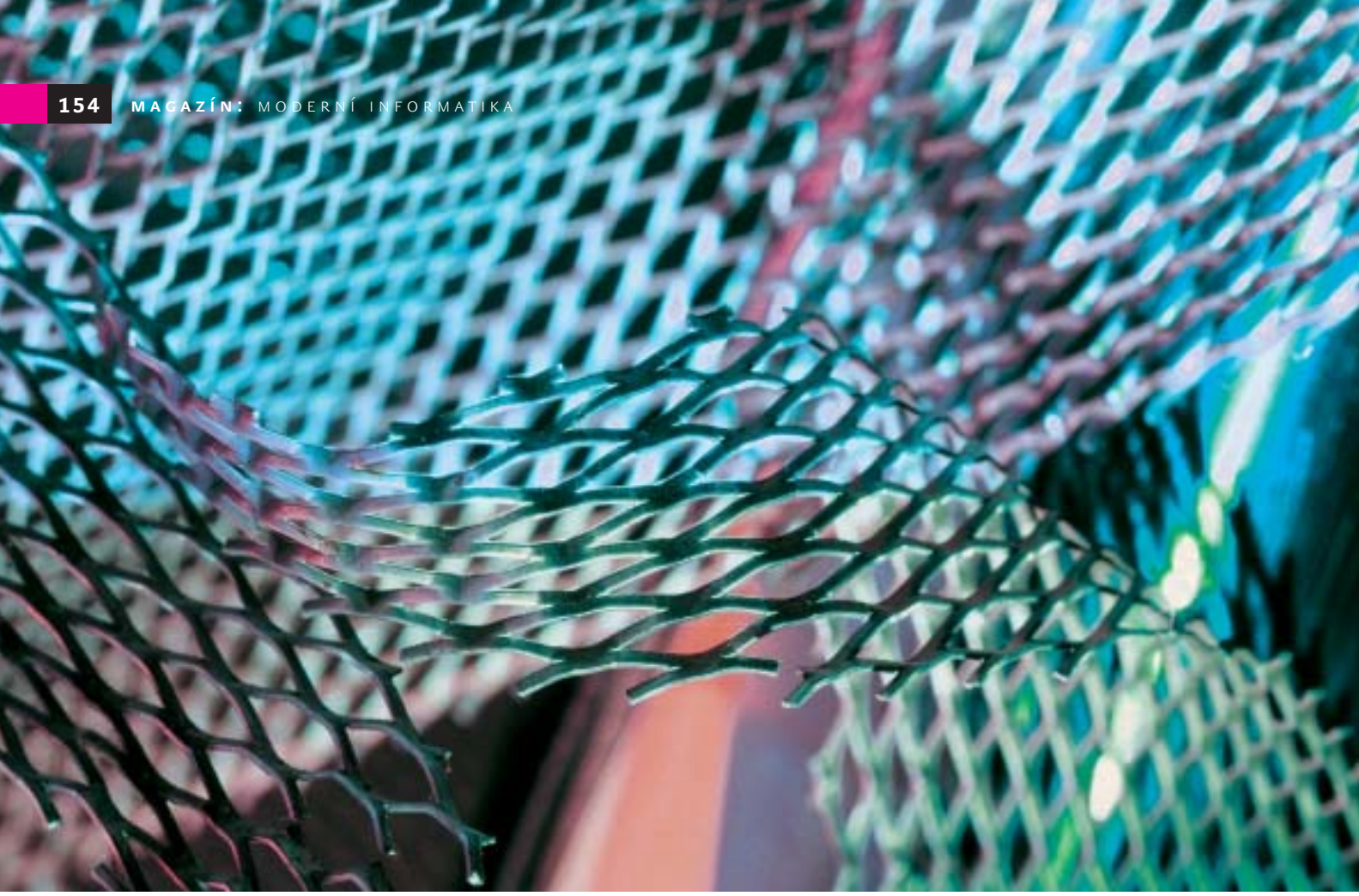


JEMNÝ ÚVOD DO KVANTOVÉHO POČÍTÁNÍ

(2.)

Od **bitů** ke **qubitům**

V druhé části našeho povídání se zaměříme na srovnání efektivity kvantových a klasických počítačů. Ukážeme si, jaké teoretické nástroje zde máme k dispozici a jakých výsledků s nimi bylo dosud dosaženo.

V tomto článku od bitů i qubitů trochu odbočíme, abychom si připravili půdu pro další výklad. Budeme se proto věnovat informatické disciplíně zvané ***teorie složitosti***, bez jejíchž základů se na cestě za poznáním schopností kvantových počítačů neobejdeme. Poznamenejme, že její výklad lze účelně pojmout v zásadě dvěma extrémními způsoby: čistě formálně, nebo čistě populárně. Zde budeme sledovat spíše onu populární linii; zájemcům preferujícím formální přístup doporučuji výborně zpracovanou úvodní knihu [3].

