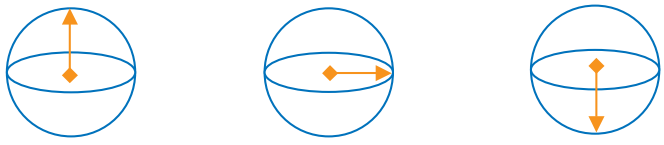
Napišme si tedy, co to vlastně ten qubit je. S výhodou zde využijeme Hilbertova prostoru, který je pro popis kvantového světa velmi příhodný. Omezíme se jen na jeho základní vlastnosti, tedy na to, že jde o unitární lineární prostor, který je úplný. Pro účely kvantové mechaniky se tyto prostory konstruují nad tělesem komplexních čísel, což znamená, že komplexní čísla zde vystupují v roli skalárů. Stav jednoho qubitu, který budeme značit jako $|\psi\rangle$ (tento symbol pochází z Diracovy „ket-bra notace" a nazývá se *vektor ket*), je považován za prvek dvourozměrného Hilbertova prostoru $\boldsymbol{H_2}$. Prvky báze tohoto prostoru symbolicky označujeme jako vektory $|0\rangle$ a $|1\rangle$. Jejich smyslem je reprezentovat **vlastní stavy** qubitu, které lze měřením získat (používá se také „německo-anglicky" vyhlížející termín *eigenstate*). S využitím této báze (kterou obvykle konstruujeme jako ortonormální) lze stav qubitu popsat takto:

$|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, kde koeficienty $\omega_0, \omega_1 \in \boldsymbol{C}$

Pro názornost zde budeme předpokládat, že báze použitého prostoru je tvořena vektory $|0\rangle = (1,0)^T$ a $|1\rangle = (0,1)^T$. Prvky báze si tedy představujeme jako sloupcové vektory jednotkové matice 2 x 2. To nám umožňuje chápat stav jako sloupcový vektor $|\psi\rangle = (\omega_0, \omega_1)^T$. Uvedená superpozice (skládání) vlastních stavů nám zachycuje právě zmíněnou základní „rozdvojenost" v chování qubitu. Pokud se jej nebudeme snažit „změřit" (měření je třeba chápat velmi obecně jako snahu o získání informace o vlastním stavu qubitu, a to jakýmkoliv způsobem), bude setrvávat v uvedené superpozici stavů, ze které se dokáže i dále vyvíjet (transformovat do jiné superpozice). Jakmile ale chceme jeho stav zjistit, ukáže se nám tento qubit vždy jen v jednom ze svých vlastních stavů. Nějaký superponovaný stav tedy ve skutečnosti nikdy neuvidíme. Navíc po přechodu do vlastního stavu už není možné vrátit qubit do původní superpozice, proto někdy hovoříme o *kolapsu kvantového systému* (či *destrukci superpozice*).

Kvantová mechanika nám odhaluje fascinující oblasti mikrosvěta. Bohužel zatím nedokážeme nabízené poznání plně pochopit – jen matematicky popsat. I s takovou „troškou" lze však dokázat divy.

Teď se samozřejmě vnucuje otázka, jak vlastně víme, že qubity se mohou nacházet v superponovaných stavech, když jsme nikdy takové stavy nemohli „na vlastní oči" spatřit. Na to současná fyzika odpovídá experimenty – sice nejsme schopni vidět přímo superpozice, ale jsme schopni vidět jistá „podivná" chování experimentů, která lze vysvětlit právě přijetím hypotézy o existenci superponovaných stavů. Proč však nevidíme „skutečné" superpozice, ale jen jejich důsledky, na to neznáme uspokojivou odpověď; vyskytují se dokonce názory, že k destrukci superpozice dochází až v našem mozku, kde se projevuje omezenost našeho vědomí (třeba nutná právě k tomu, aby vůbec nějaké vědomí vzniklo...). Tak nám nezbývá, než toto chování přijímat jen skrze jeho matematický popis a pokusit se ho v informatice k něčemu rozumnému využít.



