Velmi stručný úvod do kvantového počítání

prof. RNDr. Luděk Kučera, DrSc.
MFF UK a FIT ČVUT

14. prosince 2021

Úvod

Vývoj kvantových počítačů a algoritmů pro ně je téma, které je s námi již poměrně dlouhou dobu (s přihlédnutím k tomu, co v informatice při jejím prudkém vývoji znamená "dlouhá doba"). Stále ale není jasné, zda v budoucnu kvantové počítání vyspěje do prakticky použitelných aplikací, nebo zda zůstane zajímavou teorií.

Zájem o kvantové algoritmy prudce vzrostl poté, co Peter Shor publikoval v roce 1994 algoritmus pro faktorizaci čísel, který by tento problém vyřešil v polynomiálně omezeném čase a byl by tedy prakticky využitelný, pokud by existovaly prakticky využitelné kvantové počítače (které ani letos dostupné nejsou a v informatických kruzích dosud ani není shoda na tom, zda někdy budou - přinejmenším v podobě, na které by se Shorův algoritmus dal provozovat).

Problém faktorizace čísel totiž není jen nějaký odtažitý pojem z teorie čísel, který zajímá pár podivínů, kteří se této teorii věnují. Bezpečnost kryprografického protokolu RSA, ze kterého vychází nyní všudypřítomná zabezpečená počítačová komunikace, je založena na tom, že pokud je dáno číslo n o stovkách cifer, které je součinem dvou zhruba stejných prvočísel p a q, neumíme tyto faktory nalést dostatečně rychle ani za pomoci největších současných počítačů.

Kvantové počítače by proto zcela změnily komunikaci pomoci počítačů (nutno uvést, že už teď jsou známy kryptografické protokoly, které by byly bezpečné na kvantových počítačích = jou to kvantové algoritmy, které zatím provozovat nejdou).

Obecné povědomí o tom, co pojmy "kvantový počítač" a "kvantový algoritmus" je poměrně malé, a to i na MFF UK nebo FIT ČVUT. Dají se zde nalézt specializované přednášky na tato témata, ale obvykle pro velmi úzký okruh zájemců v nejvyšších ročnících, nebo častěji až v doktorandském studiu. Mnoho studentů (a myslím i pedagogů) má představu, že kvantový počítač by v zásadě počítal stejným způsobem jako ty

současné klasické počítače, ale mnohem rychleji (aniž by byla přesnější představa o tom, co to znamená "mnohem").

Cílem tohoto textu, který se vyvinul z přednášky o teorii složitosti na FIT ČVUT, je ukázat, že matematický model, pro který jsou vytvářeny kvantové algoritmy, je zásadně odlišný od von Neumannovského modelu počítače a naznačit, jak se tento model vyvinul z kvantové teorie, která byla vytvořena začátkem minulého století a dát studentům možnost aby si sami utvořili názor na to, zda kvantové počítače jsou budoucností informatiky, nebo (z praktického hlediska) jen slepou uličkou.

Vysvětlit podrobně Shorův algoritmus není jednoduché a tento text se o to ani nepokouší, ale směřuje k tomu, aby student pochopil základní princip kvantových algoritmů na příkladu Simonova algoritmu, který se svým charakterem Shorovu dosti podobá. Základní text se snaží vysvětlit princip matematického modelu kvantového počítače a je také naznačeno, jak se problém faktorizace převede na hledání periody exponenciální funkce v modulární aritmetice, což je problém, který Shorův algoritmus řeší.

V dodatku, který čtenář, zajímající se jen o podstatu kvantových algoritmů číst nemusí, je stručně popsán RSA kryptosystém a doplněn důkaz lemmatu, užívaného pro převod faktorizace na hledání periody.

V dodatku je také popsán pravděpodobnostní Rabin-Millerův test prvočíselnosti a způsob jeho použití pro hledání velkých prvočísel, která jsou potřeba pro RSA kryptosystém.

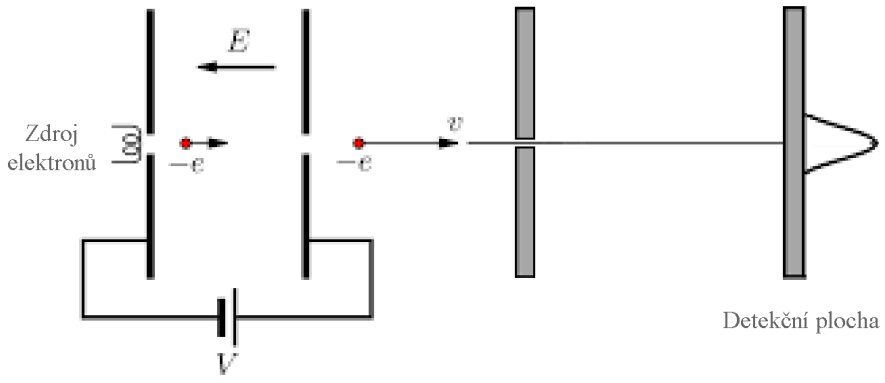
Kvantový bit (qubit)

Posíláme-li proud elektronů proti bariéře, ve které je velmi malý otvor, velikostí srovnatelný s velikostí elektronů, a měříme, jak se pohybují elektrony za bariérou, zjistí se nepřekvapivý fakt, že většina elektronů se za otvorem pohybuje ve svém původním směru. Jen málo elektronů se vydá jiným směrem (třeba jsou to ty, které narazily nebo nějak interagovaly s okrajem otvoru). Ukazuje to křivka za stínítkem s detektory na Obr. .

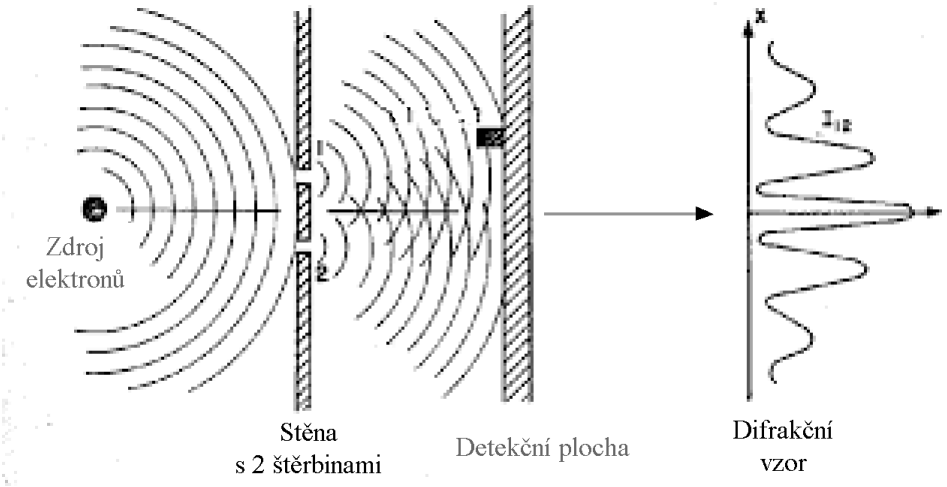
Jestliže se ale udělají otvory stejné velikosti dva, velmi blízko u sebe, pak by se dalo čekat, že budou elektrony nezávisle na sobě procházet jedním nebo druhým otvorem, a na stínítku za bariérou se objeví dvě takřka úplně se překrývající maxima výskytu elektronů.

Tak to ale ve skutečnosti nedopadne: na stínítku se objeví řada maxim ve směrech podstatně odlišných od původního směru elektronů od jejich zdroje k otvorům, viz Obr. . Maxima jsou od sebe oddělena minimy, kam elektronů dopadá jen málo.

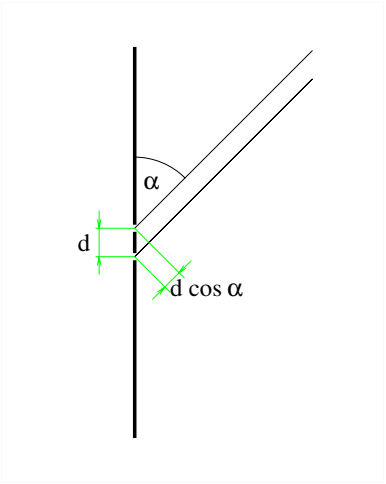
Jediný způsob, jak si dovedeme vysvětlit toto podivné chování, je následující:



Obrázek 1:



Obrázek 2:



Obrázek 3:

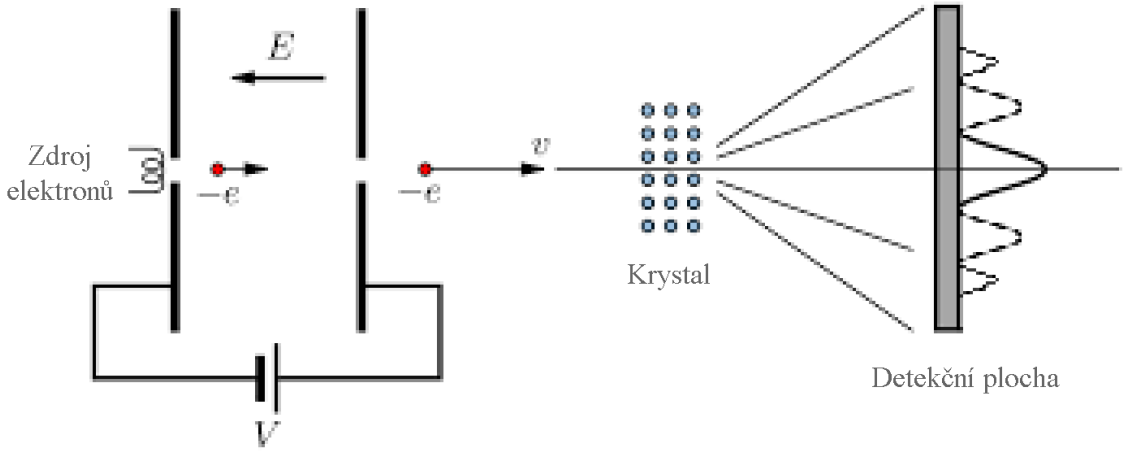
elektron se po průchodu otvorem změní ve *vlnění*, které se šíří všemi směry do prostoru za bariérou; pokud jsou použity dva otvory, pak v různých směrech dochází k interferenci vln, které jsou proti sobě posunuty.