ÉRA TURINGOVÝCH STROJŮ

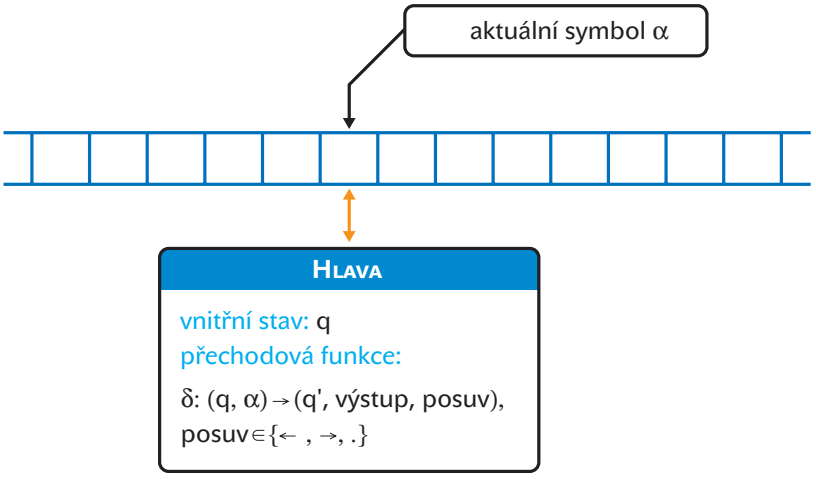
Psal se rok 1900, když německý matematik David Hilbert (ano, právě ten, po němž nazýváme prostor popisující stav kvantového systému) přednesl na mezinárodním matematickém kongresu v Paříži svých proslulých 23 problémů, jejichž vyřešení se z jeho pohledu zdálo být pro tehdejší matematiku zásadní. A byl to, mimo jiné, právě třiadvacátý Hilbertův problém, který o 36 let později přivedl anglického matematika Alana Turinga k formulaci konceptu tzv. ***Turingova stroje***.

Turingovým cílem bylo poznat meze mechanických výpočetních systémů – zejména s ohledem na to, co jsou tyto stroje schopny vůbec vyřešit. Z dnešního úhlu pohledu bychom také mohli říci, že Turing se zabýval otázkou, jaké úlohy lze naprogramovat a nechat vyřešit počítačem, a jaké nikoliv. Poznání těchto mezí bylo pro úspěšné vyřešení 23. Hilbertova problému podstatné, neboť volná formulace jeho zadání se ptá, zda lze sestavit výpočetní stroj, který bude sloužit pro rutinní rozhodování o platnosti či neplatnosti předložených výroků vzhledem ke stanovené teorii. Stroj na každý předložený výrok jasně odpoví: Platí/neplatí. Podle této formulace byl celý problém pojmenován jako ***rozhodovací problém*** (v originále *Entscheidungsproblem*).

Úkolem Turingova stroje bylo mechanickým způsobem simulovat práci matematika provádějícího formální důkaz. Základním prvkem (samozřejmě abstraktního) stroje (viz obrázek 1) je proto *hlava*, která je schopna pohybovat se vpřed nebo vzad po *nekonečně dlouhé pásce* rozdělené na políčka, kde každé políčko může obsahovat nějaký symbol z konečné abecedy znaků (většinou se volí abeceda binární), nebo být prázdné. Činnost tohoto stroje sestává z posloupnosti jednotlivých kroků. V každém kroku je z aktuální pozice hlavy přečten symbol na pásce a na základě tohoto symbolu a *vnitřního stavu* stroje dojde k:

- přechodu do nového vnitřního stavu;
- zápisu symbolu na pásku (formou přepisu symbolu na aktuální pozici hlavy);
- přesunu hlavy o jedno políčko vzad, vpřed, anebo hlava zůstane na původním místě.

Obdobou programu je u Turingova stroje takzvaná *přechodová funkce*, která na základě aktuálního symbolu z pásky a vnitřního stavu stroje určuje následující vnitřní stav, symbol zapsaný na pásku a případný pohyb



Obr. 1. Schéma deterministického Turingova stroje

hlavy. Vstupní úloha se tomuto stroji předkládá tak, že se před jeho spuštěním zapíše na pásku a hlava se nastaví na začátek této úlohy. Poté se stroj spustí a čeká se, až dojde k jeho zastavení v některém z *koncových stavů* (zvláštní kategorie vnitřních stavů). Odpovědí je pak buď aktuální konfigurace pásky, nebo přímo hodnota koncového stavu. S jistou dávkou představivosti lze nahlédnout, že tento stroj se vlastně navenek chová právě tak, jako když matematik pracuje se svými poznámkami.

