FYZIKA KVANTOVÝCH POČÍTAČŮ (1)

Kvantové počítače: hardware

Pokud jste v předcházejících číslech Chipu sledovali seriál Od bitů ke qubitům, určitě vám také vrtala hlavou otázka, jak vlastně kvantový počítač fyzicky realizovat, jak v něm potřebné atomy „upnout“, sledovat jejich chování atd. Tento příspěvek by mohl některé z těchto věcí objasnit.

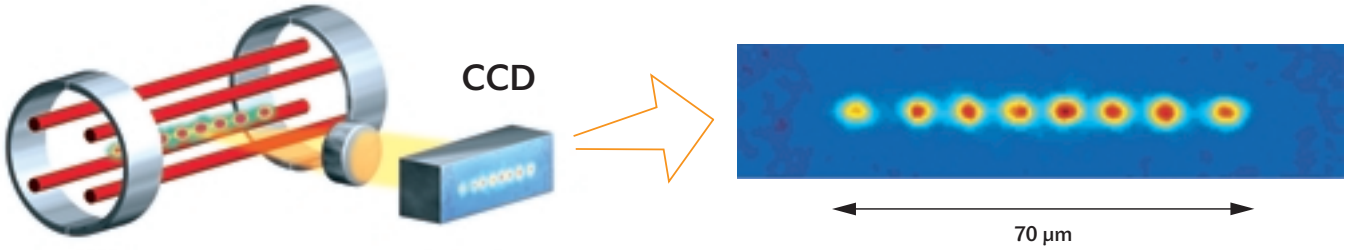
Ve zmíněných článcích [1] jste se mohli seznámit se základními principy kvantových počítačů (viz též např. [2]), a to zejména z matematického, či, chcete-li, z abstraktního pohledu. Připomeňme si zde stručně základní teze:

- Kvantové počítače mohou pracovat s kvantovou superpozicí všech možných stavů kvantového registru – v jistém smyslu tedy mohou v jediném kroku sledovat mnoho různých cest zároveň a zásadně tak urychlit některé výpočty.
- Dimenze stavového prostoru kvantového registru roste exponenciálně s počtem kvantových bitů (qubitů) v registru.
- Kvantovým algoritmem rozumíme řízenou unitární evoluci vhodného kvantového systému zakončenou kvantovým měřením.
- Pro některé úlohy není znám klasický postup, při němž by počet operací, které je třeba provést, nerostl exponenciálně s délkou vstupu (tj. s počtem vstupních bitů). Kvantové počítače ale pro stejné úlohy mohou nabídnout postupy, při nichž počet operací roste s délkou vstupu nanejvýš jako polynom konečného stupně. Typickými problémy, které by kvantové počítače dokázaly zvládnout v polynomiálním čase, ale pro které není znám žádný klasický polynomiální algoritmus, jsou faktorizace (rozklad čísla na prvočinitele) a výpočet diskrétního logaritmu. Je zřejmé, že realizace kvantového počítače, který by tyto úlohy dokázal efektivně vyřešit pro dostatečně dlouhé vstupní hodnoty, by položila na lopatky téměř všechny běžně užívané kryptosystémy s veřejným klíčem.

V tomto článku už přejdeme od abstraktní teorie k reálnému „hardwaru“ a budeme se zabývat možnými implementacemi kvantových počítačů. Pokusíme se stručně vysvětlit vybrané fyzikální principy, na jejichž základě by se v budoucnu mohlo podařit kvantový počítač vybudovat, shrneme současný stav v oblasti experimentálního bádání a upozorníme na některé obtíže.

CHLADNÉ IONTY V PASTI

Ionty, tedy elektricky nabité atomy, jsou nadějným kandidátem pro experimentální testování kvantových algoritmů. I když rozsáhlé kvantové počítače náleží zatím stále spíš do oblasti sci-fi, na „iontových procesorech“ byly již laboratorně odzkoušeny mnohé důležité elementy kvantového počítání. Kvantový registr je v daném případě realizován řetězcem laserově vychlazených iontů nacházejících se v *lineární pasti* [3] – viz obrázek 1. Každý iont reprezentuje jeden kvantový bit (qubit). V pasti jsou ionty drženy prostřednictvím elektrických sil. Celá past je umístěna ve vakuu. Pomocí důmyslného postupu tzv. laserového chlazení je iontům odebírána kinetická energie, až se kmity celého řetězce iontů dostanou do kvantového stavu s nejnižší vibrační energií. Dvě vnitřní energetické hladiny každého iontu odpovídají „logickým“ bázovým stavům qubitu, $|0\rangle$ a $|1\rangle$.