Přesněji řečeno, elektron se za dvojí dírkou ve vlnění *nezmění*, on už před nimi vlněním *také* byl, ale tam dával popis jeho chování při klasickém pohledu, který ho vnímá jako kuličku, nerozlišitelný od popisu, který nám v této primitivní situaci dává zhruba sto roků stará vlnová teorie, ale za dvoudírkou s klasickou kuličkovou teorií nevystačíme. Elektron se tedy někdy chová ne jako kulička, ale jako vlnění.

Na Obr. vidíme analýzu maxim a minim: štěrbiny jsou dvě, vzdálené o d a ve směru udaném úhlem α je dráha vlny ze spodní štěrbiny delší o $d\cos\alpha$. Pokud je tento rozdíl rovný polovině délky vlny, spojené s elektronem, pak se maxima (resp. minima) vlny z horní štěrbiny setkávají s minimy (resp. maximy) vlny ze spodní štěrbiny a navzájem se ruší - v takovém směru pak má složená vlna malou amplitudu a následkem toho v tom směru dopadá málo elektronů. Pokud ale je délkový posun rovný délce vlny, pak se maxima potkávají s maximy a minima s minimy, vlny se vzájemně zesilují a v takovém směru pak se nachází jedno z vedlejších maxim dopadu elektronů.

Podrobněji a v duchu kvantové teorie je to tak, že *nelze* na rozdíl od naší běžné fyzikální intuice přesně určit, kde se elektron bude nacházet, ale intenzita vlny v daném místě (přesněji druhá mocnina její absolutní hodnoty) udává pravděpodobnost, že elektron, jehož chování vlna popisuje, se objeví zrovna v tom daném místě.

Teprve když elektronů v daném pokusu běží ohromná množství, pak statistické zákony velkých čísel způsobí, že počty elektronů dopadajících do různých míst na de-



Obrázek 4:

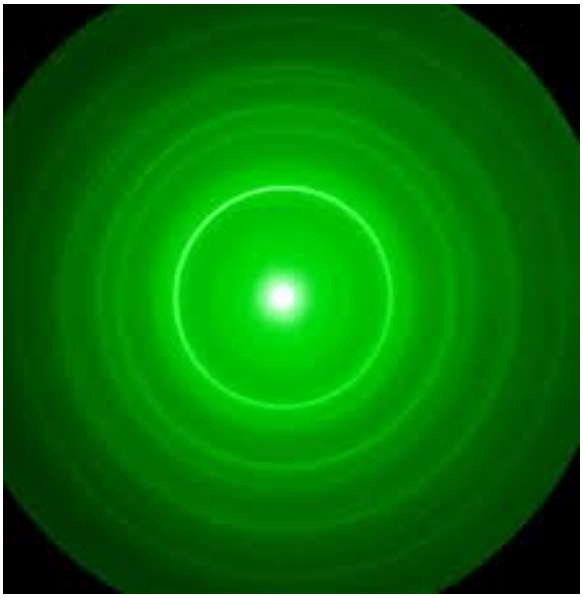
tekčním stínítku “zhmotní”.

Tento jev se běžně používá pro studium vlastností krystalů - jeden nebo dva otvory pro průchod elektronů o průměru srovnatelném s průměrem elektronu pochopitelně vyrobit neumíme, ale krystalová mřížka, Obr. , se chová jako soustava pravidelně umístěných otvorů vhodné velikosti. Vlnovou délku vlny související s elektronem už umíme vypočítat - podle rovnice, kterou objevil de Broglie, je rovna h/p, kde h je Planckova konstanta a p je relativistická hybnost elektronu, která se obvykle snadno určí z urychlujícího napětí elektronu a pak můžeme na základě výše uvedené analýzy z difrakčního obrazce, jehož typický příklad je na Obr. , určovat rozměrové konstanty krystalu.

I když Einstein byl většinu života velkým odpůrcem kvantové mechaniky, je ale přitom jedním z jejích zakladatelů. V roce 1905 publikoval kromě článku, popisujícího teorii relativity, také článek vysvětlující fotoefekt: působí-li se na některé materiály elektromagnetickým vlněním (např. světlem), z materiálu vyskakují elektrony. Zjistilo se ale, že nezávisí příliš na intenzitě vlnění - je-li jeho vlnová délka příliš dlouhá, elektrony se materiálu nevyrazí ani při extrémně velké intenzitě záření, zatímco světlo o krátké vlnové délce emituje elektrony již při velmi malých intenzitách.

Einstein foto efekt vysvětlil tím, že na elektromagnetické vlny se díval ne jako na vlnění, ale jako na kuličky, jejichž energie závisí na vlnové délce světla. Čím je vlnová délka kratší, tím mají kuličky světla (fotony) větší energii. Bez ohledu na to, kolik kuliček je, musí každá z nich mít alespoň jistou minimální energii, aby mohla z materiálu vyrazit elektron. Světlo se tedy někdy nechová jako vlnění, ale jako proud kuliček.

Dohromady z toho postupně vyplynulo, že v kvantové mechanice má vše duální po-



Obrázek 5:

dobu - částice jsou asociovány s *vlnovou funkcí*. Dosud nepanuje shoda o tom, zda vlnová funkce je něco, co reálně existuje a nebo je to jen naše matematická pomůcka, s jejíž pomocí jsme schopni dopředu vypočítat průběh různých fyzikálních jevů na kvantové úrovni. Ale bez vlnové funkce řadu fyzikálních jevů nejsme schopni vysvětlit, zatímco s ní jsou naše předpovědi podivuhodně přesné.

Je to tak, že pokud chceme popsat chování nějaké částice (foton, elektron,...), rovnice kvantové mechaniky nám v konkrétní situaci určí vlnovou funkci, která pak udává pravděpodobnost, že se částice vyskytuje v určitém místě, nebo má určitou hybnost, a pod. (Přesněji řečeno, pravděpodobnosti udává druhá mocnina absolutní hodnoty vlnové funkce). Zajímavé je, že abychom byli schopni vlnovou funkcí kvantové jevy dobře popsat, musíme připustit, že to je funkce s komplexními hodnotami; může tedy nabývat kromě kladných i záporné hodnoty, ale také hodnoty čistě imaginární, či obecné komplexní.

Vlnová funkce, popisující nějakou částici, se vypočte naprosto přesně; vlastnosti částice, které se týká, však vlnová funkce neurčuje jednoznačně - obecně se např. částice na základě výpočtu může vyskytovat v mnoha možných polohách a z vlnové funkce vyčteme jen pravděpodobnosti, kde se částice může nacházet. Že se nám pak okolní svět jeví dokonale deterministický, vyplývá až ze statistického zákona velkých čísel, neboť jevů na naši úrovni pozorování se účastní daleko více než miliardy kvantově se chovajících částic.

V kvantové mechanice neplatí to, na co jsme z běžného života zvyklí - že můžeme fyzikální objekty pozorovat, aniž bychom je tím nějak ovlivňovali. Abychom např. mohli elektron vidět, musel by k nám vyslat alespoň jeden foton - a to by bylo již velké ovlivnění situace. Stručně řečeno, jak například určíme přesně polohu částice, popsané pravděpodobnostně vlnovou funkcí, ovlivníme tím systém tak, že vlnová funkce, představující předpokládané chování systému v nepřítomnosti interakce s okolím, přestane udávat pravděpodobnosti výskytu částice pro různá místa prostoru a částice ke již lokalizována v jediném místě - tam, kde byla nalezena.

Zjednodušením výše popsaného se dostáváme k pojmu *kvantový bit* - anglický název *quantum bit* se obvykle zkracuje na *qubit*. Je to částice nebo jiný objekt, podléhající zákonitostem kvantové mechaniky, který se může vyskytovat v jednom ze dvou jasně odlišených stavů (nebo obecněji vlastnost může nabývat hodnot ze dvou jasně odlišených disjunktních *množin* stavů).