$|\psi\rangle = |1\rangle$ (vlastní stav $|1\rangle$) | $|\psi\rangle = (1/2)^{1/2}(|0\rangle + |1\rangle)$ (vyvážená superpozice vlastních stavů) | $|\psi\rangle = |0\rangle$ (vlastní stav $|0\rangle$)

Obr. 1. Grafické znázornění stavu jednoho qubitu v Riemannově kouli

Věnujme se v krátkosti ještě významu skalárních koeficientů vystupujících v popisu stavu qubitu. Předpokládejme, že budeme pracovat s normovanými koeficienty, což je v podstatě jen matematická úprava, která zde není na újmu obecnosti. Potom pro koeficienty platí vztah:

$|\omega_0|^2 + |\omega_1|^2 = 1$. Navíc, jak fyzikové zjistili, hodnoty $|\omega_i|^2$ odpovídají pravděpodobnostem, že při následujícím měření přejde daný qubit do vlastního stavu |i>. Pokud tedy například máme $|\psi> = (1/2)^{1/2}(|0> + |1>)$, potom následující měření poskytne s 50% pravděpodobností výsledek |0> a se stejnou pravděpodobností výsledek |1>.

Pro lepší představu si můžeme vektor |ψ> zobrazit v (tzv. Riemannově) kouli. Výsledky tohoto zobrazení pro různé hodnoty koeficientů ω_i vidíme na obrázku 1. Význam stočení vektoru okolo horizontální osy je zřejmý, natočení kolem vertikální osy má význam pro interference mezi qubity. Rozhoduje o tom, které složky superpozice tím budou potlačeny a které naopak zvýrazněny. Pomocí interference tak můžeme kvantový počítač během výpočtu lépe soustředit na určité hodnoty výsledků.

Kvantové registry

Lapidárně řečeno, kvantový registr získáme tím, že do kvantového systému umístíme více qubitů. S přidáním dalších qubitů se exponenciálně zvětšuje dimenze prostoru, který stav daného registru popisuje. Obecně platí, že n-qubitový registr je popsán Hilbertovým prostorem dimenze 2^n. Tento prostor lze chápat jako tenzorový součin prostorů odpovídajících jednotlivým qubitům. Konkrétně pro dva qubity tedy dostáváme čtyřrozměrný prostor $\boldsymbol{H}_4^{(1,2)} = \boldsymbol{H}_2^{(1)} \otimes \boldsymbol{H}_2^{(2)}$, kde dvourozměrné prostory $\boldsymbol{H}_2^{(1)}$ a $\boldsymbol{H}_2^{(2)}$ korespondují s prvním, respektive s druhým qubitem v našem registru. Bázi budeme opět považovat za sloupcové vektory jednotkové matice, nyní typu 4 x 4, a tyto vektory budeme symbolicky značit |00> až |11>. Stav kvantového registru pak popíšeme jako superpozici bázových vektorů:

$|\psi> = \omega_{00}|00> + \omega_{01}|01> + \omega_{10}|10> + \omega_{11}|11>$, kde $\omega_{00}, \omega_{01}, \omega_{10}, \omega_{11} \in \boldsymbol{C}$

Analogicky jako při měření jednoho qubitu dostaneme měřením kvantového registru o dvou qubitech vždy jeden ze čtyř vlastních stavů. Pokud se však na systém „nedíváme“, může se nacházet v libovolné superpozici těchto stavů. Rozdělení výsledků měření v závislosti na koeficientech superpozice se chová opět analogicky k případu s jedním qubitem.

Kvantové registry nejen přirozeně zachovávají exotické vlastnosti qubitů, ale navíc přidávají další specialitu. Podívejme se na stav $|\psi> = (1/2)^{1/2}(|01> - |10>)$. Tento stav je zajímavý tím, že pokud změříme hodnotu jednoho z dvojice qubitů, známe automaticky hodnotu druhého z nich. Vzdálenost mezi těmito dvěma qubity zde přitom nehraje roli. Takto na papíře to sice vypadá jako veselá matematická hříčka, ale experimenty potvrdily, že „matka Příroda“ se takto skutečně chová! I když jedna částice bude na Zemi a druhá na Měsíci, víme v okamžiku změření jedné, do jakého stavu zkolabovala ta druhá. Musíme ovšem dodržet uzavřenost kvantového systému, což je jistě pro takováto měřítka dnes velmi obtížný problém. Uvedeným stavům se říká „propletené“ (v angličtině *entangled*) a matematicky je poznáme tak, že je nelze rozložit na prosté tenzorové součiny stavů dílčích qubitů.

Opět tedy narážíme na něco nového, co přichází teprve s konstrukcí kvantového registru. Stejně jako v případě podivného chování qubitů i zde se vedou dlouhé debaty o tom, co vlastně za možností takového nelokálního chování stojí. Dodejme, že propletenost stavů je nejen to pravé „koření“ k superpozici stavů, díky němuž mohou kvantové počítače zvládnout více než ty klasické, ale že jsou tyto stavy také úzce spojeny s fenoménem kvantové teleportace (čtenáři sci-fi teď jistě ožili...). Laicky řečeno, právě díky propleteným stavům můžeme „odsud“ nechat něco „zmizet“ tak, aby se „tam“ to samé zase „objevilo“ (zatím tento trik fyzika umí pouze s kvantovými stavy částic, ale i to je velmi zajímavé).

