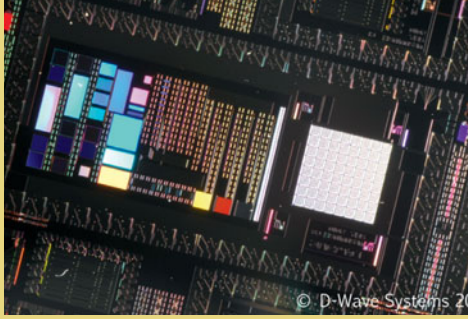
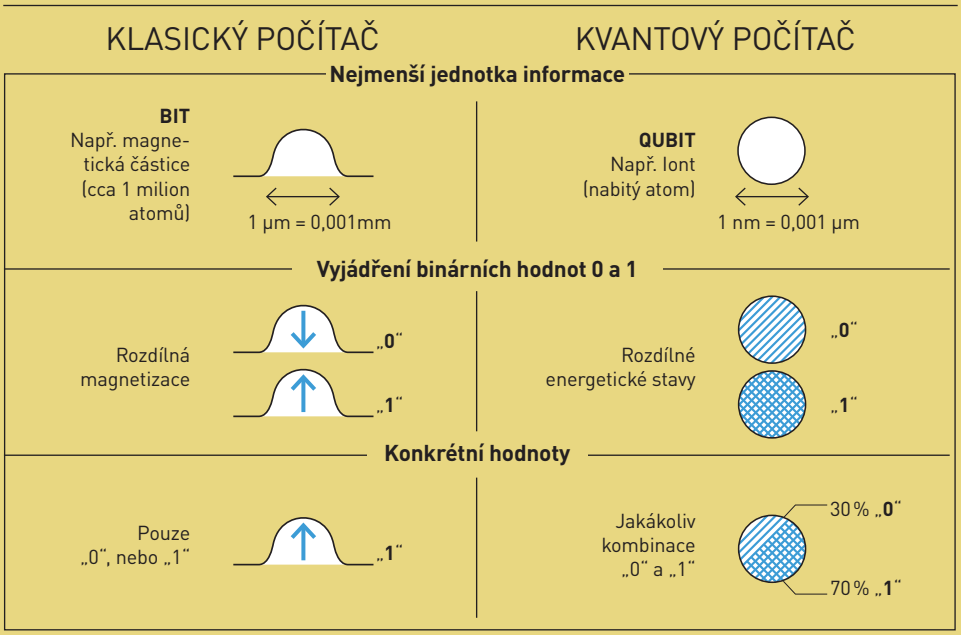
KVANTOVÉ POČÍTAČE



Běžné počítače používají jedničky a nuly. Kvantové počítače počítají pouze s pravděpodobností jedniček a nul. Proto také mohou v extrémně krátkém čase zpracovávat ohromné množství dat. Vděčí za to dvěma fyzikálním jevům, zvaným superpozice a kvantové provázání.