Příkladem může být elektron - u elektronu pozorujeme tak zvaný *spin*, jev, který vyvolává podobnou elektromagnetickou odezvu, jako když se elektricky nabité makroskopické těleso otáčí. U elektronu je jeho "rychlost otáčení" stálá, ale elektron se může "otáčet" ve směru nebo proti směru hodinových ručiček. Spin elektronu tedy může nabývat dvou hodnot, které se označují +1/2 a -1/2 a lze je použít jako možných hodnot kvantového bitu.

Je řada dalších konfigurací, podléhajících zákonitostem kvantové mechaniky a použitelných pro uchování jednoho bitu informace (fotony, ionty,...). Potíž je, že fotony není možné udržet na jednom místě, elektrony jsou také velmi čilé, ionty je sice například možné uvěznit v mřížce vhodného krystalu, ale v poslední době se zdá, že se k reprezentaci qubitu bude výhodné používat smyček vodiče ze supravodivého materiálu mikroskopických velikostí.

Při teplotě, při které je materiál smyčky supravodivý (obvykle jen několik stupňů Kelvina), takovou smyčkou může obíhat elektrický proud, aniž bychom jej museli nějak popohánět a aniž by se jeho velikost s časem zmenšovala, jako tomu je v případě smyčky z vodiče, který má ohmický odpor. A do smyčky může být elektrický proud naindukován tak, aby obíhal ve směru nebo proti směru hodinových ručiček, což opět dává možnost zakódovat jeden bit informace. Výhodou je, že takové smyčky mohou být výhodně fixovány na pevný substrát a proto se s nimi dobře pracuje.

Po abstrakci od konkrétní fyzikální implementace jsou hodnoty qubitu z historických důvodů obvykle zapisovány jako $|0\rangle$ a $|1\rangle$.

Jak již bylo naznačeno, kvantový systém je obecně popsán vlnovou funkcí (nebo funkcemi), ze kterých teprve odvozujeme pravděpodobnosti, s jakou nastávají konkrétní situace (například lokalizace uvažované částice v jistém místě).

Qubit (kvantový bit) proto pro nás bude výraz

$$\alpha|0\rangle + \beta|1\rangle, \qquad \text{kde } \alpha \text{ a } \beta \text{ jsou komplexní čísla taková, že} \qquad |\alpha|^2 + |\beta|^2 = 1$$

a $|\alpha|^2$ a $|\beta|^2$ budou pravděpodobnosti, že popisovaný qubit má hodnotu $|0\rangle$, respektive $|1\rangle$.

S kvantovým bitem bude možno provádět *kvantové operace*, které budou spočívat v jistým způsobem prováděných změnách hodnot α a β. Po celou dobu práce s kvantovým bitem ale nebudeme mít žádnou informaci o jeho skutečné hodnotě.

Až na konci výpočtu (nebo přesněji na konci používání daného kvantového bitu, což může být i daleko před koncem celého výpočtu) jeho hodnotu *změříme*. Jak bylo uvedeno, hodnoty $|\alpha|^2$ a $|\beta|^2$ v okamžiku měření qubitu dávají výše uvedeným způsobem *pravděpodobnosti*, že tento kvantový bit po změření dá hodnotu $|0\rangle$ nebo $|1\rangle$. Změřením qubitu pozbudou hodnoty α a β svého významu, s qubitem už nebude možné pracovat tak, jako tomu bylo před změřením.

Tak například qubity

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - i\frac{1}{\sqrt{2}}|1\rangle$$

jsou všechny ekvivalentní v tom smyslu, že po jejich změření lze se stejnou pravděpodobností (rovnou 1/2) očekávat i hodnotu $|0\rangle$ i hodnotu $|1\rangle$.

To ale neznamená, že by tyto qubity byly ekvivalentní. Pokud bychom na ně aplikovali nějakou kvantovou operaci (například otočení o malý úhel, viz dále) a teprve potom je změřili, pravděpodobnosti hodnot $|0\rangle$ už pro ně budou odlišné $|1\rangle$, a to obecně pro každý z nich jinak. Z tohoto důvodu potřebujeme mít kvantový bit popsán tak, jak to bylo uvedeno výše, abychom byli schopni popsat chování skutečných kvantových objektů.

Jiným často používaným qubitem je výraz

$$\sin\theta|[\rangle 0] + \cos\theta|1\rangle,$$

který splňuje qubitou podmínku, protože je známo, že $\sin^{\theta} + \cos^2\theta = 1$. U něj už pravěpodobnosti hodnot $|0\rangle$ a $|1\rangle$ jsou obecně různé a závisejí na hodnotě θ.

Jen ještě jedna formální dohoda - uvádění hodnot α a β v takovém tvaru, aby platilo $|\alpha|^2 + |\beta|^2 = 1$ je někdy velmi únavné - viz vzorce uvedené výše jako příklady qubitů, které jsou "zamořeny" odmocninou z 1/2. Proto budeme v dalším psát qubity často ve tvaru $\alpha|0\rangle + \beta|1\rangle$, kde α a β *nesplňují* podmínku $|\alpha|^2 + |\beta|^2 = 1$ s tím, že budeme vědět, že zápis (tedy α a β) je nutno ještě vydělit číslem $\sqrt{|\alpha|^2 + |\beta|^2}$, abychom dostali korektně zapsaný qubit.

Například výše uvedené příklady qubitů tedy budeme psát prostě jako

$$|0\rangle + |1\rangle, |0\rangle - |1\rangle, |0\rangle + i|1\rangle, |0\rangle - i|1\rangle.$$

Kvantové operace s qubitem

Zatím jsme mluvili jen o jednom qubitu a proto se omezíme na operace s jedním qubitem; pro účely tohoto textu to bude dostatečné. Kvantovou operaci budeme definovat tak, že popíšeme, kam se zobrazí hodnoty $|0\rangle$ a $|1\rangle$, a pak toto zobrazení lineárně doplníme pro libovolný stav qubitu.

Pro popis kvantové operace Φ tedy potřebujeme čtyři čísla $A_{i,j}$, kde $i, j = 0, 1$ taková, že $|A_{i,0}|^2 + |A_{i,1}|^2 = 1$ pro $0, 1$ a definujme

$$\Phi(|0\rangle) = A_{0,0}|0\rangle + A_{0,1}|1\rangle,$$

$$\Phi(|1\rangle) = A_{1,0}|0\rangle + A_{1,1}|1\rangle.$$

Pro jednoduchost budeme opět používat při zápisu čísla $A_{i,j}$, která nesplňující výše uvedené podmínky, mlčky předpokládajíce, že si je čtenář vydělí odpovídajícími hodnotami $\sqrt{|A_{i,0}|^2 + |A_{i,1}|^2}$

Lineárním rozšířením míníme, že

$$\Phi(\alpha|0\rangle+\beta|1\rangle) = \alpha(A_{0,0}|0\rangle+A_{0,1}|1\rangle)+\beta(A_{1,0}|0\rangle+A_{1,1}|1\rangle) = (\alpha A_{0,0}+\beta A_{1,0})|0\rangle+(\alpha A_{0,1}+\beta A_{1,1})|1\rangle.$$

V dalším budeme potřebovat jen dvě z většího množství kvantových operací:

Otočení Pro jistou komplexní hodnotu θ položme

$$\Phi(|0\rangle) = \cos(\theta)|0\rangle - \sin(\theta)|1\rangle,$$

$$\Phi(|1\rangle) = \sin(\theta)|0\rangle + \cos(\theta)|1\rangle.$$

Je zřejmé, že operace je v normovaném tvaru, její název se odkazuje do geometrie roviny, kde podobný vzorec popisuje transformaci souřadnic bodů roviny při jejím otočení o úhel θ se středem otáčení v počátku souřadnic.

Hadamardova transformace

$$\Phi(|0\rangle) = |0\rangle + |1\rangle,$$

$$\Phi(|1\rangle) = |0\rangle - |1\rangle.$$

Jedná se o velmi jednoduchou, ale také velmi užitečnou transformaci (je potřeba její koeficienty zanormovat na $\pm 1/\sqrt{2}$).

Entanglement

Anglický výraz entanglement se do češtiny se překládá nejčastěji jako provázanost. Znamená, že dva kvantové bity mají své stavy jistým způsobem koordinované. Matematicky to pro případ dvou provázaných qubitů popíšeme tak, že jejich společný stav je popsán jako

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

kde α, β, γ a δ jsou čtyři komplexní čísla taková, že $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Výraz $|ij\rangle$ znamená, že první bit má hodnotu i a druhý hodnotu j, je to tedy zkratka za $|i\rangle|j\rangle$. Nemusí ale platit žádné další podmínky.

Jeden z extrémních případů, který je mimořádně zajímavý a přitom jednoduchý a v kvantovém počítání hojně používaný, je stav

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Tento stav znamená, že změříme-li hodnotu jednoho z bitů, můžeme dostaneme se stejnými pravděpodobnostmi $|0\rangle$ i $|1\rangle$, ale pokud pak změříme hodnotu druhého bitu, provázanost zajistí, že naměříme ***vždy stejnou*** hodnotu jako u prvého bitu.