Vývoj kvantového registru

Kvantový registr v současné době představuje srdce každého kvantového počítače. U klasických počítačů kdysi registr také hrával hlavní roli, pak však na sebe většinu pozornosti strhly procesory, neboť především ony určovaly možnosti celého systému. U kvantových počítačů je situace malinko odlišná – hlavní schopnosti, které jsou pro informatiku zajímavé, pocházejí z fyzikálních vlastností kvantových registrů. Zbytek jsou „jen“ pomocné nástroje pro manipulaci s těmito registry. V centru pozornosti tedy zůstává kvantový registr a jeho vývoj.

Pod označením *vývoj registru* máme na mysli způsob, jakým se postupně mění jeho stav. Pokud není kvantový registr sledován, vyvíjí se jeho stav dle známé Schrödingerovy rovnice (publikované už v roce 1926), kterou zde použijeme ve tvaru:

$$ih \frac{\delta | \psi (t) >}{\delta t} = H (t) | \psi (t) >$$

Hodnota h zde znamená redukovanou Planckovu konstantu (jednotka Js) a matice $\boldsymbol{H}(t)$ představuje takzvaný Hamiltonův operátor (*hamiltonián*), který odráží energetickou konfiguraci systému. Pokud se omezíme na časově nezávislý hamiltonián, můžeme Schrödingerovu rovnici řešit jako:

$$| \psi (t) > = e^{\frac{-iHt}{h}} | \psi (0) > = U (t) | \psi (0) >, \text{ kde } U (t) \equiv e^{\frac{-iHt}{h}}$$

Sestavení velkých kvantových počítačů brání zejména problémy s dekoherencí. K jejich zvládnutí bude nutný nejen dostatek prostředků, ale také hlubší poznání mikrosvěta samého.

V duchu tradice (vzpomeňme si na chování qubitů a registrů) se i zde dostáváme k jedné podstatné kvantové zvláštnosti, neboť uvedený evoluční operátor $\boldsymbol{U}(t)$ musí představovat unitární matici. K takové matici vždy existuje matice inverzní (a je rovna její konjungované transpozici), což znamená, že její působení v roli operátoru musí být vždy vratné. Odtud pak plyne, že vývoj kvantového systému musí být reverzibilní, a tím je dáno i to, že **celý výpočet musí být do posledního qubitu vratný**.

Tento důsledek je ovšem třeba dobře interpretovat, a proto se u něho na chvíli zastavíme. Zcela pomýlenou interpretací je tvrzení, že kvantový systém umožňuje snadno invertovat ty funkce, o kterých prohlašujeme, že jsou jednosměrné (lze snadno vypočítat $y = f(x)$, ale pro náhodně volené y je neschůdné spočítat $x = f^{-1}(y)$). Správná interpretace chápe, že má-li být jednosměrná funkce vůbec realizovatelná na kvantovém počítači, musí se upravit tak, aby celý výpočet jako jeden proces byl **vratný**. Cokoliv, co není vratné, nám kvantový počítač jako svůj program jednoduše nepřijme.

Z tohoto pohledu je přímý výpočet jednosměrných funkcí na klasických počítačích jakýsi luxus, za který platíme mnohonásobně většími energetickými ztrátami, než by bylo nutné. Možnost provést výpočet nevratně však někdy může mít své kouzlo – například v kryptografii. Kdyby se někomu podařilo veškerou „Přírodu“ popsat jako jeden velký kvantový počítač, potom bychom o tuto výsadu nejspíš přišli, neboť v rámci tohoto velkého „Počítače“ by musely být všechny děje

už vratné a prostě bychom pak informaci nutnou pro zpětný chod neměli kam schovat. To je však těžká utopie, takže zatím můžeme informace nutné pro invertování jednosměrných funkcí nechat během výpočtů klidně „vyletět komínem“, aniž bychom se museli bát, že z tohoto kouře někdo zpětně zrekonstruuje vstupní data (pozor ovšem na postranní kanály, které jsou schopny dokonale využít každého nedopalku...).

