FYZIKA KVANTOVÝCH POČÍTAČŮ (2.)

Kvantové počítače: hardware

Cesta vedoucí "od bitů ke qubitům" zatím asi připadá schůdnější matematikům než fyzikům. Právě z jejich pohledu jsme se fenoménem kvantových počítačů začali zabývat v minulém čísle, zdaleka však nebylo řečeno vše.

Seznámili jsme se zatím se dvěma možnostmi, jak kvantový počítač uvést v život. Nyní budeme pokračovat pohledem na další tři fyzikální platformy, které vzbuzují určité naděje na jeho realizaci.

KVANTOVÁ OPTIKA

Další oblastí, která se dočkala pozornosti fyziků a která je jedním z adeptů na praktickou realizaci kvantových hradel, je kvantová optika. Již v roce 1989, tedy v raných dobách kvantového počítání, navrhl G. J. Milburn obvod pro Fredkinovo hradlo, sestavený výhradně z optických elementů [1]. Jako nosiče logických stavů sloužily procházející fotony. Hradlo bylo realizováno relativně jednoduchým optickým obvodem. K interakci mezi fotony, nesoucími jednotlivé qubity, docházelo v tzv. *nelineárním optickém prostředí*. Potíž však byla v tom, že pravděpodobnost požadovaného procesu je velmi malá a účinnost hradla tedy velmi nízká. „Účinnost" takových nelineárních procesů totiž závisí na intenzitě vstupních optických polí a při extrémně nízkých intenzitách odpovídajících jednotlivým fotonům už pro daný účel nevyhovuje. Nedávno však byl navržen způsob, jak se bez nelineárního prostředí obejít.

Logické hodnoty bitů se dají zakódovat do stavů fotonů mnoha způsoby. Na rozdíl od původního Milburnova návrhu, kdy logická nula znamená stav bez fotonu a logická jednička stav s fotonem, je obvykle výhodnější použít *polarizační kódování*. Polarizace fotonů má velmi těsnou analogii se spiny jader v NMR, avšak místo spinu „nahoru" či „dolů" u jádra budeme u fotonů mluvit o horizontální či vertikální polarizaci.

Lze sestavit kvantový obvod s výhradně lineárními optickými prvky, úspěšně však funguje pouze s jistou pravděpodobností.

Pro úspěšné kvantové počítání je především nutné zvládnout jednoqubitové operace, tedy umět manipulovat s jednotlivými fotony. Při sestavování jednoqubitových hradel nelineární prvky nepotřebujeme. Tato hradla lze zkonstruovat pouze pomocí *pasivních lineárních optických elementů*, třeba děličů svazku (polopropustných zrcadel) a prvků zajišťujících fázový posuv (prodlužujících optickou dráhu). Po průchodu těmito elementy se zachovává celkový počet fotonů.

Pro kvantové počítání je ale nezbytné sestavit také nejméně jedno alespoň dvoukubitové hradlo, např. C-NOT (podmíněná negace). Jak už název napovídá, takové hradlo vyžaduje interakci dvou qubitů, a zde už proto potřebujeme nelineární proces, který by byl schopen zajistit interakci „nosných" optických polí. Už víme, že málo účinné nelineární optické prostředí na tento úkol nestačí, nakonec se však podařilo najít cestu, jak se jeho použití vyhnout – zrodil se koncept tzv. *lineárně optického kvantového počítání* (LOQC) [2].

Vícequbitová hradla se v tomto řešení realizují *nedeterministicky* (to znamená, že ne vždy zafungují). Nelinearitu (nutnou pro interakci) zde nahrazují vlastnosti kvantového měření. Proces měření je proces *nelineární* – nezachovává lineární kvantové superpozice, protože při něm dochází k tzv. kolapsu vlnové funkce. Je to ale také proces *náhodný*, neboť předem nevíme, jaký výsledek obdržíme – superpozice náhodně zkolabuje do jedné ze svých bázových složek, a správné funkci hradla tedy odpovídají pouze některé výsledky (proto mluvíme o nedeterministickém chování hradel).