Obecně u stavu dvojice provázaných qubitů jestliže naměříme u prvního (levého) qubitu hodnotu $|0\rangle$, pak druhý qubit se bude chovat, jako by měl stav $\alpha|0\rangle + \beta|1\rangle$ (nutno zanormovat) a jestliže naměříme u prvního qubitu hodnotu $|1\rangle$, pak druhý qubit se bude chovat, jako by měl stav $\gamma|0\rangle + \delta|1\rangle$ (také nutno zanormovat), obdobně pokud byl nejdříve změřen druhý qubit.

Pozoruhodné je, že dosáhneme-li u dvou qubitů provázanosti, můžeme je od sebe dosti daleko vzdálit a jejich provázanost trvá a její trvání se zdá být časově neomezené, nedojde-li k závažnému ovlivnění dvojice z vnějšku. Kvantovou provázanost se již podařilo prokázat i na vzdálenost přes 1000 km a nezdá se, že by podobná vzdálenost byla nějakým principiálním způsobem omezena.

Provázanost qubitů je naprosto základní prvek, na kterém jsou založeny všechny netriviální kvantové algoritmy. Mechanismy, který ke vzniku provázanosti vedou, nejsou dosud dobře známy, takže podle mne nejsou všechny postupy a přístupy, používané v teorii kvantových algoritmů, dosud zcela experimentálně ověřeny.

Albert Einstein měl vůči kvantové mechanice velké výhrady a možnost provázanosti považoval za absurdní, protože kdyby se dvě provázané částice dostatečně vzdálily a pak současně změřily (nebo změřily s odstupem kratším, než doba, kterou by světlo potřebovalo na překonání vzdálenosti mezi částicemi), znamenalo by to, že koordinace mezi změřenými hodnotami částic by proběhla větší rychlostí, než je rychlost světla, což

pro Einsteina byla největší rychlost, kterou se ve vesmíru může pohybovat *cokoli*, tedy i informace o hodnotě, kterou poskytlo změření jedné z částic.

Proto Albert Einstein a jeho kolegové z Princetonu, Boris Podolsky a Nathan Rosen, navrhli experiment, nazývaný podle jejich jmen EPR experiment, který měl možnost provázání popřít. Experiment je založen na následující hře:

Dvě osoby, pojmenované způsobem v teoretické informatice obvyklým jako Alice a Bob, hrají proti Věře (verifikátor). Věra vygeneruje náhodné bity x a y, pošle x Alici a y Bobovi. Alice pošle Věře bit a, Bob pošle Věře bit b. Alice s Bobem vyhráli, jestliže $a \oplus b = x \wedge y$ (to znamená, že pokud $x = y = 1$, pak Alice a Bob musí poslat různé bity, ve zbývajících 3 případech musí poslat bity stejné).

Pokud se Alice s Bobem mohou domluvit, pak je pro ně snadné vždy vyhrát. Například Alice vždy bude posílat 0 a Bob hodnotu $x \wedge y$ (k čemuž musí vědět, jaký bit poslala Věra Alici).

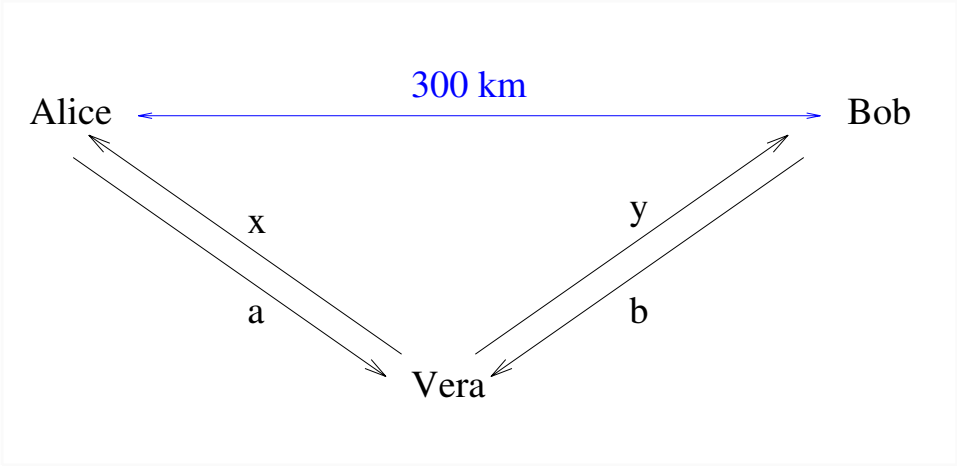
Pokud se Alice a Bobem nedomlouvají a pokud Věra generuje bity x a y opravdu náhodně, pak Alice s Bobem mohou vyhrávat s pravděpodobností 3/4, třeba tak, že oba budou vždy posílat bit 0 (a tedy prohrají jen když $x = y = 1$, což se stane s pravděpodobností 1/4.

Snadno se ale dokáže, že pokud se Alice s Bobem nemohou domluvit, pak s větší pravděpodobností než 3/4 vyhrávat *nemohou*. Alice má totiž jen 4 možné deterministické strategie: vždy posílat 0 nebo 1, vracet vždy x nebo vždy vracet negaci x, obdobně pro Boba. Přímočarým probráním všech 16 možností strategie Alice a Boba se ukáže, že vždy v alespoň jedné ze 4 možností pro x a y Alice s Bobem prohrají. Pokud budou pro každou hru Alice i Bob svou strategii vybírat náhodně, nepomůže jim to, protože pro každé kolo hry vyberou náhodně jednu z 16 možných dvojic deterministických strategií.

EPR experiment je pak možno provést například takto, viz Obr. : Postavte Alici a Boba 300 km od sebe, Věru mezi ně. Své zprávy si zasílají světelným signálem a Věra požaduje odpovědi do 1,5 milisekundy poté, co odeslala x a y. Jelikož za 1 ms světlo urazí asi 300 km, mají Alice a Bob ještě 0,5 ms k dobru na vypracování své odpovědi (takže ji nebudou provádět sami, ale svěří to elektronice, pro kterou je to docela dlouhá doba), ale nemají čas na to, aby přijali signál od Věry, poslali jeden druhému info a pak poslali odpověď Věře. A Einstein s kolegy vyzvali: tak si zkuste v této situaci využít provázanosti částic k tomu, aby Alice s Bobem vyhrávali s pravděpodobností větší než 3/4 (t.zn. aby využili provázanost k nějaké formě koordinace svých postupů).

A několik let poté, co Einstein zemřel se to opravdu povedlo. Ukážeme nyní, jak se to dá provést. Alice s Bobem si připraví pro každou hru dvojici provázaných qubitů ve stavu

$$|00\rangle + |11\rangle$$



Obrázek 6:

(nutno zanormovat). Provází je třeba někde poblíž Věry a pak si je odvezou do svých herních pozic a čekají na bity od Věry. Pak hrají takto

- jestliže Alice dostane od Věry bit 1, provede na svůj qubit operaci otočení o 22,5 stupňů, neboli o $\pi/8$ (viz výše), dostane-li 0 nechá svůj qubit beze změny.
- jestliže Bob dostane od Věry bit 1, provede na svůj qubit operaci otočení o -22,5 stupňů, neboli o $-\pi/8$ (viz výše) - tedy o stejný úhel, ale v opačném směru než Alice, dostane-li 0 nechá svůj qubit beze změny.
- pak oba své bity *změří* a výsledek měření odešlou Věře.

Myšlenka tohoto postupu je následující:

- pokud dostanou Alice i Bob bit 0, nechají své provázané částice v původním stavu, takže změřením dostanou stejné hodnoty - tak jak je potřeba;
- pokud dostanou Alice a Bob různé bity, jeden z nich stav svého qubitu změní, druhý ne. To vede k tomu, že občas odpoví různě - tedy špatně - ale nebude se to stávat často;
- pokud pokud dostanou Alice i Bob bit 1, otočí stavy svých qubitů opačnými směry a daleko častěji se bude stávat, že změřením dostanou různé hodnoty - tedy tak, jak je to v této situaci potřeba.

Volba úhlu je zdůvodněna takto (viz následující výpočet): pošle-li Věra $x = y = 1$, bude rozdíl natočení qubitů Alice a Boba 45 stupňů a s výhodou užijeme toho, že pro tento úhel mají sinus a kosinus stejné hodnoty.

Takže nyní propočítáme, že provedené operace opravdu vedou k vítězství s větší pravděpodobností, než jsou 3/4:

Případ $x = y = 0$ je zřejmý, Alice i Bob zaručeně odešlou stejný bit, jsa koordinování nezměněným párem qubitů $|00\rangle + |11\rangle$.