K vývoji kvantového registru také patří zmínka o problémech s **nechtěnými destrukcemi stavů**, někdy též hovoříme o *efektu dekoherence*. Hlavním činitelem je zde již několikrát zmíněný požadavek „nepozorovaného vývoje“. Na to jsou kvantové systémy až chorobně přecitlivělé. I nepatrná interakce kvantového systému s okolím může mít za následek jeho kolaps, což samozřejmě znamená, že výpočet končí neúspěchem. S trochou nadsázky lze říci, že jakmile má kvantový počítač sebemenší podezření, že předává svému okolí nějakou informaci, ihned se hroutí (nebo alespoň nevhodně „proplétá“ se svým okolím).

Svého času se situace zdála tak neúnosná, že se vůbec přestávalo věřit v možnost takový počítač sestavit a udržet v činnosti. Novou naději přinesla teorie kvantových samoopravných kódů spolu se zlepšením technologické základny. Pro větší délky registrů je však i dnes udržení koherentního vývoje teprve hudbou budoucnosti.

Kvantové obvody

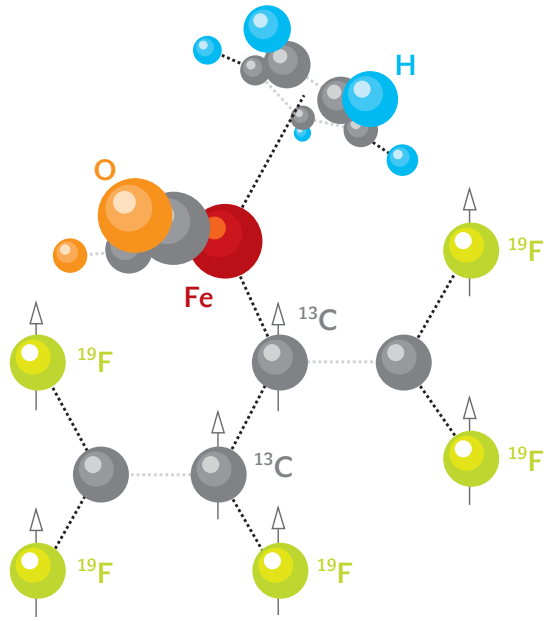
Kvantové obvody jsou nejpoužívanějším základním nástrojem pro popis výpočtů na kvantových počítačích. Mají podobu acyklických grafů, kde uzly představují operace prováděné pomocí kvantových bran a hrany popisují způsob propojení těchto bran; jedna hrana většinou odpovídá jednomu qubitu. V papírové podobě takové schéma připomíná klasický počítač, ovšem při jeho realizaci už veškerá analogie mizí. Každá kvantová brána je popsána unitární čtvercovou maticí. Z těchto matic a z grafu popisujícího výpočet se pak určitým způsobem zpětně odvodí hamiltonián kvantového systému tak, aby výsled-

(x, y, z) → (x, y, z xor (x and y))					
vstup			výstup		
x	y	z	x′	y′	z′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Obr. 2. Popis Toffoliho (CCN) brány

(x, y, z) → (x, (not (x) and z) or (x and y), (not (x) and y) or (x and z))					
vstup			výstup		
x	y	z	x′	y′	z′
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	0	0	1
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

Obr. 3. Popis Fredkinovy brány



Kvantový registr „in natura“

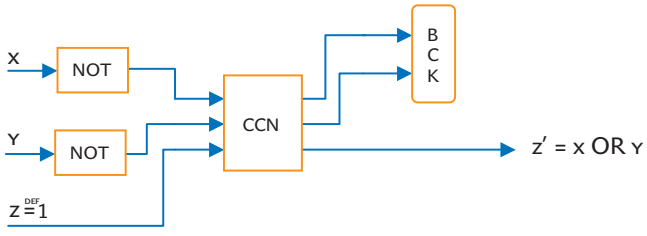
Pokud vám k výkladu chybí nějaká fyzikální představa, podívejte se na obrázek. Je na něm (samozřejmě jen schematicky a stylizovanými symboly, jimiž jsme si zvykli zobrazovat atomární struktury) znázorněn sedmiqubitový registr v molekule sloučeniny $C_{11}H_5F_5O_2Fe$ – právě ten, který se loni v prosinci proslavil zmíněným řešením faktorizace. Vy pozorní jste si jistě povšimli, že ačkoliv kvůli zjednodušení výkladu vysvětlujeme základní princip na příkladu spinu elektronů, zde se v roli qubitů používá spin celých atomů. Tato „nuance“ však pro náš „uživatelský“ pohled není podstatná.

ný vývoj odpovídal aplikaci zvolených operátorů na centrální registr. Toto je sice značně zhuštěný pohled na věc, nicméně pro hrubou ilustraci zde postačí.