Obr. 1. V levé části obrázku je schéma lineární pasti používané na univerzitě v Innsbrucku. V ose pasti jsou drženy laserově vychlazené ionty. Vpravo je osmice iontů zviditelněná speciálním zobrazovacím zařízením. (Podle internetové prezentace R. Blatta, Universität Innsbruck, Institut für Experimentalphysik, *http://online.itp.ucsb.edu/online/qinfo_co1/blatt/*)

Zapisování informace do qubitů a požadované „logické" operace se provádějí následujícím způsobem: Každému iontu je přiřazen laser, který podle potřeby vytvoří elektromagnetické vlnění, s nímž iont interaguje. (Připomeňme si, že frekvence elektromagnetického vlnění ν a energie odpovídajícího fotonu E jsou svázány vztahem $E=h\nu$, kde h je Planckova konstanta.) Působením laserových pulzů vhodné délky a polarizace, jejichž frekvence je zvolena tak, aby odpovídala energetickému rozdílu vnitřních energetických hladin iontu, lze realizovat přechody mezi stavy $|0\rangle$ a $|1\rangle$ i vytvářet jejich lineární superpozice (tj. $\alpha|0\rangle+\beta|1\rangle$, kde α a β jsou komplexní čísla) u každého jednotlivého iontu.

Vzájemná interakce mezi qubity (tedy mezi jednotlivými ionty) je zprostředkována vibračním neboli tzv. *fononovým* modem kolektivního těžišťového pohybu všech iontů (ionty v pasti mohou kmitat podobně jako kuličky na pružinách). Laserové pulzy, jejichž frekvence se liší od frekvence odpovídající rozdílu vnitřních energetických hladin právě o frekvenci těžišťového fononového modu (tj. o frekvenci kmitů řetězce iontů), umožňují vedle přechodů mezi vnitřními hladinami navíc také excitovat (vybudit) nebo deexcitovat zmíněný vibrační modus, a zajistit tak interakci mezi různými qubity.

Konkrétně tak lze uskutečnit např. přechod z horní energetické hladiny („1") do základní („0") se současným vybuzením fononového modu nebo provést podmíněnou změnu fáze základního stavu $|0\rangle$. (V kvantových superpozicích $\alpha|0\rangle+\beta|1\rangle$ popisujících vnitřní stavy iontů mají důležitý význam nejen velikosti komplexních koeficientů α a β, ale i jejich fáze.) Druhá možnost znamená operaci, při níž dojde ke změně fázového faktoru u základního stavu – to ovšem jen tehdy, je-li zároveň vybuzen fononový modus. K tomu je ovšem potřeba další vnitřní energetická hladina iontu. Přechod na ni vyžaduje jinou polarizaci světla laseru. Dá se ukázat, že popsané operace s ionty jsou postačující ke konstrukci libovolného kvantového hradla [3]. První experimentální implementace kvantového hradla C-NOT (řízeného NOT) byly na iontech vyzkoušeny už v polovině 90. let minulého století [4, 5].

Využití chladných iontů v pasti naráží na dva hlavní problémy. První se týká tzv. dekoherence a je víceméně společný všem fyzikálním implementacím kvantových počítačů. Druhý souvisí s praktickým omezením počtu iontů (tedy qubitů), které lze v pasti udržet a s nimiž je možné pracovat.

Dekoherence je proces, v němž se samovolně (nezaměňovat s kolapsem kvantového systému způsobeným měřením) ztrácí informace o vzájemných fázích jak v superpozicích stavů jednotlivých qubitů, tak kvantových registrů sestávajících z více qubitů. Je důsledkem interakce systému s okolím. Narušuje stavy superpozice i tzv. *entanglement* („provázanost") mezi qubity, což jsou nezbytné ingredience kvantového výpočtu. Odizolovat systém dokonale od okolí je nesnadná věc. Potíž je navíc v tom, že na jedné straně chceme interakci qubitu s okolím co nejvíce omezit, ale na straně druhé nutně potřebujeme, aby jednotlivé qubity vzájemně silně interagovaly (řízeným způsobem).

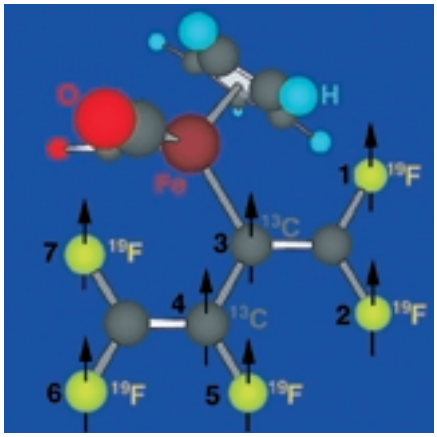
Důležitým ukazatelem je poměr středního času, za nějž dojde k dekoherenci, k času potřebnému na jednu logickou operaci – tento poměr, zhruba řečeno, udává, kolik operací se stihne provést. Uvedený poměr se u reálných experimentů s chladnými ionty v pasti pohybuje dnes v řádu desítek, maximálně stovek, teoreticky by však mohl dosáhnout hodnot 10^5 až 10^6. Vliv dekoherence lze částečně omezit kvantovými opravnými kódy [6] a kódováním informace do podprostorů invariantních vůči kritickým dekoherenčním účinkům – i tento „trik" už byl na iontech testován experimentálně [7]. Ve všech provedených experimentech však fyzikové zatím dokázali manipulovat jen s malými počty qubitů (iontů) a nikde zatím nepřekročili desítku.