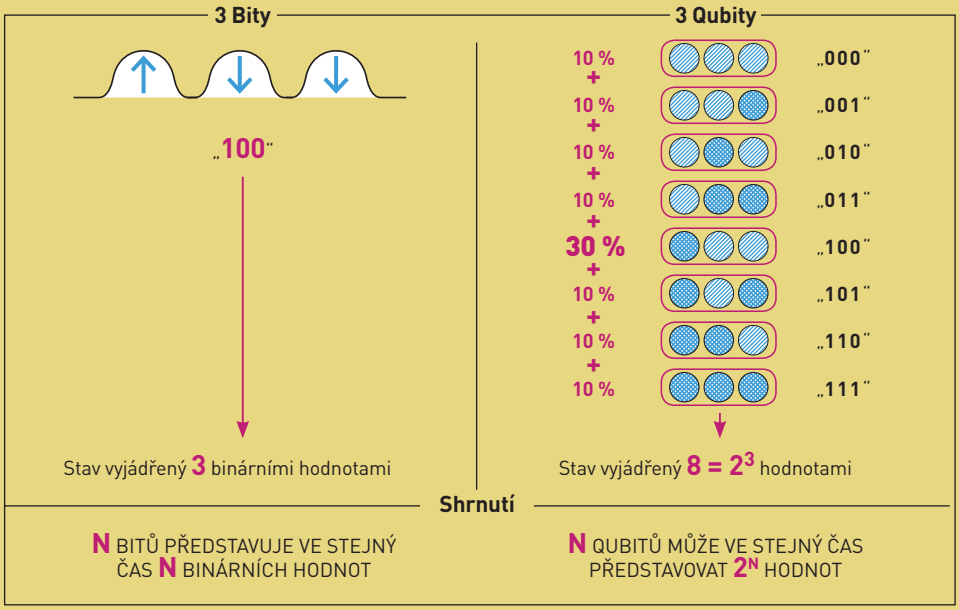
SUPERPOZICE

Kvantový bit (qubit) může zároveň nabývat hodnoty „1“ i „0“, avšak nabývá jí s určitou pravděpodobností, např. 30 % a 70 %. To znamená, že existuje 70% pravděpodobnost, že daný qubit má hodnotu „1“. Výhodou je, že kvantové počítače vykazují zároveň různé bitové hodnoty, avšak s různou úrovní pravděpodobnosti.



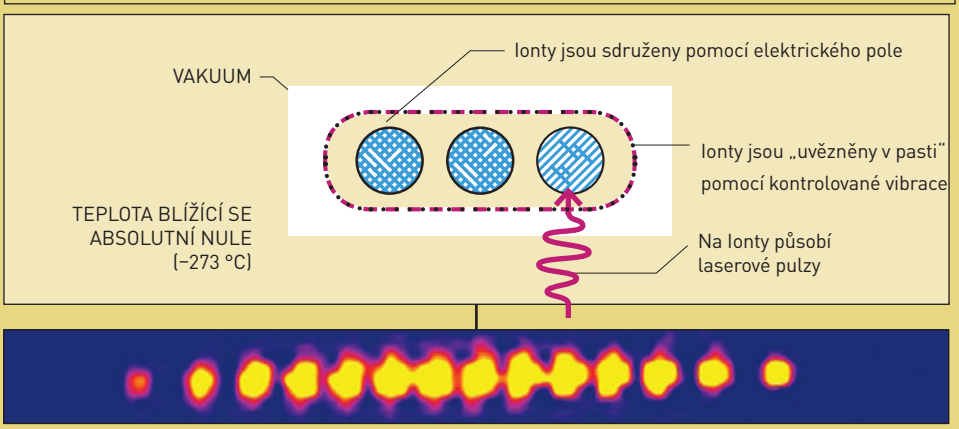
KVANTOVÉ PROVÁZÁNÍ

Několik qubitů může zároveň dosahovat stejného stavu. Například tři qubity mohou nabýt hodnoty všech možných kombinací od „000“ do „111“, přičemž každý stav je reprezentován určitou pravděpodobností. Například stav „100“ tak nikdy nebude jednoznačný, bude mít jen vyšší pravděpodobnost než ostatní. Výhodou je, že N qubitů může zároveň představovat 2^N hodnot. 10 quibitů tedy může dosahovat 1 024 hodnot.



VYUŽITÍ

Aby mohly kvantové jevy, jako je superpozice a kvantové provázání, nastat a co nejdelší čas trvat, musí být systém odstřižen od externích vlivů. Pro účely výpočtu je kvantový bit (qubit) ovlivňován laserovým pulzem, který mění stav všech kvantových provázání.



QUBITY: Nevypočitatelná logika paralelních výpočtů

Kvantové počítače mohou zásadně zrychlit chod počítačů a přinést revoluci do IT. První komerčně dostupná zařízení jsou již na trhu.

MARTIN MICHL

Společnosti Lockheed Marin, Google a NASA mají jedno společné: vlastní kvantový počítač, vyvinutý firmou D-Wave. Jakmile se objevily první zprávy o funkčním kvantovém počítači, okamžitě se ozvaly varovné hlasy. A obavy jsou namístě – takový počítač by totiž dokázal snadno rozluštit jakékoliv v současnosti používané šifrování. Kvantové počítače pracují na principu složitých zákonů kvantové atomární fyziky a jsou naprosto odlišné od počítačů, jaké známe a používáme dnes. Nejmenší informační jednotkou, se kterou pracují, je tzv. qubit (kvantový bit). Na rozdíl od běžného bitu nedosahuje pouze hodnot „0“, nebo „1“, ale nabývá obou hodnot najednou. Díky tomu mohou kvantové počítače zpracovávat mnohonásobně větší objemy dat. Pouhých 250 qubitů dokáže najednou uchovat více informací, než kolik je atomů ve vesmíru. Nejnovější počítač od společnosti D-Wave má mít dokonce 512 qubitů!

