Igor Jex

Kvantové počítače

Pokroky matematiky, fyziky a astronomie, Vol. 41 (1996), No. 6, 311--317

Persistent URL: http://dml.cz/dmlcz/137609

Kvantové počítače

Igor Jex, Praha

Kvantové počítače jsou fyzikální systémy zahrnující kvantové soustavy, jejichž časový vývoj se dá chápat jako jistý druh výpočtu. Příspěvek podává některé základní definice a možné způsoby realizace.

Úvod

Počítače se staly naším každodenním společníkem. Pronikly do všech oblastí lidské činnosti a znásobily tak naše možnosti. Počítače mají dlouhou historii sahající hluboko do minulosti. Od jednoduchých počítadel přes mechanické kalkulátory až k dnešním superpočítačům jejich vývoj přímo odrážel technologickou vyspělost naší civilizace. V čem ale spočívá skutečný rozdíl mezi dnešním počítačem a (v případě, že by byl dokončen) kalkulátorem Charlese Babbagea? Rozdíl je v první řadě technologický. V současnosti používáme podstatně rychlejší součástky na bázi polovodičů, díky kterým jsme podstatně zkrátili dobu elementárních úkonů. Existují ale úlohy, pro které jsou i současné počítače beznadějně pomalé. Takovou úlohou je například rozklad velkých (mnohociferných) čísel na prvočinitele.

Představte si, že dostaneme za úkol najít dva netriviální dělitele daného čísla, třeba čísla 27233. Pomocí papíru a tužky by nám to zabralo zcela jistě víc než pár minut. Ověřit, že uvedené číslo je součinem 113 a 241, bude trvat několik sekund (opět jenom s použitím papíru a tužky). Důvod, proč tomu tak je, nemá svoji příčinu v tom, že někdo počítá pomaleji a druhý rychleji, ale v tom, že zatím lidstvo nenašlo rychlý (efektivní) algoritmus pro rozklad čísla na prvočinitele. Pro násobení takový algoritmus známe a učili jsme se ho na základní škole.

Zda je algoritmus pomalý nebo rychlý, se dá samozřejmě specifikovat přesněji. Pro pomalé algoritmy je typické, že počet kroků nutných k jejich vykonání roste exponenciálně s velikostí vstupu, tj. s počtem cifer čísla N v binárním zápisu. Například elementární postup při prvočíselném rozkladu čísla N je zkusit vydělit dané číslo všemi čísly menšími nebo nanejvýš rovnými $\sqrt{N}$. Počet čísel S, která je třeba ověřit, roste jako

$$S \approx k \exp(\tfrac{1}{2} \log_2 N),$$

kde $\log_2 N$ udává velikost vstupu. Poznamenejme také, že elementární testy dělitelnosti tento počet drasticky nemění, tj. závislost by byla exponenciální, i když s trochu jiným faktorem k. V případě rychlých algoritmů by měla být závislost ne exponenciální, ale polynomiální

$$S \approx P_l(\log_2 N),$$

Ing. Igor Jex, CSc. (1962), katedra fyziky FJFI ČVUT Praha, Břehová 7, 115 19 Praha.

kde P je polynom jistého stupně l.

Může se zdát, že v praktickém životě na problémy spojené s rychlostí algoritmů narážet nebudeme. Rozvoj komunikace nás ale už dlouho učí něčemu jinému. S rostoucí možností komunikace roste i potřeba lidí zachovat si jistou míru soukromí nebo alespoň některé informace a zprávy si ponechat jen mezi sebou a osobou, pro kterou jsou určeny. Tohoto cíle je většinou dosaženo použitím tajného klíče nebo metody, která pro nezasvěceného navzdory své jednoduchosti bude vyžadovat obrovské materiálové nebo časové náklady.

Kryptografie

Jednou ze spolehlivých metod, jak ukrýt svoji zprávu, je šifrování pomocí metody RSA [1]. Velikou výhodou této metody je, že zašifrovat může kdokoliv. Klíč je veřejně přístupný třeba ve formě seznamů čísel podobných telefonním seznamům. Dešifrovat zprávu může ale jenom ten, kdo zná tajný klíč. Získat klíč je z veřejně dostupných dat (seznamů) v principu možné, prakticky ale neproveditelné.