Jinými slovy: Podle toho, jaký výsledek dostaneme na detektorech na pomocných optických modech (na zpracovávaných qubitech samozřejmě žádné přímé měření neprovádíme), poznáme, zda požadovaná operace byla úspěšně vykonána či nikoliv. Úspěšnost hradla je tedy z principu vždy nižší než

100 %. Vzdor této zásadní nevýhodě však mohou být nedeterministická hradla vhodnější než technologicky značně limitovaná hradla s optickými nelineárními prvky.

Umíme tedy sestavit kvantový obvod s výhradně lineárními optickými prvky, ovšem fungující úspěšně pouze s určitou pravděpodobností. Pro nejjednodušší LOQC variantu hradla C-NOT vychází pravděpodobnost úspěchu 1/16. Je zřejmé, že pravděpodobnost úspěšného zafungování vícehradlového obvodu sestaveného z takových nedeterministických hradel bude s rostoucím počtem hradel rychle klesat. Naštěstí existuje způsob, jak pravděpodobnost úspěchu jednotlivých hradel zvýšit, teoreticky dokonce libovolně blízko jedné. Podstata použitého „triku" je založena na *kvantové teleportaci* [3].

Teleportační „udělátko" je nezbytným artiklem každého správného sci-fi filmu. Na rozdíl od filmařů jsou sice fyzikové v současnosti schopni kvantově teleportovat pouze jednotlivé částice, ale i tak se jedná o pozoruhodnou věc. Kvantová teleportace nachází zajímavá uplatnění i při kvantovém přenosu a zpracování informace. V roce 1999 Gottesmann a Chuang ukázali, jak ji využít i při konstrukci kvantových hradel [4]. Pomocí teleportace je totiž možné nejen přesně zrekonstruovat (obecně neznámý) stav kvantového systému někde jinde (může to být libovolně daleko, nicméně rychlost přenosu nikdy nepřekročí rychlost světla), ale také ho požadovaným způsobem pozměnit, například provést na něm určitou „logickou" operaci.

K tomu sice potřebujeme předem připravit určitý pomocný systém v poměrně složitém přesně definovaném tzv. *entanglovaném stavu*, ale tento stav závisí pouze na tom, jakou operaci chceme provést, nikoli na stavech vstupních qubitů. Takový stav můžeme vytvořit pomocí nedeterministických hradel (jeho přípravu můžeme opakovat tak dlouho, až se nám podaří). V případě potřeby pak takto „off-line" připravenou operaci aplikujeme prostřednictvím teleportace na qubity zakódované ve stavech příchozích fotonů.

Qubit by mohl být reprezentován stavem elektronu v polovodičové struktuře zvané kvantová tečka.

Bohužel ani teleportaci nelze pomocí lineárních optických elementů provést se stoprocentní účinností. Budeme-li ale zvyšovat počet pomocných fotonů, lze se účinnosti 100 % libovolně přiblížit. Celé hradlo se tím však výrazně komplikuje a příprava vhodného stavu pomocného systému může pak být značně zdlouhavá.

Závěrem se zmiňme o několika dalších problémech, které obecně kvantově optické systémy doprovázejí. Především zatím neexistují spolehlivé *jednofotonové zdroje*. Když si uvědomíme, že běžná žárovka produkuje asi 10^{19} fotonů za sekundu, lze tušit, o jak obtížný úkol se jedná, máme-li připravit přesně jeden foton. Další problém je s *detektory světla*. Když už máme v obvodu jeden či dva fotony, musíme je také umět detekovat a zjistit jejich počet. Doposud nemáme detektory, které by dokázaly spolehlivě rozlišit např. alespoň jeden a dva fotony. Současné detektory pouze poznají, zda na ně nějaké fotony dopadly nebo nedopadly, a i to pouze s účinností nanejvýš tak kolem 70 %. Potíže samozřejmě způsobuje také šum reálných detektorů.