Pokud Alice dostane 0 a Bob 1, pak jejich provázané qubity přejdou (viz definice operace otočení qubitu, uvedená výše) do stavu

$$\cos(\pi/8)|00\rangle - \sin(\pi/8)|01\rangle + \sin(\pi/8)|10\rangle + \cos(\pi/8)|11\rangle.$$

Jestliže Alice změří na svém qubitu hodnotu 0, stav dvojice qubitů zdegeneruje na $\cos(\pi/8)|00\rangle - \sin(\pi/8)|01\rangle$, tedy pravděpodobnost, že Bob naměří stejnou hodnotu jako Alice je $\cos^2(\pi/8)$. Podobně je tomu i když Alice naměří 1, protože pak stav dvojice degeneruje na $\sin(\pi/8)|10\rangle + \cos(\pi/8)|11\rangle$. Stejně tak i pokud dostane Alice 1 a Bob 0, dokáže se obdobně, že pravděpodobnost, že oba odešlou stejnou hodnotu je zase $\cos^2(\pi/8)$.

Nakonec pokud Alice i Bob dostanou 1, bude po provedených rotacích opačnými směry stav dvojice qubitů

$$[\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle][\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle] +$$

$$+[\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle][-\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle] =$$

$$= (\cos^2(\pi/8)|00\rangle + \cos(\pi/8)\sin(\pi/8)|01\rangle - \sin(\pi/8)\cos(\pi/8)|10\rangle - \sin^2(\pi/8)|11\rangle +$$

$$+(-\sin^2(\pi/8)|00\rangle + \sin(\pi/8)\cos(\pi/8)|01\rangle - \cos(\pi/8)\sin(\pi/8)|10\rangle + \cos^2(\pi/8)|11\rangle) =$$

$$= (\cos^2(\pi/8) - \sin^2(\pi/8))|00\rangle + 2\cos(\pi/8)\sin(\pi/8)|01\rangle -$$

$$-2\sin(\pi/8)\cos(\pi/8)|10\rangle + (\cos^2(\pi/8) - \sin^2(\pi/8))|00\rangle =$$

$$= \cos(\pi/4)|00\rangle + \sin(\pi/4)|01\rangle - \sin(\pi/4)|10\rangle + \cos(\pi/4)|11\rangle,$$

protože je známo, že $\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha)$ a $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$.

Protože ale sinus i kosinus úhlu 45 stupňů, neboli $\pi/4$, jsou stejné, dostáváme, že všechny koeficienty stavu mají stejnou absolutní hodnotu, takže pravděpodobnosti všech čtyř možností jsou stejné a proto budou Alice a Bob odpovídat různě (tedy vyhrávajícím způsobem) s pravděpodobností 1/2, a stejně (tedy prohrávajícím způsobem), také s pravděpodobností 1/2).

Jelikož každá kombinace bitů x a y nastává s pravděpodobností 1/4, pak protože $\cos^2(\pi/8) \geq 0,85$, bude celková pravděpodobnost výhry Alice a Boba nad Věrou rovna

$$\frac{1}{4} + \frac{1}{2}\cos^2(\pi/8) + \frac{1}{4}\frac{1}{2} \geq 0,25 + 0,425 + 0,125 = 0,8,$$

tedy větší než 3/4=0,75.

Kvantový registr

Výrazem kvantový registr rozumíme libovolné množství navzájem provázaných qubitů. Pokud je jich n, potřebujeme k popisu jejich stavů celkově 2^n čísel $A_{b_1 b_2 \ldots b_n}$, kde $b_1, \ldots, b_n = 0, 1$. Stav je pak popsán jako

$$\sum_{b_1 \ldots b_n = 0,1} A_{b_1 b_2 \ldots b_n} |b_1 \ldots b_n\rangle.$$

Představme si například *uniformní* stav kvantového registru s n bity, což je stav, kdy všechny koeficienty $A_{b_1 b_2 \ldots b_n}$ jsou stejné (a tedy musí být rovné $2^{-n/2}$ aby součet jejich druhých mocnin dal 1). Před *změřením* hodnot qubitů v registru tedy stav registru v sobě zahrnuje *všechny* potenciální konečné hodnoty $|b_1 \ldots b_n\rangle$, kterých je ohromné množství (konkrétně 2^n).

Uniformní stav kvantového registru je často používaný výchozí stav pro kvantový algoritmus. Je ho možné dostat snadno z ještě jednoduššího *nulového* stavu $|00 \ldots 0\rangle$ (to je ten, ve kterém bychoms určitostí - tedy s pravděpodobností 1 - naměřili pro každý qubit registru hodnotu $|0\rangle$) tak, že na každý qubit registru aplikujeme nezávisle Hadamardovu transformaci, protože ta hodnotu $|0\rangle$ převádí (viz výše) do $|0\rangle + |1\rangle$, tedy do uniformního stavu.

Faktorizace

Jak již bylo uvedeno, hlavní důvod, proč je kvantovému počítání věnována taková pozornost a tolik finančních prostředků, je Shorův algoritmus z roku 1994, pomocí kterého by kvantový počítač rozumné velikosti uměl provést faktorizaci i obrovských čísel ve velmi krátké době, což by to znamenalo totální prolomení RSA šifry. Dodejme k tomu jen, že dnes, po 27 letech od Shorova objevu, máme stále k dispozici jen kvantové počítače velmi "nerozumné" velikosti, kterými by se podařilo možná faktorizovat jen čísla, jejichž klasická faktorizace není problém. Přesto je ale Shorův výsledek stále hlavním hnacím motorem kvantového počítání.

Shorův algoritmus ve skutečnosti nehledá faktory čísle $n = pq$, ale řeší jiný problém, který s faktorizací složeného čísla má na první pohled jen málo co společného:

Nechť jsou dána celá kladná čísla n a a, kde $a < n$. Uvažujme celočíselnou funkci $\phi(x) \equiv a^x \ mod \ n$. Řád čísla a vzhledem k n je nejmenší celé kladné číslo r takové, že $a^r \equiv 1 \ mod \ n$.

Uvážíme-li, že $\phi(0) \equiv a^0 = 1$, znamená to, že řád je *periodou* funkce ϕ, protože se snadno ukáže, že pro každé x je, počítáno modulo n,

$$\phi(x + r) \equiv a^{x+r} = a^x a^r \equiv a^x \cdot 1 = a^x \equiv \phi(x)$$

a ukáže se také snadno, že

$$\phi(x) = \phi(y) \quad \text{právě tehdy, když } x - y \text{ je násobkem periody } r \qquad (P)$$

Jak se ale znalost určování řádu/periody dá využít k faktorizaci složeného čísla? Je zřejmé, že k nalezení všech prvočinitelů složeného čísla n stačí umět nalézt netriviálního (ale ne nutně prvočíselného) dělitele d (netriviální znamená $1 < d < n$) nebo zjistit, že neexistuje, protože pak opakujeme stejný postup hledání netriviálních dělitelů na d a n/d tak dlouho, až dostaneme samotná prvočísla.

K nalezení dělitele stačí nalézt nějaké celé číslo $m < n$ takové, že $\gcd(m, n) > 1$ (kde používám anglickou zkratku "gcd" - greatest common divisor - pro označení největšího společného dělitele): známe-li n i m, pak určit $\gcd(m, n)$ (třeba Euklidovým algoritmem) je snadné a tento $\gcd(m, n)$ je náš hledaný netriviální dělitel d.

Než se pustíme do dalšího výkladu, připomenu, že malá Fermatova věta říká, že je-li p prvočíslo, pak $a^{p-1} \equiv 1 \ mod \ n$ pro každé celé číslo a, $1 < a < p$. A v dodatku o testování prvočíselnosti je dokázáno, že pokud pro nějaké celé číslo s platí, že $s^2 \equiv 1 \ mod \ p$, pak prvočíselnost p implikuje, že s musí být rovno 1 nebo -1 modulo p.

Nyní uvedu dvě lemmata, která ukazují, jak algoritmus pro výpočet řádu/periody využít k faktorizaci. Budu přitom předpokládat, že n je součinem dvou neznámých prvočísel p a q (tak jak je to u RSA šifrování); důkaz pro obecné složené n je velmi podobný, ale nepřehlednější a tak si ho odpustím.