Představme si, že převedeme tajnou zprávu na jedno číslo, které si označíme jako M. Abychom mohli dané číslo bezpečně odeslat libovolným veřejným informačním kanálem, odesílatel si v příslušném seznamu najde dvě čísla uvedená pro příjemce, a to e a m. Číslo $m = pq$ je voleno ve formě součinu dvou velkých prvočísel (typicky padesát až stociferných). Zprávu M, kterou chceme poslat, zakódujeme následovně

$$T = M^e \pmod{m},$$

kde $\bmod m$ je zbytek při dělení M^e číslem m. Číslo T se veřejným kanálem odešle. V případě, že by zpráva M byla delší než m, rozdělíme ji na úseky kratší než m a každý úsek zakódujeme zvlášť. Příjemce zná pro zvolený exponent e příslušný inverzní exponent f takový, že

$$M = T^f \pmod{m},$$

a provedením umocnění si zpětně zprávu dešifruje. Bezpečnost uvedeného způsobu komunikace se zakládá na exponenciální časové náročnosti úlohy najít exponent f v případě neznalosti dělitelů čísla m. Exponent f je možno určit pomocí vztahu

$$f = e^{\Phi(\Phi(m))-1} \pmod{\Phi(m)},$$

kde $\Phi(x)$ udává počet čísel nesoudělných s x a menších než x. V případě čísla m by platilo $\Phi(m) = (p-1)(q-1)$. Čistě pro ilustraci si čtenář může zkusit zašifrovat a dešifrovat třeba číslo $M = 5$ pomocí exponentu $e = 11$ a modulu $m = 187$. Kdybychom pro reálný případ skutečně chtěli za každou cenu zprávu dešifrovat, nejspíš bychom spustili řadu počítačů a hledali neznámé dělitele (nebo se poohlédli na stole u příjemce). Zdá se tedy, že máme skutečně bezpečný způsob, jak komunikovat v soukromí. Situace

se ale může změnit. Existují totiž návrhy pro principiálně sestrojitelné fyzikální zařízení, které jsou schopny realizovat obrovské množství paralelních výpočtů najednou. Ukazuje se, že k dosažení tohoto cíle je nutné použít kvantové systémy [2, 3, 4]. Proti klasickým počítačům jsou kvantové počítače schopny realizovat některé výpočty, které v klasickém případě potřebují ke své realizaci čas exponenciálně narůstající s délkou vstupu. Kdyby tyto systémy skutečně byly realizované, soukromí při komunikaci touto metodou by nemohlo být garantováno.

Kvantová mechanika

Představme si dvouhladinový kvantový systém, jehož stavy popíšeme stavovými vektory $|x\rangle$, kde $x = 0, 1$. Tento systém je zvykem označovat jako *kvantový bit* neboli *qubit*. V klasickém případě takový systém s dvěma možnými stavy je buď ve stavu 0 nebo 1. Analogický kvantový systém je možno připravit v libovolné komplexní lineární superpozici těchto dvou stavů

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

s normovací podmínkou $|c_0|^2 + |c_1|^2 = 1$. S každým stavem je možno manipulovat prostřednictvím unitárních operací. Označíme-li $|0\rangle = \binom{1}{0}$, $|1\rangle = \binom{0}{1}$, pak obecná unitární operace je reprezentována parametrizovanými unitárními maticemi 2×2, typů

$$R_1 = \begin{pmatrix} \exp(\mathrm{i}\alpha)\cos\varphi, & \exp(\mathrm{i}\beta)\sin\varphi \\ -\exp(\mathrm{i}\alpha)\sin\varphi, & \exp(\mathrm{i}\beta)\cos\varphi \end{pmatrix}$$

nebo

$$R_2 = \begin{pmatrix} \exp(\mathrm{i}\alpha)\cos\varphi, & \mathrm{i}\exp(\mathrm{i}\beta)\sin\varphi \\ \mathrm{i}\exp(\mathrm{i}\alpha)\sin\varphi, & \exp(\mathrm{i}\beta)\cos\varphi \end{pmatrix}.$$

Jako speciální příklad můžeme zvolit matici realizující rotaci o úhel $\varphi = 45°$ ($\alpha = \beta = 0$)

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & -1 \\ 1, & 1 \end{pmatrix}.$$

Pomocí těchto transformací jsme schopni s libovolnou přesností aproximovat předepsanou transformaci, a to pomocí polynomiálního počtu kroků.

Pomocí elementárních jednotek — qubitů můžeme následně zkonstruovat *kvantový registr* neboli soustavu (vzájemně neinteragujících) qubitů. Předpokládejme, že počet těchto jednotek je k. Stav celého registru je pak možno psát jako

$$|\Psi\rangle = \sum_{n=00\ldots0}^{11\ldots1} c_n|n\rangle.$$

Kvantový stav $|0\rangle$ odpovídá situaci, kde každá z jednotek se nachází ve stavu 0, stav $|11\ldots1\rangle$ stavu se všemi qubity ve stavu $|1\rangle$. Celkově máme takto k dispozici 2^k stavů.