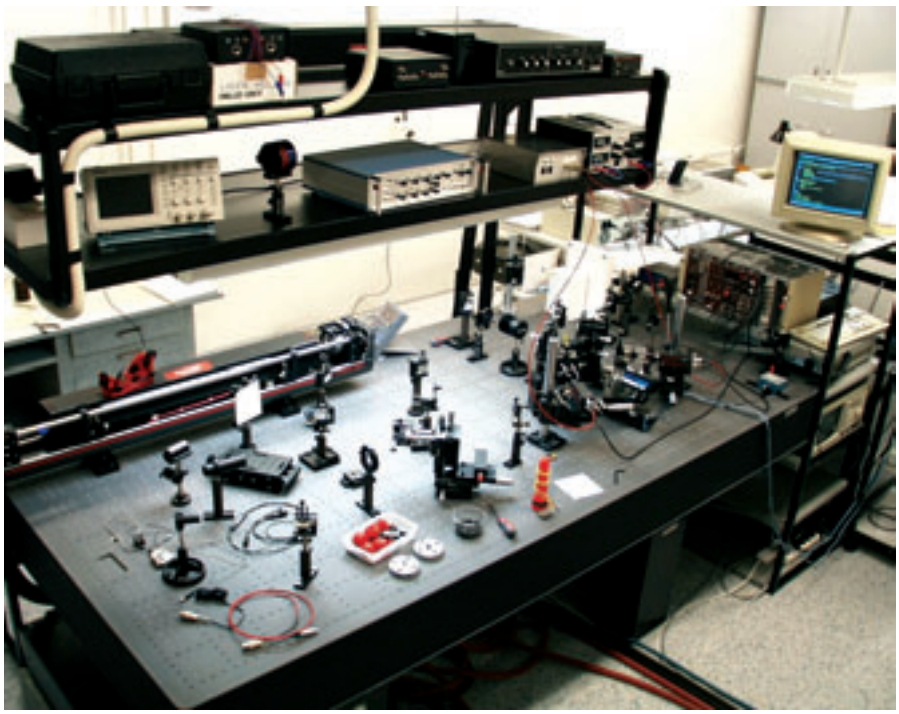
Důležitou výhodou optického kvantového počítání je kompatibilita s kvantovými komunikačními prostředky, které je v mnoha ohledech užitečné budovat právě na bázi kvantové optiky. Fotony nesoucí qubity mohou být přivedeny přímo na vstup optického kvantového počítače. I když použití nedeterministických hradel při konstrukci kvantových počítačů je stále diskutabilní, mohou se taková hradla uplatnit v jednodušších kvantových „logických" obvodech použitelných v kvantových komunikačních systémech.

Kvantová elektrodynamika v dutině

Někde na rozhraní iontů v pasti a kvantové optiky se nachází další adept pro realizaci kvantového počítání. Je jím kvantová elektrodynamika v rezonátoru (dutině), tedy CQED – z anglického *Cavity Quantum ElectroDynamics*. Popišme si stručně princip této metody, aniž bychom však zacházeli do hlubších podrobností.

Podobně jako v případě iontů v pasti, i zde jsou nositeli informace jednotlivé atomy. Pomocí speciálních technik jsou umístěny mezi dvě vysoce odrazivá zrcadla (tedy do optického rezonátoru). Do energetických stavů každého atomu v rezonátoru lze zakódovat stav qubitu. Tyto vnitřní stavy atomů (tedy stavy jednotlivých qubitů) lze ovládat pomocí vhodných laserových pulzů, což umožňuje realizovat jednoqubitová hradla.