Lemma 1 *Jestliže $s^2 \equiv 1 \ mod \ n$, ale s není ani +1 ani -1 modulo n, pak platí, že $gcd(s - 1, n) > 1$.*

Proof Rovnost $s^2 \equiv 1 \ mod \ n$ znamená, že $s^2 - 1 = (s + 1)(s - 1) \equiv 0 \ mod \ n$, neboli $(s + 1)(s - 1)$ je dělitelné číslem n. Pokud ale s není ani +1 ani -1 modulo n, znamená to, že ani $(s - 1)$ ani $(s + 1)$ nejsou 0 modulo n, tedy ani jedno z nich není číslem n dělitelné. To je možné jen tak, že jeden z prvočinitelů p a q čísla n dělí $(s - 1)$ (ale ne

$(s+1)$) a druhý dělí $(s+1)$ (ale ne $(s-1)$). Pak ale $gcd(s-1,n)$ vychází roven tomu prvočiniteli, který dělí $(s-1)$. ♣

A nyní lemma podstatně složitější, jeho důkaz je uveden pro úplnost v dodatku, ale zde bude jen naznačena hlavní myšlenka důkazu:

Lemma 2 *Nechť n je složené číslo a uvažujme množinu $M = \{x \in \{2,3,\ldots,n-1\} | gcd(x,n) = 1\}$. Pak alespoň jedna čtvrtina prvků x množiny M je takových, že řád r čísla x vzhledem k n je sudý a $x^{r/2} \not\equiv +1 \ mod\ n$ a $x^{r/2} \not\equiv -1 \ mod\ n$.*

Proof Počítáme-li modulo $n = pq$, pak je vhodné místo každého čísla a v rozmezí $0 <= a < n$ uvažovat dvojici $a \ mod\ p, a \ mod\ q$, protože tento vztah je vzájemně jednoznačný. Je-li r řád čísla a a je sudý, pak $a^{r/2}$ je +1 nebo -1 modulo p a ukáže se, že jsou ty možnosti stejně pravděpodobné, podobně i modulo q. Jestliže ale jedno z čísel $a^{r/2} \ mod\ p$ a $a^{r/2} \ mod\ q$ je +1 a druhé je -1, pak $a^{r/2} \ mod\ n$ není ani +1 ani -1. A také se ukáže, že řád čísla a je sudý asi v polovině případů. ♣

Použití obou lemmat pro faktorizaci daného složeného čísla n je snadné. Náhodně volme celá čísla x v rozmezí $1 < x < n$. Pokud trefíme x takové, že $gcd(x,n) > 1$, máme vyhráno, tento největší společný dělitel je netriviálním dělitelem čísla n, viz lemma uvedené výše. V opačném případě je $x \in M$ a druhé lemma říká, že s pravděpodobností alespoň 1/4 platí, že řád r čísla x vzhledem k n je sudý a číslo $s = x^{r/2}$ není ani +1 ani -1 modulo n. Pokud řád r umíme vypočíst, pak první lemma nám dá netriviálního dělitele čísla n.

Simonův algoritmus

Jak bylo ukázáno v předchozí kapitole, pro faktorizaci složených čísel (a tím i pro rozlomení RSA šifrovacího systému) by bylo dostatečné umět efektivně řešit následující problém:

Je dána funkce ϕ, jejíž hodnoty je snadné počítat a platí pro ni, že existuje r (perioda funkce ϕ) takové, že $\phi(x) = \phi(y)$ právě tehdy, když r dělí rozdíl $x - y$. Nalezněte r.

Pro funkci $\phi(x) = a^x \ mod\ n$ se problém dá účinně řešit na hypotetickém kvantovém počítači Shorovým algoritmem.

Shorův algoritmus je ale dost složitý - využívá netriviálním způsobem diskrétní Fourierovu transformaci implementovanou na kvantovém počítači (patrně víte, že Fourierovo spektrum funkce závisí na její periodě, což je myšlenka, na které je Shorův algoritmus založen). Proto místo něj popíšeme daleko jednodušší Simonův algoritmus, který řeší problém, který se dá formulovat velmi podobně jako problém hledání periody funkce.

Podobnost není jen formální, základní koncepce Simonova a Shorova algoritmu jsou podobné, takže znalost Simonova algoritmu Vám umožní učinit si představu o i tom, jak asi pracuje Shorův algoritmus, nejznámější výpočetní způsob v teoretickém kvantovém počítání.

Problém, který je řešen Simonovým algoritmem je následující:

Problém: Je dáno celé kladné číslo n a funkce $\psi : \{0,1\}^n \to \{0,1\}^n$, jejíž hodnoty je snadné počítat a platí pro ni, že existuje n-tice bitů a taková, že

$$\psi(x) = \psi(y) \quad \text{právě tehdy, když } x = y \text{ nebo } x \oplus y = a.$$

Nalezněte n-tici a.

Podrobněji rozepsáno podmínka říká, že existují bity $a_1, a_2, \ldots, a_n$ takové, že

$$\psi(x_1, x_2, \ldots, x_n) = \psi(y_1, y_2, \ldots, y_n)$$

platí právě když posloupnosti $(x_1, x_2, \ldots, x_n)$ a $(y_1, y_2, \ldots, y_n)$ jsou si rovny nebo

$$x_i \oplus y_i = a_i \text{ pro všechny } i = 1, 2, \ldots, n.$$

Předpoklad, že "hodnoty ψ je snadné počítat" je dosti mlhavý, ale je možné ho blíže precizovat tak, že se jedná o funkci, kterou lze určit pomocí krátké posloupnosti základních aritmetických operací, jako je sčítání a násobení a logických operací, jako je negace, konjunkce nebo disjunkce (Shorova funkce $\phi(x) = a^x \ mod \ n$ tento předpoklad očividně splňuje).

Základní koncepce Simonova algoritmu je následující: vytvoříme kvantový registr, který bude mít $2k$ qubitů $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n$ (plus pomocné qubity pro výpočet funkce ψ), které budou na počátku provázány tak, že
qubity $u_1, u_2, \ldots, u_n$ jsou v uniformním stavu (například transformovány z nulového stavu Hadamardovou transformací, viz výše), a
pro $i = 1, 2, \ldots, n$ jsou qubity u_i a v_i provázány tak, že jsou si rovny.

Přesněji řečeno, kvantový registr je ve stavu

$$\frac{1}{2^{n/2}} \sum_{b_1 \ldots b_n = 0,1} |b_1 b_2 \ldots b_n b_1 b_2 \ldots b_n\rangle.$$

Kvantový registr je tedy inicializován tak, že prvních n qubitů je v uniformním stavu a dalších n qubitů jsou vlastně jejich kopie.

Základní dva kroky Simonova algoritmu jsou následující:

1. Na qubity $v_1, v_2, \ldots, v_n$ aplikujeme funkci ψ. Podrobněji řečeno přejdeme do stavu

$$|x_1, \ldots, x_n s_1, \ldots, s_n\rangle,$$

kde $(s_1, \ldots, s_n) = \psi(\ (x_1, \ldots, x_n)\ )$.

2. Změříme n pravých qubitů kvantového registru (tedy ty, na které byla aplikována funkce ψ).

Kdybychom změřili pravou polovinu qubitů hned na začátku, zdegenerovala by levá polovina na superpozici těch jejích stavů, které jsou v souladu s pravou polovinou - tedy na jediný stav, rovný tomu, co bylo naměřeno napravo.

Po provedení kroku 1 to ale bude tak, že levá polovina qubitů zdegeneruje na uniformní superpozici těch stavů, které jsou v souladu s tím, co bylo naměřeno napravo. To znamená, že pokud jsme napravo naměřili $|w_1, \ldots, w_n\rangle$, pak levá polovina degeneruje na uniformní superpozici těch jediných **dvou** stavů $|u_1, \ldots, u_n\rangle$ pro které platí

$$\psi(u_1, u_2, \ldots, u_n) = (w_1, w_2, \ldots, w_n).$$

No a vlastnost funkce ψ říká, že ty dva stavy, které splňují právě uvedenou podmínku, jsou takové, že jeden z nich se dostane z druhého symetrickou diferencí (exklusivním **or**) s posloupností $a_1, a_2, \ldots, a_n$.

Nepozorný čtenář může zajásat: z ohromného počtu stavů, které by se po provedení kroků 1. a 2. mohly s nenulovou pravděpodobností objevit (je jich 2^n z celkového počtu 2^{2n} možných stavů registru s $2n$ qubity) jsme změřením pravé poloviny qubitů dostali *dva* možné stavy levé poloviny a pokud je oba získáme, jejich symetrickou diferencí dostaneme hledaný vektor a. AA ten nepozorný čtenář si může myslet, že oba je získat jistě nebude složité: změřením levé poloviny qubitů dostaneme s pravděpodobností 1/2 jeden nebo druhý stav. Stačí to měření zopakovat několikrát, aby "vyskočil" i ten druhý a máme vyhráno.

Tak si to ale na neštěstí může představovat jen nepozorný čtenář, ale ve skutečnosti to tak dělat nejde - levou polovinu qubitů můžeme změřit jen *jednou*, pak se všechno kouzlo kvantového počítání ztratí a ten druhý stav se již nedozvíme. A opakováním celého postupu včetně opětovného měření pravé poloviny qubitů dostaneme náhodný prvek z *jiné* dvojice stavů, který s tím předchozím není v žádném vztahu.

Přesto i ten nepozorný čtenář si povšiml toho hlavního, co se v Simonově algoritmu děje: po jistých úpravách jsme změřením pravé půlky qubitů zredukovali exponenciálně velké množství stavů, které v sobě obsahují jistým způsobem všechna možná řešení, na dva, které stále to řešení umožní získat.

Musíme ale postupovat opatrněji. Popsat tento opatrný postup detailně dá více námahy, než vysvětlit výše uvedené kroky 1 a 2. Je to ale záležitost povýtce technická, která nepřinese hlubší porozumění toho, proč by kvantové algoritmy měly za jistých

okolností daleko překonávat výpočty klasické, takže jen naznačím, jak se postupuje dál a detailní důkaz toho, že postup funguje, přináším v dodatku pro zvídavé a odhodlané čtenáře:

Po provedení kroků 1. a 2. aplikujeme na každý (dosud panenský) qubit levé části Hadamardovu transformaci.