Kvantový registr lze implementovat pomocí řetězce laserově vychlazených iontů umístěných v lineární pasti.

Nukleární magnetická rezonance

Nukleární magnetická rezonance (NMR), veřejnosti známá spíše z lékařských diagnostických metod, umožnila jako první platforma realizovat „úplný" kvantový výpočet. Jako kvantový registr slouží v tomto případě organické molekuly. Qubity jsou reprezentovány orientací spinů jader atomů. Úspěch týmu IBM s faktorizací čísla 15 (viz [8]) vyvolal jistou euforii a vizi o možném rychlém rozšíření komplexnějších kvantových obvodů. Abychom však trochu zchladili přemíru optimismu, podotkněme předem, že NMR v takové podobě, jak ji známe dnes, je z hlediska dalšího vývoje pravděpodobně ta nejméně vhodná metoda...

Povězme si nejprve něco o samotné NMR. Tato v současnosti robustní a spolehlivá technika, vyvinutá v padesátých letech 20. století, nachází široké uplatnění nejen ve fyzice, ale také v chemii a medicíně. Abychom pochopili, jak se může uplatnit i v kvantových výpočtech, musíme si nejdříve vysvětlit pojem spin. *Spin* je kvantová vlastnost jader atomů, elektronů i jiných kvantových částic, analogická magnetickému momentu známému z klasické fyziky. Pro nás je důležité, že průmět vektoru spinu do libovolné osy (v rámci „kvantování", a na rozdíl od klasické fyziky) nabývá pouze diskrétních hodnot a že lze vybrat případy, kdy průmět spinu může nabývat právě jen dvou hodnot.



Obr. 2. Molekula $C_{11}H_5F_5O_2Fe$ použitá při realizaci Shorova algoritmu na NMR počítači. „Výpočetní" atomy, které sloužily jako kvantový registr, jsou označeny šipkami. (Zdroj: IBM Almaden Research Center, San Jose, California, USA)

Takové dva diskrétní stavy se přímo nabízejí k zakódování dvou „logických hodnot" qubitu. A protože jsme v kvantovém světě, lze jádro připravit v libovolné superpozici různých průmětů spinu. Vložíme-li částici s nenulovým magnetickým momentem do silného magnetického pole, začne vektor magnetického momentu rotovat kolem osy magnetického pole s tzv. *Larmorovou rezonanční frekvencí*. Lze si to představit jako precesní pohyb dětské káči v gravitačním poli. Něco podobného se děje i s jadernými spiny v molekule, ocitnou-li se v magnetickém poli.

Dvěma možným hodnotám projekce spinu do směru siločar magnetického pole (po směru nebo proti směru) odpovídají dvě různé energie jádra v poli. Jejich rozdíl je úměrný právě Larmorově rezonanční frekvenci a závisí na intenzitě přiloženého pole (v praxi se pohybuje v řádu jednotek tesla) a na chemickém okolí jádra. Spinový stav jádra (tj. konkrétní podobu superpozice dvou opačných spinových stavů) lze ovládat pomocí vysokofrekvenčních pulzů o rezonanční frekvenci jádra. Protože každé jádro v molekule má tuto frekvenci vzhledem k různému chemickému okolí mírně odlišnou, je možné ovlivňovat cíleně různá jádra a „adresovat" tak jednotlivé qubity.

„Posvítíme-li" na vybrané jádro pulzem elektromagnetického záření o vhodné frekvenci, lze spinem „pootočit" (tj. lze vytvořit požadovanou superpozici); velikost a osa otočení závisí na délce pulzu a jeho intenzitě. Z daného stavu qubitu lze tedy vytvořit libovolný jiný stav. Tímto způsobem můžeme realizovat jakékoliv jednoqubitové hradlo. Pro dvouqubitovou interakci je nutné zajistit vzájemné ovlivnění dvou spinů. To se fyzikálně děje prostřednictvím *spin-spinové interakce* (magnetické momenty na sebe vzájemně působí). Aplikujeme-li na takto svázaná jádra patřičnou sekvenci pulzů, máme dvouqubitové hradlo.

Jádra ale nevydrží ve specifických stavech neomezeně dlouho. Po určité době dojde vlivem interakce s okolím k už zmíněné dekoherenci. Doba, za kterou se to stane, je ale oproti jiným metodám značná – se současnou technologií v řádu desítek sekund (!), přičemž možnosti nejsou zdaleka vyčerpány. To patří k jedné z největších výhod platformy NMR. Díky tomu lze v současnosti dosáhnout stovek až tisíců operací.