K důležitým unitárním operacím realizovaným nad registrem patří diskrétní Fourierova transformace [5, 6, 7, 8]. Tato transformace je schopna převést registr z daného stavu $|n\rangle$ do stavu, kde bude všech $K = 2^k$ stavů zastoupeno se stejnou statistickou vahou. Transformační matice $k \times k$ má obecný tvar (s přesností na fázi)

$$U = \frac{1}{\sqrt{k}} \begin{pmatrix} 1, & 1, & \ldots, & 1 \\ 1, & x, & \ldots, & x^{k-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1, & x^{k-1}, & \ldots, & x^{(k-1)(k-1)} \end{pmatrix},$$

kde $x = \exp(\mathrm{i}2\pi/k)$. Podotkněme ještě, že stejně jako Fourierovu transformaci i všechny ostatní použité operace v případě kvantových počítačů je možné velice efektivně realizovat. Pro jejich implementaci je vždy nutný pouze polynomiální počet kroků. Díky tomuto faktu nedojde k rozhodujícímu zpomalení výpočtu z důvodu konstrukce zařízení.

Předpokládejme teď, že máme za úkol najít dělitele jistého čísla N. Tímto problémem se zabýval P. Shor [9] a ukázal, že pomocí kvantových počítačů je úkol možné řešit za exponenciálně kratší čas, než je tomu v případě klasických počítačů a algoritmů, tj. v polynomiálním čase.

V úvodu jsme uvedli, že nejjednodušším způsobem je zkoušet jako dělitele všechna čísla nanejvýš rovna $\sqrt{N}$ (metoda hrubé síly). Díky faktu, že kvantová teorie je lineární a jako vstup lze použít libovolnou superpozici, byl by kvantový počítač schopen dojít ke správnému výsledku v průběhu jednoho výpočtu. Dejme tomu, že superpozice by vypadala následovně:

$$|\Psi\rangle = \frac{1}{2^{k/2}} \sum_{n=00\ldots0}^{11\ldots1} |n\rangle.$$

Problémem by v tomto okamžiku ale bylo, jak správný výsledek vyčíst z obrovského množství výstupních údajů, kterých bude 2^k; srovnání s hledáním jehly v kupce sena je více než výstižné! V podstatě si však musíme poradit ještě s jedním problémem. Když se totiž podíváme na jeden z výsledků, víme z kvantové teorie, že automaticky ztratíme všechny ostatní výsledky a v případě nevyhovujícího výsledku, který je velice pravděpodobný, jsme nuceni spustit výpočet znovu (problém redukce v kvantové teorii měření). Tímto postupem bychom ale nedělali nic jiného, než co dělá klasický počítač.

Podstatné zjednodušení řešení tohoto problému navrhl P. Shor [9]. Úlohu najít rozklad čísla na jeho prvočinitele převedl na úlohu najít periodu vhodně zvolené funkce a pomocí zjištěné periody najít vhodného kandidáta pro prvočíselný rozklad. Když takového kandidáta najdeme, je lehké ověřit, zda tento kandidát skutečně je řešením našeho problému.

Shorův algoritmus

Základem pro Shorův algoritmus je řešení rovnice

$$z^2 \equiv 1 \pmod{N},$$

která pro složená čísla má kromě triviálních řešení $z \equiv \pm 1 \pmod{N}$ i netriviální řešení $z \equiv \pm a \pmod{N}$. Řešení možno najít následujícím postupem. Zvolíme si náhodně $y < N$. Pro nesoudělná y a N existuje exponent r takový, že

$$y^r \equiv 1 \pmod{N}.$$

Pro sudé r pak nacházíme řešení

$$z = y^{r/2}$$

pro výchozí kvadratické rovnice a tím i kandidáta na netriviální dělitel čísla N. Jako ilustrativní příklad se můžeme pokusit rozložit na prvočinitele číslo 21. Zvolme si $y = 2$ a spočítáme zbytek 2^j po dělení 21 (funkce je periodická). Zjistíme, že v tomto případě $r = 6$ (perioda funkce). Z toho plyne dál, že $z = 2^3 = 8$ a následně máme jako možné dělitele 21 čísla 7 nebo 9.