Dá se dokázat, že pak po změření takto transformované levé poloviny qubitů dostaneme náhodný vektor, který je *kolmý* na hledaný vektor a.

Nyní tedy stačí celý postup (kroky 1. a 2. i Hadamardův krok) opakovat tak dlouho, až dostaneme $n-1$ lineárně nezávislých vektorů kolmých na a, které vytvářejí bázi vektorového podprostoru vektorů kolmých na vektor a. Nyní již aplikace známých metod lineární algebry umožní nalézt hledaný vektor a jako řešení soustavy $n-1$ lineárních rovnic o n neznámých.

Musím uvést, že zde uvažuji n-dimenziální vektorový prostor ne nad tělesem reálých nebo komplexních čísel, ale ***nad tělesem $\mathbf{Z}_2$ celých čísel modulo 2***, které má jen dva prvky 0,1, násobení je klasické a operace sčítání $\oplus$ je definovaná $0 \oplus 0 = 1 \oplus 1 = 0$ a $0 \oplus 1 = 1 \oplus 0 = 1$.

Kritika Simonova algoritmu a kvantového počítání obecně

Zatímco předchozí úvahy jsou převzaty z moudrých knih (konkrétně z knihy Sanjeev Arora a Boaz Barak: Computational Complexity: A Modern Approach, jejíž draft je stále k dispozici na webu Princeton Univ. a najdete je také třeba ve Wikipedii), tato kapitola vyjadřuje výhradně můj osobní, celkem kritický pohled na možnosti praktické realizace kvantových algoritmů, jako jsou algoritmy Simonův a Shorův.

Většina kritiky kvantové teorie a projektů kvantových počítačů se týká technických otázek. Bylo zde uvedeno, že změření hodnot qubitů v registru kvantového počítače znamená konec výpočtu, protože změření je možné jen v souvislosti s ovlivněním stavu počítače natolik, že už nadále si nemůžeme myslet, že počítá podle našeho algoritmu. K nechtěnému "změření" přitom může dojít působením vnějších vlivů (kosmické záření, interakce se součástmi počítače, které nejsou "výpočetní jednotkou" a pod.). Z tohoto důvodu velice záhy dochází k "dekoherenci" a výpočet přestane být korektní, takže doba pro provedení výpočtu je obvykle velmi krátká a jen obtížně se ji daří prodlužovat.

Kvantové počítače jsou svou povahou analogové a pravděpodobnostní a řada výtek míří právě k tomu.

Dle mého názoru ale nejzávažnější pochybnost o možnosti praktické realizace algoritmů, jako je Simonův, se skrývá hned v úvodu popisu algoritmu: uvedeme $2n$ qubitů do stavu, že k-tý v levé polovině je provázán ve stylu $|00\rangle + |11\rangle$ s k-tým v pravé po-

lovině a ***s žádným jiným***. Koeficienty u jednotlivých stavů registru, jejichž superpozicí celkový uniformní stav je, jsou extrémně malé, například pro $n = 100$ by byly řádově 0,00000000000000000000000001. Lze si představit, že šum, způsobený okolím, by v případě fyzicky existujícího kvantového počítače byl při nastavování uniformního stavu Hadamardovými transformacemi řádově výrazně větší a tedy bychom vůbec nebyli schopni uniformního stavu dosáhnout.

A nemožnost dosáhnout uniformního stavu nebo stavu hodně blízkého může mít i ještě hlubší příčinu. Mechanismus, umožňující provázání stavů, není znám; zatím byly zkoumány většinou soubory malých počtů částic (často jen 2), pokud byly pozorovány velké soubory, pak jen *existence* jejich provázání, aniž by byly zkoumány jemnosti koeficientů α pro jednotlivé stavy.

Dovedu si představit, že v *kvantové* mechanice, kde skoro vše je kvantováno, budou i koeficienty $\alpha_{i_1 \ldots i_n}$ nabývat jen hodnoty z diskrétní škály dané kvanty, která bude odpovídat hypotetickým částicím (mohlo by se jim třeba říkat entangleony) zodpovědným za realizaci provázání. Při takové představě by ovšem možnost přesného provázání velkého počtu částic byla omezena - možnost získat stav, který je uniformní superpozicí neomezeně velkého souboru základních stavů, by byla vyloučena - a přitom je to předpoklad, bez kterého teoretické kvantové algoritmy nejsou myslitelné (a nebo by jejich výkonnost byla zásadně omezena). Naše současné znalosti mechanismu provázání neumožňují říci o tomto potenciálním, ale zásadním, omezení kvantových výpočtů nic bližšího.

Představa, že do globálního stavu kvantově provázaného registru můžeme superpozicí vložit exponenciálně mnoho základních stavů je podle mne projevem bláhové nevědomosti o tom, jak rychle roste exponenciála, nebo hrubým podceněním toho růstu.

Ta nevědomost je rozšířená mezi laiky - je známa historie o odměně pro vynálezce šachové hry - šach si myslel, že $2^{64} - 1$ zrníček obilí bude pár pytlů, ale kdyby zrníčko mělo třeba $5 \times 2 \times 2$ milimetry, pak jelikož 2^{63} je přibližně třetí mocnina 2 milionů, potřebovali bychom pro odměnu za šachy sýpku např. 10 km $\times$ 4 km $\times$ 4 km.

A co víc, kdyby si podobně řekl o odměnu vynálezce hry *go* s deskou 19×19 hracích bodů, nevešla by se odměna ani do celého nám známého vesmíru, potřebovali bychom dokonce takových vesmírů řádově tisíc trilionů, protože vidíme asi do vzdálenosti

$$15 \text{ mld. světel. let} \approx 15{\cdot}10^9{\cdot}300000\text{km/sec} \cdot 365{\cdot}24{\cdot}3600\text{sec} \approx 0,15{\times}10^{24}\text{km} = 0,15{\times}10^{30}\text{mm}$$

takže objem nám známého vesmíru je asi $0,04 \times 10^{90}$ mm^3, což je asi
$40 \times 1000^{29} \approx 40 \times 2^{290}$ krychlových milimetrů,
zatímco pro vynálezce hry go by jich bylo potřeba $20 \times 2^{19 \times 19} = 20 \times 2^{361}$ mm^3 a navíc

$$2^{360}/2^{290} = 2^{70} \approx 1000^7 = 20^{21}.$$

U matematiků by bylo možné podcenění rychlosti růstu exponenciály pochopit, některým teprve Ackermannova funkce roste dostatečně rychle, ale informatici by si měli dát pozor.

Dodatek 1: RSA šifrování

V roce 1977 Ron Rivest, Adi Shamir a Leonard Adleman publikovali způsob šifrování s otevřeným klíčem, který se postupně stal jedním z hlavních nástrojů bezpečné komunikace v digitálním světě. Není cílem tohoto článku podrobně popisovat výhody a použití RSA šifrování, uvedu pouze jeho základní princip.

Základem je velmi velké číslo n, které je součinem dvou (obvykle dosti podobně velkých) prvočísel, tedy $n = pq$. Číslo n je veřejně známo a každý, kdo si ho přečte, umí šifrovat. Na druhé straně čísla p a q jsou pečlivě chráněna tím, kdo je vytvořil a kdo je příjemcem šifrovaných zpráv, protože jen takový uživatel sítě umí zašifrované zprávy dešifrovat.

Proto se RSA šifrování říká šifra s otevřeným klíčem. U dřívějších systémů každý, kdo se seznámil s šifrovacím klíčem, jen s vynaložením mírné duševní námahy mohl také úspěšně dešifrovat. U RSA systému je možné šifrovací algoritmus publikovat veřejně v novinách nebo na síti a přesto dešifrovat budou (za našich současných znalostí) umět jen zasvěcenci, kteří znají tajný dešifrovací algoritmus.

Princip je takovýto (všechna dále uváděná čísla jsou celá nezáporná čísla):

1. Vytvoří se dvě velká prvočísla p a q.
2. Spočítá se a zveřejní jejich součin $n = pq$, a ne ne čísla samotná.
3. Spočítá se hodnota Eulerovy funkce $\phi(n) = (p-1)(q-1)$, což je snadné pro toho, kdo zná čísla p a q, ale není znám dostatečně rychlý způsob, jak ji spočítat, známe-li pouze n.
4. Zvolí se celé číslo e, menší než $\phi(n)$ a nesoudělné s $\phi(n)$.
5. Nalezne se d takové, že $de \equiv 1 \ mod \ \phi(n)$.

Šifrování se provádí takto: zasílaná zpráva se vhodným způsobem zapíše nebo přemění na celé číslo m, které je menší než n. Kdyby byla zpráva příliš dlouhá, rozdělí se do bloků, které se šifrují a odesílají každý zvlášť. Zašifrovaným textem je pak číslo

$$c = m^e \ mod \ n.$$

Dešifrování zašifrované zprávy c se provede výpočtem

$$m = c^d.$$

O tom, že výraz c^d bude skutečně původní číslo m svědčí následující úvaha:

$$c^d \equiv (m^e)^d = m^{de} = m^{1+k(p-1)(q-1)} = m \cdot \left(m^{p-1}\right)^{k(q-1)} \equiv m \ mod\ p,$$

protože malá Fermatova věta říká, že $m^{p-1} \equiv 1 \ mod\ p$, a podobně je tomu i modulo q, což dává podle čínské větě o zbytcích i rovnost $c^d \equiv 1 \ mod\ n$.