Až doposud je vše snadné. Každá molekula se může chovat jako kvantový počítač a čím více jader by obsahovala, tím složitější obvody bychom mohli sestavovat. Zde se ale dostáváme k hlavnímu problému. Současné NMR počítání není založeno na jedné molekule, ale na souboru obsahujícím kolem 10^{23} molekul. Je to jednak proto, že manipulace s jednou molekulou není vůbec snadná, především však proto, že odezva jedné molekuly umístěné v magnetickém poli je tak slabá, že je současnou technikou neměřitelná.

Soudobé NMR počítače se proto konstruují tak, že „výpočetní" molekuly (ve značném počtu) plavou v kapalině za pokojové teploty. Tato startovací podmínka s sebou nese řadu podstatných problémů. Před začátkem kvantového výpočtu by bylo třeba spiny jader ve všech molekulách přivést do přesně definovaného kvantového stavu (musí to být tzv. *čistý stav*), což ale s popsaným obsáhlým souborem jde těžko. Soubor se nachází v rovnovážném termodynamickém stavu, kdy jsou spiny „rozházeny" rovnoměrně do všech směrů – jde tedy o kvantovou „statistickou směs". Uvedený problém se řeší tak, že se určitým způsobem upřednostní jeden spinový směr a se vzniklou odchylkou od rovnovážného stavu se zachází jako s obdobou čistého stavu – „pseudočistým stavem". Rovnovážný zbytek je vůči libovolným výpočetním transformacím imunní a tvoří jakési „pozadí" nevstupující do výpočtu.

Ono „upřednostnění směru" lze uskutečnit mnoha způsoby a kolem tohoto fenoménu byla vybudována samostatná teorie. V experimentu s faktorizací byla použita metoda tzv. *časového průměrování* – v několika různých experimentech se vždy na stejný vzorek v rovnováze aplikovala řada pulzů. Ty měly za následek přerozdělení distribuce stavů v látce (v každém jednotlivém experimentu trochu jiné). Na každém vzorku pak byl aplikován algoritmus faktorizace. Zprůměrováním výsledků se dosáhlo stejného efektu, jako by v látce existoval pseudočistý stav.

Je to tak trochu magie. Každopádně je podstatou pseudočistého stavu kolektivní chování mnoha spinů a vyvstává otázka, co se vlastně při výpočtech děje. V ideálním případě jedné molekuly by po měření spinu nastal kolaps vlnové funkce, ale zde k žádnému „kolektivnímu kolapsu" nedochází. Výsledkem totiž není projekce jednoho spinu do zvolené osy, ale střední hodnota jako odezva souboru jader. S jistou nadsázkou lze říci, že výpočty prováděné technikou NMR nejsou opravdové kvantové výpočty, ale určitá emulace kvantového počítání. To souvisí s otázkou, zda tato platforma vykazuje všechny „správné" rysy kvantového světa, jako je například možnost realizace entanglementu.

NMR se tedy zasloužila o první kroky k praktické realizaci něčeho velmi podobného kvantovému počítači. Avšak jak už jsme předeslali, jedná se spíše o určitý mezikrok k opravdovému kvantovému počítání, daný současnou technologickou úrovní. K dalším nevýhodám patří velikostí molekuly omezený počet qubitů pro kvantový registr. Udává se principiální omezení řádově desítek qubitů.

Metoda založená na současné NMR je spíše jen emulací kvantového počítání.

Příště

Iontová past a nukleární magnetická rezonance nejsou jedinými platformami, na nichž je potenciálně možné realizovat kvantové výpočty. Na další možnosti se podíváme v příštím čísle, kde se také pokusíme alespoň o rámcové porovnání efektivity jednotlivých metod.

■ ■ ■ Kamil Brádler, Miloslav Dušek, Karel Král, Marian Čerňanský, *autor@chip.cz*
(Autoři se mj. zabývají kvantovou optikou a kvantovou teorií informace na MFF UK, PřF UP a FZU AV ČR.)

Literatura:

[1] Chip 3/02, 4/02, 5/02.
[2] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge, 2000).
[3] J. I. Cirac, P. Zoller, Phys. Rev. Lett. 74, 4091 (1995).
[4] C. Monroe et al., Phys. Rev. Lett. 75, 4714 (1995).
[5] B. Schwarzchild, Physics Today 49, 21 (1996).
[6] A. Calderbank, P. Shor, Phys. Rev. A 54, 1098 (1996).
[7] D. Kielpinski et al., preprint na arXiv.org: quant-ph/0102086 (2001).
[8] L. M. K Vandersypen et al., Nature 414, 883 (2001).