Implementace této metody pro rozklad čísla N na kvantovém počítači pak vypadá takto. Potřebujeme najít periodu funkce $f_N(x) = y^x \pmod{N}$, tj. takové r, že $f_N(x + r) = f_N(x)$. Pro začátek potřebujeme kvantový systém složený ze dvou registrů stejné délky L vytvořené z l qubitů $L = 2^l$ a budeme dále předpokládat, že $L > N^2$. Počáteční stav obou registrů bude

$$|0\rangle|0\rangle.$$

První registr převedeme pomocí Fourierovy transformace do superpozice se všemi stavy $|x\rangle$ zastoupenými se stejnou pravděpodobností

$$\frac{1}{\sqrt{L}} \sum_x |x\rangle|0\rangle.$$

Náhodně zvolíme y a necháme spočítat pro každé x hodnotu $f_N(x)$, která bude uložena v druhém registru. Po realizaci výpočtu bude soustava dvou registrů ve stavu

$$\frac{1}{\sqrt{L}} \sum_x |x\rangle|f_N(x)\rangle.$$

Provedeme zpětnou transformaci na prvním registru a tím převedeme systém do stavu

$$\frac{1}{L} \sum_{x,n} \exp(\mathrm{i}2\pi nx)\, |n\rangle|f_N(x)\rangle.$$

V tomto okamžiku se hodnoty prvého registru zkoncentrovaly (díky periodicitě funkce $f_N(x)$ a realizované transformaci) kolem násobků základní frekvence L/r. Měřením na prvním registru získáme hodnotu h, která bude velice blízká jistému násobku základní frekvence jL/r. Ze znalosti k a L jsme pak schopni najít hledanou periodu r pomocí klasických, ale (v počítačovém smyslu) efektivních metod.

Předložená metoda je svou povahou statistická. Ne každý běh kvantového počítače dává hledaný výsledek. Může například dojít k tomu, že se náhodně zvolí nevhodné číslo y. To ale nepředstavuje nijak zvláštní problém nebo překážku. Několik opakování

běhu počítače nezpůsobí exponenciální zpomalení výpočtu, ale vede k nalezení správného kandidáta. Z fyzikálního hlediska je podstatně nebezpečnější vliv ztrát a okolí na fungování registrů. Vlivem okolí některé realizace kvantové dynamiky mají větší pravděpodobnost, což způsobuje, že na druhém registru nebudeme mít k dispozici dostatečný počet reprezentativních výsledků. Pak nám ani Fourierova transformace nepřinese hledaný výsledek — museli bychom počítač použít opakovaně stejně často jako klasický počítač, což by vedlo k exponenciálnímu zpomalení výpočtu, a tedy efektivnímu znehodnocení Shorova algoritmu [10].

Druhým kritickým momentem celé konstrukce je vliv chyb v systému. V každém kroku, když dochází k manipulaci s qubity, máme co činit s problémem přesně nastavit (spojité) parametry transformací. Zdaleka není triviální tento druh chyb dostat pod kontrolu a zaručit tak spolehlivé fungování celého systému.

Kvantové obvody a logické jednotky

Ukázali jsme, jaké transformace potřebujeme pro realizaci kvantového počítače. Stejně jako v případě klasických počítačů je možné i pro kvantové počítače navrhnout elementární stavební jednotky — *logické obvody* [11]. Z fyzikálního hlediska jsou tyto obvody konstruovány ze dvou kvantových podsystémů. V závislosti na stavu jednoho podsystému je realizován jistý druh unitární evoluce na druhém (řízeném) podsystému [12, 13, 14, 15, 16]. Dynamika může vypadat následovně

$$\hat{U} = \sum_k |k\rangle\langle k| \otimes \hat{U}_k = \sum_k \hat{P}_k \otimes \hat{U}_k.$$

Projektory $\hat{P}_k$ představují řídící systém a unitární transformace $\hat{U}_k$ představují časový vývoj řízeného systému. Nejjednodušším příkladem logického obvodu je analogie klasického řízeného NOT. Jeho kvantová obdoba je popsána transformací

$$|\varepsilon_1\rangle|\varepsilon_2\rangle \longrightarrow |\varepsilon_1 \oplus \varepsilon_2\rangle|\varepsilon_2\rangle$$

soustavy složené ze dvou qubitů, kde operace $\oplus$ značí součet modulo 2. Jednoduchým rozšířením řízeného NOT získáme univerzální logickou jednotku, pomocí které je možné vybudovat libovolný logický obvod [13, 15].