Šifrování je bezpečné, pokud ze znalosti n není možno v rozumně krátké době ani za pomoci nejsilnějších počítačů nalézt jeho faktorizaci $n = pq$.

Dodatek 2: Testování prvočíselnosti a hledání velkých prvočísel

RSA metoda vyžaduje umět vytvořit velká prvočísla (třeba stovky či dokonce tisíce cifer), která nejsou známa z žádného seznamu prvočísel. Provádí se to tak, že se najde hodně velké liché číslo, které se pak zvyšuje o 2 tak dlouho, až se najde prvočíslo. Věty o hustotě prvočísel (zde neuváděné) říkají, že umíme-li rychle testovat prvočíselnost, na první prvočíslo se přijde obvykle dostatečně brzo.

Jak se tedy dá testovat prvočíselnost. Systematické hledání faktorů třeba Eratosthenovým sítem je pro obrovská čísla extrémně pomalé a tudíž nepoužitelné. Je znám deterministický algoritmus, který prvočíselnost umí otestovat. Sice je pro něj dán relativně dobrý (polynomiální) odhad doby výpočtu v závislosti na počtu číslic testovaného čísla, ale pro praktické účely je stále příliš pomalý a také složitý.

Používá se proto pravděpodobnostní algoritmus, které se sice může splést (o nějakém složeném čísle může chybně prohlásit, že to je asi prvočíslo - na opačnou stranu se nikdy nesplete), ale pravděpodobnost chyby se dá snížit natolik, že je menší než odhadovaná pravděpodobnost, že na nás zrovna v tu chvíli z vesmíru spadne obrovský meteorit a výsledek už nebudeme potřebovat.

Základem, ještě ne úplným, ale ve většině případů dostatečným, je malá Fermatova věta: pokud p je prvočíslo, pak pro každé a takové, že $1 < a < p$, je $a^{p-1} \equiv 1 \ mod\ p$.

Jestliže tedy nalezneme a takové, že $a^{p-1} \not\equiv 1 \ mod\ p$, pak p určitě *není* prvočíslo, je to číslo složené. Pokud zkoušíme takové a najít a nedaří se to, pak po jisté době kapitulujeme a prohlásíme p za (asi) prvočíslo.

Tento postup funguje obvykle velmi dobře, ale jsou jistá složená čísla, pro které je takových průkazů složenosti tak málo, že je hodně nepravděpodobné, že se na ně trefíme náhodně. Proto test (průkaz složenosti za pomoci vhodného a) zesílíme.

Vyjdeme přitom z následujícího tvrzení:
Je-li p prvočíslo a x je celé číslo v rozmezí $1 \leq x < p$ takové, že $x^2 \equiv 1 \ mod\ p$, pak je

buď $x \equiv 1 \ mod \ p$ nebo $x \equiv -1 \ mod \ p$.

Předpoklad o x totiž říká, že $(x^2 - 1) \equiv 0 \ mod \ p$, neboli $(x + 1)(x - 1) \equiv 0 \ mod \ p$. Pokud je p prvočíslo, pak sčítání a násobení modulo p vytváří *těleso*, což mimo jiné znamená, že pokud $ab \equiv 0 \ mod \ p$, pak musí být buď $a \equiv 0 \ mod \ p$ nebo $b \equiv 0 \ mod \ p$, což v našem případě říká, že buď $(x + 1) \equiv 0 \ mod \ p$ nebo$(x - 1) \equiv 0 \ mod \ p$.

Sluší se poznamenat, že uvedené nemusí platit, pokud p není prvočíslo. Například $2 \cdot 4 \equiv 0 \ mod \ 8$ a $3^2 = 9 \equiv 1 \ mod \ 8$, ale $3 \not\equiv \pm 1 \ mod \ 8$.

Nechť je tedy dáno testované číslo p a náhodně zvolené a.

Pokud $a^{p-1} \equiv 1 \ mod \ p$, tak zkusíme číslo

$$x = a^{\frac{p-1}{2}}.$$

Protože $x^2 \equiv 1 \ mod \ p$, pak pokud p je prvočíslo, z výše uvedeného plyne, že x musí být buď +1 nebo -1.

Zjistíme-li tedy že x není ani +1 ani -1, pak p je určitě složené a testování končí.

Pokud $a^{(p-1)/2} \equiv -1$, test už dále nepokračuje, ale pokud $a^{(p-1)/2} \equiv 1$ a $p - 1$ je dělitelné 4, zkusíme podobně zda $x = a^{(p-1)/4} \equiv \pm 1$ atd.

Formálně tedy:

Test(a,p)
k = 1;
loop: spočítej $x = a^{(p-1)/k}$;
jestliže x není ani +1 ani -1 modulo p, pak konec výpočtu, p je číslo složené;
jestliže x je -1 modulo p, pak konec výpočtu, vypadá to, že p je prvočíslo;
(pokud dojdeme sem, je $x \equiv 1 \ mod \ p$)
k = k*2; jestliže $p - 1$ je dělitelné číslem k, pak goto loop,
jinak konec výpočtu, vypadá to, že p je prvočíslo.

Například $a = 44$, $p = 129$ (není prvočíslo, $129 = 3 \cdot 43$):
platí $44^{128} \equiv 44^{64} \equiv 44^{32} \equiv 44^{16} \equiv 44^8 \equiv 44^4 \equiv 44^2 \equiv 1 \ mod \ 129$
ale $44^1 = 44 \not\equiv \pm 1$.

Na druhé straně například pro $a = 256$, $p = 257$ (je prvočíslo):
$256^{256} \equiv 256^{128} \equiv 256^{64} \equiv 256^{32} \equiv 256^{16} \equiv 256^8 \equiv 256^4 \equiv 256^2 \equiv 1 \ mod \ 257$
protože $a \equiv -1 \ mod \ 257$

Dodatek 3: Důkaz z kapitoly o Simonovu algoritmu

Uvažujme kvantový registr s n qubity a prozkoumejme nejprve, jak vypadá Hadamardova transformace jeho stavu $x = |x_1 x_2 \dots x_n\rangle$.

Jsou-li $u = (u_1, \ldots, u_n)$ a $u = (u_1, \ldots, u_n)$ dva bitové vektory (tedy jejich složky jsou O nebo 1), pak označíme jako $u \odot v$ číslo

$$u \odot v = u_1 v_1 + \cdots + u_n v_n \ mod\ 2.$$

Výraz $\odot$ tedy označuje skalární součin v n-dimenzionálním prostoru nad tělesem Z_2 celých čísel modulo 2.

Součin $u \odot v$ je tedy vždy 0 nebo 1.

Hadamardova transformace stavu $|b\rangle$, kde b je 0 nebo 1, se dá napsat jako $|0\rangle + (-1)^b|1\rangle$.

Proto Hadamardova transformace registru $|b_1 \ldots b_n\rangle$ bude

$$(|0\rangle + (-1)^{b_1}|1\rangle)(|0\rangle + (-1)^{b_2}|1\rangle)\cdots|0\rangle + (-1)^{b_n}|1\rangle = \sum_{y\in\{0,1\}^n} (-1)^{b_1 y_1 + \cdots + b_n y_n}|y_1 \ldots y_n\rangle =$$

$$= \sum_{y\in\{0,1\}^n} (-1)^{b\odot y}|y\rangle.$$

Po prvních dvou krocích Simonova algoritmu je levá polovina qubitů ve stavu, který je roven součtu dvou elementárních stavů, které jsou funkcí Φ Simonova algoritmu převáděny do téhož vektoru, toho, který byl změřen na pravé polovině qubitů algoritmu. Označíme-li jeden jako x, pak druhý bude na základě vlastností funkce Φ roven $x \oplus a$.

Nyní se podívejme, jak se součtový stav $x+(x\oplus a)$ změní Hadamardovou transformací. Na základě výše uvedeného dostaneme

$$\sum_y \left((-1)^{x\odot y} + (-1)^{(x\oplus a)\odot y}\right)|y\rangle = \sum_y \left((-1)^{x\odot y} + (-1)^{x\odot y}(-1)^{a\odot y}\right)|y\rangle.$$

Na pravé straně vidíme, že součet dvou členů v koeficientu u nějakého $|y\rangle$ je nenulový právě když $a\odot y$ je roven nule. Po Hadamardově transformaci je tedy levá polovina qubitů ve stavu, který je roven uniformní superpozici stavů, daných právě těmi vektory y, které jsou kolmé na a (neboli těch, pro které je $a \odot y = 0$). Ať tedy změřením levé poloviny Hadamardovsky transformované levé poloviny bitů dostaneme jakýkoli vektor, víme, že bude kolmý na a-

Dodatek 4: Důkaz lemmatu z kapitoly o faktorizaci

Bude v blízké době doplněn.