Jak ale zařídit, aby atomy interagovaly mezi sebou a abychom mohli vytvořit i vícequbitová hradla? K tomu účelu poslouží tzv. *rezonátorový mod* záření. Mezi zrcadly rezonátoru může totiž vznikat stojaté elektromagnetické vlnění – takovým stojatým vlnám říkáme rezonátorové mody. V rezonátoru může



Kvantové počítání zatím ještě znamená především experimenty, spoustu přístrojů a hodně trpělivosti. Podobně jako na tomto obrázku z jedné vídeňské laboratoře to dnes vypadá na stolech mnoha světových výzkumných pracovišť - zpravidla nejviditelnější komponentou kvantového počítače je komplikovaný laserový systém.

být třeba jen jeden foton, nebo v něm nemusí být žádný foton, ale také může být záření v rezonátoru popsáno superpozicí těchto stavů, nebo může být dokonce *entanglováno* se stavy atomů. Atom může za vhodných podmínek foton do rezonátorového modu vyslat, nebo ho z něj naopak pohltit – to je podstatou interakce dvou qubitů.

Ve skutečnosti je situace poněkud složitější. Důležité je, aby atom nemohl s polem v rezonátoru interagovat, „kdy se mu zlíbí" – chceme, aby spolu vzájemně interagovaly jen ty atomy (qubity), které vybereme. V praxi k tomu potřebujeme ještě další energetickou hladinu v atomech a laserové svazky s regulovatelnou intenzitou, kterými si na zvolené atomy „posvítíme".

Experimenty s CQED již byly provedeny, mj. s atomy rubidia (viz např. [5]). Počítá se s tím, že by operace bylo možné realizovat řádově na desítkách qubitů. I zde je samozřejmě největším nepřítelem nechtěná interakce s okolím – dekoherence. Je způsobena jednak spontánní emisí z pomocné energetické hladiny atomů, ale také ztrátami a znáhodněním fáze záření v rezonátoru.

Kvantové tečky

Jak jsme viděli, vhodnými objekty pro reprezentaci qubitů jsou např. atomy (případně ionty nebo jádra atomů). Jednotlivé atomy jsou však příliš malé a velmi nesnadno se s nimi manipuluje jako s individuálními objekty. Dnes nicméně známe objekty, které se atomům v některých důležitých ohledech velmi podobají a práce s nimi není technicky tak nesnadná. Jsou to tzv. polovodičové *kvantové tečky* a jejich soustavy neboli agregáty (např. dvojice atd.) [6, 7].

Co je to kvantová tečka? Jak známo, každý polovodič může obsahovat nosiče náboje, díky nimž je částečně vodivý. Nosiči náboje mohou být vodivostní elektrony a díry, zde ale budeme pro jednoduchost mluvit jenom o elektronech.

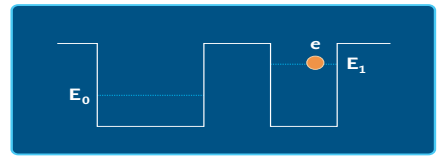
Různé polovodiče se od sebe liší v řadě ohledů. Jednou z důležitých vlastností, kterými se polovodiče mohou vzájemně odlišovat, je charakteristická úroveň potenciální energie, na které se elektrony v polovodiči pohybují (fyzikové mluví o energii dna vodivostního pásu). Mysleme si, že máme dva různé polovodiče, které se liší svými fyzikálními vlastnostmi, a označme si je písmeny *T* a *M*. Kdybychom chtěli přenést elektron z polovodiče *T* do polovodiče *M*, ve kterém je úroveň potenciální energie elektronu vyšší než v polovodiči *T*, museli bychom elektronu dodat určitou energii, která by mu umožnila příslušný potenciální rozdíl překonat. Kdyby ale elektron takovou energii nedostal, zůstal by ve svém pohybu omezen na oblast polovodiče *T* (zůstal by lokalizován v polovodiči *T*).