Již v devadesátých letech teoreticky dokázali američtí vědci Lov Grover a Peter Shor, že kvantové počítače by dokázaly prohledávat velké databáze a provádět faktorizaci velkých čísel mnohem efektivněji než klasické počítače. Kvantové výpočty by také radikálně zkrátily výpočetní čas potřebný k prolomení šifrovacích metod AES a RSA a prakticky by tak ohrozily samotnou existenci tohoto typu zabezpečení. I když jsou již dnes dostupné první komerční systémy kvantové kryptografie, které pracují s qubity, prozatím se používají pouze k výměně bezpečnostních klíčů.

Extrémní požadavky

Přes všechny obavy a nadšení se ozývají skeptické hlasy, které zpochybňují to, zda společnost D-Wave opravdu sestavila funkční kvantový počítač. Na vývoji podobného stroje pracují vědecké týmy již řadu let, a přesto se jim dodnes nepodařilo postoupit dál než k prvním laboratorním krůčkům. Důvodem jsou zejména obzvláště náročné technologické předpoklady: nejprve ze všeho je třeba vytvořit qubity z částic atomu, protože požadované kvantové jevy se odehrávají právě pouze na úrovni těchto subatomárních částic. Za druhé je tento systém nutné dokonale oddělit od okolí a zchladit jej na teplotu blížící se absolutní nule, protože jinak by kvantové jevy byly okamžitě rušeny externími vlivy. Třetí problém pak spočívá v tom, že k uzavřenému a podchlazenému systému musí existovat přístup zvenčí. Pouze tak lze totiž do systému zadávat výchozí hodnoty qubitů, zajistit kvantově-mechanické provázání qubitů, ovládat požadované operace a nakonec i přečíst výsledky provedených výpočtů. Vývojáři doposud využívali do role qubitů jednotlivé ionty nebo fotony, jaderné spiny atomů, a dokonce páry supravodivých elektronů, přičemž všechny tyto systémy se v podstatě vymykají hranicím naší představivosti.

Před zveřejněním zprávy společnosti D-Wave držel rekord systém 14 qubitů řetězených z iontů vápníku, který vyvinuli v roce 2011 na univerzitě v Innsbrucku, a prototyp bristolské univerzity, který v roce 2012 dokázal rozložit číslo 21 na součinitele 3 a 7. To jsou ale jen drobné úspěchy. V čem se od nich D-Wave liší? Spekulace se pomalu uklidňují s tím, jak tato společnost zveřejňuje další údaje o tom, co se vlastně skrývá v počítači uzavřeném do ohromné černé skříně. D-Wave používá qubity vytvořené ze supravodivých smyček, uložených na mikročipu, které řídí a jejichž výsledky čte dnes běžně komerčně dostupná elektronika. Kritici tedy spekulují, zda se opravdu jedná o kvantově mechanicky provázaný stroj, nebo zda nejde o obyčejný počítač.

Použití je stále omezené

Zajímavostí stroje D-Wave není pouze jeho technologická výbava, ale též celý koncept tohoto počítače. Jeho program dokáže prozatím řešit jedinou úlohu, kterou je známý „Problém obchodního cestujícího“, tedy algoritmus, který má ze seznamu míst a vzdáleností mezi nimi vyvodit nejvýhodnější možnou trasu, která protne každé město jen jednou a poté se vrátí do výchozího bodu. Tento problém řeší systém D-Wave podle fyzikálního principu minimální energie a postupně se blíží ideálnímu řešení, které je následně přečteno prostřednictvím elektroniky počítače. Zde však narážíme na další problém kvantových počítačů: jelikož qubity nabývají hodnot nula a jedna pouze s určitou pravděpodobností, tak i správný výsledek má pouze určitou pravděpodobnost. Výpočty, ze kterých vyšel, je nutné dostatečněkrát opakovat, dokud výsledek nedosáhne dostatečně statisticky akceptovatelné jistoty.

Ohromný potenciál kvantových počítačů spočívá v jejich výpočetní rychlosti, kterou zajišťuje masivní a v podstatě nezměřitelná úroveň paralelizace výpočtů. Zároveň ale i tyto počítače podléhají zákonům informatiky, a i když dokážou řešit úlohy v extrémně rychlém čase, hodí se pouze na takový typ úloh, ve kterých je možné z velkého množství pravděpodobných řešení „odhadnout“ jednu správnou odpověď. To je právě i případ výše zmíněného Groverova i Shorova algoritmu a „Problému obchodního cestujícího“. Všechny tři problémy patří do stejného typu úloh a jsou si v základu podobné.

Co se týče běžného zpracování dat, jakým je například komprimace videa nebo 3D výpočty, nepřináší kvantový počítač žádné rychlostní výhody. Do jaké míry dokáže D-Wave pomoci Googlu při analýze dat, tedy zůstává záhadou. AUTOR@CHIP.CZ