Nezodpovězenou otázkou stále ještě zůstává, jaké fyzikální procesy jsou schopné indukovat požadovanou dynamiku. V tomto směru jsou slibné nedávné experimenty s chladnými ionty v magnetických pastech, mikrodutinová dynamika a kvantové tečky [17, 18]. V případě atomových systémů je řízeným systémem Rydbergovský atom a řídícím systémem je kvantované elektromagnetické pole v dutině (rezonátoru). Další eventualitou mohou být polarizované fotony [19, 20].

Kvantové počítače mají za sebou období bouřlivého rozvoje hlavně v rovině teoretické. Experimenty v tomto směru jsou zatím na počátku [17, 18]. I když praktická implementace je zcela jistě stále ještě spíše vizí, nová problematika stimulovala výzkum

v oblasti teorie algoritmů, zpracování a přenosu informací stejně jako v oblasti kvantové optiky. Vidíme zde i fascinující ilustraci, jak základní koncepce kvantové teorie lze využít v oblasti na první pohled odtažité, jako je rozklad na prvočinitele nebo realizace výpočtů. Lineárnost a interference amplitud pravděpodobnosti je využita ve formě masivního paralelismu pro „napočítání" dostatečného počtu testovaných příkladů. Tzv. kvantové provázání (entanglement) [4] je efektivně využito při interakci registrů a projekční postulát a neurčitost se uplatní při odečítání výsledků registru pro získání konečného výsledku výpočtu [21, 22].

Literatura

[1] M. R. SCHROEDER: *Number theory in science and communication.* Springer Verlag, Berlin 1986.
[2] R. P. FEYNMAN: Int. J. Theoret. Phys. *21* (1982), 467.
[3] D. DEUTSCH: Proc. Roy. Soc. (London) A *400* (1985), 97.
[4] A. PERES: *Quantum Theory — Concepts and Methods.* Kluwer Academic Publishers, Dordrecht, 1993.
[5] A. ZEILINGER, M. ZUKOWSKI, M. A. HORNE, H. J. BERNSTEIN a D. M. GREENBERGER: In *Fundamental Aspects of Quantum theory,* eds. J. Anandan and J. L. Safko (World Scientific, Singapore) 1994.
[6] K. MATTLE, M. MICHELER, H. WEINFURTER, A. ZEILINGER a M. ZUKOWSKI: Appl. Phys. B *60* (1995), S111.
[7] M. RECK, A. ZEILINGER, H. J. BERNSTEIN a P. BERTANI: Phys. Rev. Lett. *73* (1994), 58.
[8] P. TÖRMÄ, S. STENHOLM a I. JEX: Phys. Rev. A *52* (1995), 4853.
[9] P. W. SHOR: Proceedings of the 35th Annnual Symposium on Foundations of Computer Science (IEEE Press, Piscataway, NJ, 1994).
[10] P. W. SHOR: Phys. Rev. A *52* (1995), R2493.
[11] D. DEUTSCH: Proc. Roy. Soc. (London) A *425* (1989), 73.
[12] J. I. CIRAC a P. ZOLLER: Phys. Rev. Lett. *74* (1995), 4091.
[13] A. BARENCO, D. DEUTSCH, A. EKERT a R. JOZSA: Phys. Rev. Lett. *74* (1995), 4083.
[14] A. BARENCO, CH. H. BENNETT, R. CLEVE, DAVID P. DI VINCENZO, N. MARGOLUS, P. SHOR, T. SLEATOR, J. A. SMOLIN a H. WEINFURTER: Phys. Rev. A *52* (1995), 3457.
[15] T. SLEATOR a H. WEINFURTER: Phys. Rev. Lett. *74* (1995), 4087.
[16] I. CHUANG a Y. YAMAMOTO: Phys. Rev. A *52* (1995), 3489.
[17] C. MONROE, D. M. MEEKHOF, B. E. KING, W. M. ITANO a D. J. WINELAND: Phys. Rev. Lett. *75* (1995), 4714.
[18] Q. A. TURCHETTE, C. J. HOOD, W. LANGE, H. MABUCHI a H. J. KIMBLE: Phys. Rev. Lett. *75* (1995), 4710.
[19] S. STENHOLM: *Polarization coding of quantum information.* Preprint HU-TFT-95/31.
[20] P. TÖRMÄ a S. STENHOLM: *Polarization in Quantum Computation.* Preprint HU-TFT-96/1.
[21] CH. H. BENNETT: Physics Today *48* (1995), No. 10, p. 24.
[22] R. JOSZA a A. EKERT: Rev. Mod. Phys. (1996), v tisku.