Na obrázcích 2 a 3 vidíte popisy dvou základních reverzibilních bran, které se někdy nazývají po svých autorech Toffoliho a Fredkinova brána. Tyto brány jsou navrženy pro použití jak v klasických, tak i v kvantových počítačích. Kvůli přehlednosti jsou na obrázcích jejich funkční tabulka a popis provedeny pro bitovou logiku. Pro použití v kvantových obvodech se odvodí příslušné operátorové matice. Obě brány pracují se 3qubitovými stavy, které jsou prvky Hilbertova prostoru dimenze $2^3 = 8$. Bázi tohoto prostoru opět považujme za sloupce jednotkové matice typu 8 x 8 a tyto vektory symbolicky označme |000> až |111>. Ve vztahu k bitovým proměnným na obrázcích můžeme stav symbolizovat také jako |x,y,z>. Aplikaci dané brány na stav $|\psi\rangle$ chápeme jako násobení sloupcového vektoru stavu příslušnou maticí, což zapisujeme jako $|\psi_{i+1}\rangle = \boldsymbol{U}|\psi_i\rangle$, kde $\boldsymbol{U}$ je unitární matice popisující daný operátor. V případě Toffoliho brány je odpovídající kvantový operátor vzhledem k definované bázi určen maticí:

$$U = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix}$$

Klasické brány, jako je například známý NAND ($z = x\ NAND\ y = NOT(x\ AND\ y)$), nelze pro kvantové počítače použít, neboť ty nejsou reverzibilní. To však nevadí, neboť lze ukázat, že jak Toffoliho brána (též známá jako *Control Control Not* – CCN), tak i Fredkinova brána jsou univerzální. Pokud u Toffoliho brány nastavíme pevně vstup z = 1, potom pro výstup z' platí $z' = (x\ NAND\ y)$. Poněvadž NAND je univerzální operace (lze s ní realizovat libovolnou booleovskou funkci), je i Toffoliho brána univerzální. Pro Fredkinovu bránu zase za podmínky z = 0 platí $y' = (x\ AND\ y)$ a za podmínek z = 1 a y = 0 platí y'= NOT(x). Opět víme, že dvojice bran AND a NOT tvoří univerzální pár, takže Fredkinova brána je také univerzální.



Obr. 4. Využití CCN pro realizaci OR reverzibilním způsobem

Přímočarý přepis výpočtu z klasického počítače na kvantový by teoreticky mohl být založen na jednoduchém překreslení klasického schématu (například v realizaci s obvody NAND) do schématu využívajícího kvantové brány (například CCN). Takový přístup je naznačen na obrázku 4, kde je poněkud těžkopádně realizován reverzibilní výpočet funkce OR. K tomu jsou použity brány CCN a NOT (tato brána je triviálně také reverzibilní). Vidíme, že do registru BCK směřují dodatečné mezivýsledky, které slouží pro zpětný chod výpočtu. Tyto výsledky musí být uchovávány po celou dobu běhu kvantového programu. Tento postup však vede k fyzikálně problematickým konstrukcím, a tak se hledají důmyslnější metody konstrukce reverzibilních výpočtů. Potěšujícím zjištěním je, že každý výpočet realizovatelný na Turingově stroji (obecná abstrakce současných počítačů, viz příští díl) je možné převést do reverzibilní podoby – chce to jen čas a nemalé úsilí. Ilustraci tohoto problému spolu s představením efektivní Benettovy metody lze nalézt v [3].

A k čemu je to dobré?

Představili jsme si základní matematicko-fyzikální principy, na nichž je založena konstrukce kvantových počítačů. Ukázali jsme si, kde jsou hlavní odlišnosti od klasických počítačů, a to zejména s ohledem na „programování“ kvantových počítačů. V příštím dílu se zamyslíme nad praktickým využitím těchto strojů, kde se zaměříme na efektivitu jejich výpočtů ve srovnání s klasickými počítači, a při té příležitosti si představíme Shorův faktorizační algoritmus [3, 4]. ■ ■ ■ Tomáš Rosa, *autor@chip.cz*

Literatura:

[1] Archiv vědeckých článků arXiv, *http://arxiv.org/*

[2] Gruska, J.: *Quantum Computing*, McGraw-Hill, 1999

[3] Shor, P.-W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, extended article, 25 Jan 96, arXiv: quant-ph/9508027 v2

[4] Vandersypen, L., M., K., Steffen, M., Breyta, G., Yannoni, C.-S., Sherwood, M.-H. and Chuang, I.-L.: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature, Vol. 414, 20/27 December 2001

[5] Williams, C.-P. and Clearwater, S.-H.: *Explorations in Quantum Computing*, Springer-Verlag, 1998