Této charakteristické vlastnosti polovodičů je využito při vytváření kvantových teček. Představme si, že do vzorku materiálu typu *M* umístíme, jako rozinku dovnitř vánočky, malé zrnko materiálu typu *T*. Elektrony v polovodiči *T* zůstanou v tomto zrnku lokalizovány, pokud nedostanou energii dostatečnou k přechodu do polovodiče *M* (přesněji řečeno, budou lokalizovány přibližně v oblasti, ve které se rozprostírá materiál typu *T*). Mají-li dva polovodičové materiály ve výše zmíněné polovodičové struktuře tyto vlastnosti, mluvíme o polovodičové kvantové tečce.

Pojem *tečka* samozřejmě pochází od velmi malých rozměrů těchto útvarů. Proč ale říkáme, že je tečka *kvantová*? Je-li např. tečka z materiálu GaAs (arsenid galia) obklopena materiálem AlGaAs, pak se při rozměrech tečky kolem několika desítek nanometrů projeví (v důsledku platnosti kvantověmechanických zákonitostí) diskrétní struktura možných energií elektronu uvnitř tečky. V tom je pak kvantová tečka podobná jednotlivým atomům nebo malým molekulám. Typické rozdíly mezi energiemi jednotlivých lokalizovaných stavů elektronu v tečce jsou jednotky až desítky milielektronvoltů ($1\ \mathrm{eV} = 1{,}602 \times 10^{-19}$ J). Díky současným technologickým postupům si už dokážeme opatřit „umělé atomy" – kvantové tečky, s poměrně rozsáhlými možnostmi volby jejich vlastností.

Vraťme se však k otázce kvantového počítače. Docela realistická je představa, že máme kvantovou tečku, která má dvě diskrétní energetické hladiny a jenom jeden elektron. Taková kvantová tečka by mohla být vhodnou reprezentací kvantového bitu. Stav kvantové tečky s elektronem na energetické úrovni s nižší energií bychom mohli považovat za stav $|0\rangle$ kvantového bitu, zatímco stav s elektronem na vyšší energii by odpovídal stavu $|1\rangle$. Jelikož je kvantová tečka kvantověmechanický systém, je dobře myslitelné přivést kvantovou tečku do stavu, který je lineární superpozicí obou stavů $|0\rangle$ a $|1\rangle$.

Kvantový bit by bylo možné realizovat v kvantových tečkách i jinak. Například by nám stačila kvantová tečka s jedním lokalizovaným elektronovým stavem. Stav kvantové tečky



Kvantový bit konstruovaný na základě jednoho elektronu a dvou interagujících kvantových teček. Tečky jsou schematicky představeny pomocí dvou kvantových jam, mezi nimiž může elektron tunelovat, E_0 a E_1 označují energetické hladiny elektronu (e).

s jedním elektronem umístěným v tomto stavu by mohl být stavem $|1\rangle$ kvantového bitu, zatímco stav tečky bez elektronu by byl stavem $|0\rangle$. Nabízí se i další možná realizace kvantového bitu. V jediném lokalizovaném stavu v kvantové tečce by se nacházel právě jeden elektron, přitom dva stavy kvantového bitu by se lišily spinem elektronu.

Uvedené příklady představují možné realizace kvantového bitu v individuální kvantové tečce. Určité nadějné možnosti, jak uskutečnit v praxi kvantový bit, lze očekávat i v oblasti agregátů kvantových teček. Tak například ve dvojici kvantových teček sdílející jeden elektron by stavy kvantového bitu mohly odpovídat lokalizaci elektronu v jedné nebo druhé z kvantových teček. Jak ale dosáhnout přechodu kvantového bitu z jednoho stavu do stavu jiného? V případě kvantových bitů realizovaných pomocí posledně zmíněné dvojice kvantových teček by takovou operaci bylo možné provést s využitím kvantověmechanického jevu zvaného *tunelování*, díky němuž může elektron pronikat potenciálovou bariérou oddělující dvě sousedící kvantové tečky.

Pomocí tohoto mechanismu (pozoruhodné účinky tunelovaní koneckonců známe nejen z kvantové fyziky...) by s kvantovým bitem bylo možné uskutečnit některé operace kvantového počítání. Přiloženým elektrickým potenciálem přivedeným ke kvantové tečce pomocí vodivých struktur (v zásadě realizovatelných současnou polovodičovou technologií) je totiž možné měnit potenciálovou bariéru mezi tečkami a v důsledku toho ovládat stav kvantového bitu.

Mohlo by se snad zdát, že cesta k uskutečnění kvantového počítání s využitím kvantových teček bude celkem přímočará. Bohužel tomu tak prozatím není. Na rozdíl od jednotlivých a izolovaných atomů, ve vzorku s kvantovými tečkami jsou, jako v každé pevné látce, přítomny kmity krystalové mříže (kolektivní kmity jader atomů kolem jejich rovnovážných poloh) a ty mají často na chování elektronu značný vliv. Elektron může spontánně předávat mřížovému pohybu část své energie a sám může v průběhu tohoto vzájemného působení měnit svůj stav – v rozporu s tím, co bychom si přáli. Ukazuje se, že vliv těchto spontánních procesů na operace, které bychom rádi s kvantovým bitem prováděli, může být dost destruktivní. Otázka, jak uskutečnit kvantové počítání pomocí kvantových teček a podobných nanostruktur, proto bude nelehkou úlohou nejen pro fyziku, ale i pro další obory, jako je matematika, informatika a příbuzné technické vědy.

Porovnání platforem

Fyzikální platforma	Čas potřebný pro jednu operaci [s]	Dekoherenční čas [s]	Počet qubitů
Chladné ionty	10^{-7}	10^{-1}	50
NMR	10^{-4}	10^{4}	100
CQED	10^{-14}	10^{5}	10 – 100
Kvantové tečky	10^{-9}	10^{-6}	1000

Údaje v tabulce jsou orientační a spíše nadhodnocené vzhledem k současným technologickým možnostem (teoretická mez u NMR a současný stav, to je opravdu propastný rozdíl - viz minulý díl). Podíl hodnot v druhém a prvním sloupci naznačuje, kolik operací lze na dané platformě provést. (Všimněte si, že chybí LOQC. Pro něj není vzhledem k nedeterministickému přístupu tento typ údajů příliš vhodným ukazatelem.)

Opatrně optimistický závěr

V článku jsme naznačili možnosti pěti dnes v úvahu připadajících fyzikálních principů, které by v budoucnu mohly vést k sestrojení prakticky použitelného kvantového počítače. Porovnání jejich teoretických možností najdete v připojené tabulce převzaté z [8], ta ovšem nic neříká o jejich vyhlídkách na skutečnou realizaci. Fakt je, že žádná z metod zatím není dále než v oblasti laboratorních experimentů. Ale kdo ví, co bude za pár roků? Ostatně, řekli byste ještě někdy v polovině devadesátých let, jak brzy budeme znát lidskou DNA?

■ ■ ■ 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 FZÚ AVČR.

Tento článek vznikl v rámci realizace grantových projektů GAAV ČR č. IAA1010113 , MŠMT ČR č. OCP5.20 (K. K.), MŠMT ČR č. RN19982003014 (M. Č . a K. K.), projekt AVČR AVOZ1-010-914 (M. Č . a K. K.) a MŠMT ČR č. LN00A015 (M. D.)

Literatura:

[1] J. Milburn, Phys. Rev. Lett. 62 2124 (1989).
[2] E. Knill et al., Nature 409, 46 (2001).
[3] C. H. Bennet et al., Phys. Rev. Lett. 70, 1895 (1993).
[4] D. Gottesmann, I. L. Chuang, preprint na arXiv.org: quant-ph/9908010 (1999).
[5] L. You, M. S. Chapman, Phys. Rev. A, 62, (2000).
[6] D. Loss, D. P. DiVincenzo, Phys. Rev. A, 57, 120 (1998).
[7] J. Brown, New Scientist, 24, 21 (1994).
[8] J. Brown, Mind, Machines and the Multiverse: The Quest for the Quantum Computer (Simon & Schuster, 2000).