Původní rozhodovací problém potom přeformuloval Turing na problém ***zastavení Turingova stroje*** (v originále *Halting Problem*). V něm se ptáme, zda existuje takový Turingův stroj, který při předložení popisu jiného Turingova stroje spolu se zadáním jeho vstupu rozhodne, zda se předložený stroj někdy (v konečném čase) zastaví a předá výsledek, či zda nikdy do žádného koncového stavu nedospěje. Obdržený závěr byl tehdy dost nepříjemným překvapením: Turing zjistil, že takový stroj nelze sestavit, a že tudíž odpověď na 23. Hilbertův problém je zamítavá – matematici nemohou jednoduše předat svou práci strojům.

O ještě větší překvapení se pak postaral brněnský rodák Kurt Gödel, když ukázal, že dokonce i v samotné formální teorii, která je konzistentní (nelze zároveň dokázat platnost a neplatnost nějakého výroku), lze sestavit takový výrok, o jehož platnosti nelze rozhodnout! Dokonce tedy i „člověčí" matematik tak může být postaven před otázku, na kterou nebude schopen znát jasnou odpověď.

Blíže k praxi

Záhy s nástupem prvních „skutečných" výpočetních mechanismů se zjistilo, že nestačí jen ptát se, zda je daná úloha strojově řešitelná (Turing zavedl pojem *vypočitatelná – computable*, též se používá výraz *algoritmicky rozhodnutelná*), ale že je nutné se také ptát, jaké nároky si řešení těch řešitelných úloh klade. I v těchto otázkách si Turingovy stroje udržely své pevné pozice, čímž z dnešního pohledu daleko překročily původní snahu o vyřešení 23. Hilbertova problému. Bylo totiž ukázáno (přesněji: zčásti dokázáno a zčásti přijato jako paradigma), že Turingovy stroje jsou nejen povedenou abstrakcí výpočetních strojů, pokud jde o otázky vypočitatelnosti úloh, ale i pokud jde o otázky složitosti řešení úloh, které vypočitatelné jsou. Hlavní paradigma Turingova stroje lze názorně ilustrovat takzvanou kvantitativní Churchovou tezí (viz [4]), která zhruba říká, že *každý fyzikální výpočetní systém může být simulován na Turingově stroji s polynomiální časovou složitostí vzhledem k prostředkům použitým simulovaným systémem během výpočtu*.

Právě jsme použili pojem ***složitost***. Jak již jeho intuitivní chápání napovídá, představujeme si pod tímto pojmem náročnost výpočtu dané úlohy měřenou **spotřebou fyzikálních prostředků** (připomeňme, že provádění výpočtů chápeme jako mapování abstraktní matematiky na fyzikální procesy). Mezi tyto prostředky patří zejména **čas** (na Turingově stroji vystupuje jako počet kroků do zastavení) a **paměť** (koresponduje s využitou kapacitou pásky). V populárně laděných výkladech se většinou hlavní pozornost soustřeďuje na náročnost časovou (což už se pak explicitně nezmiňuje).

Na obrázku 2 vidíte základní dělení vypočitatelných úloh podle toho, jakou mají složitost. Do **třídy (množiny) P** (od slova *polynomial*) řadíme všechny úlohy, které jsou zvládnutelné nejhůře s polynomiální složitostí, což znamená, že jejich náročnost lze vyjádřit jako polynomiální funkci délky vstupu. Například úloha, která pro n-bitový vstup trvá $2n^2+1$ kroků, má polynomiální časovou složitost. Úlohy náležející do třídy P většinou označujeme jako *výpočetně zvládnutelné*.

Ve **třídě (množině) NP** (od výrazu *nondeterministic polynomial*) jsou úlohy, jejichž řešení lze s nejhůře polynomiální složitostí **ověřit** jako správné. Na rozdíl od úloh v P však pro úlohy v NP nemusíme být schopni sestavit polynomiálně složitý postup pro nalezení řešení. Odtud označení „nedeterministické“, neboť první část výpočtu těchto úloh spočívá laicky řečeno v „uhodnutí“ výsledku a druhá pak v jeho ověření.

Speciální skupinu úloh pak tvoří takzvané **NP-úplné** (*NP-complete*) problémy. To jsou úlohy, na jejichž řešení lze převést (s polynomiální složitostí) libovolný jiný problém ze třídy NP. Nalezení polynomiálního způsobu řešení libovolné z NP-úplných úloh by tak znamenalo, že platí rovnost P=NP. Důkaz platnosti (respektive neplatnosti) této rovnosti je pro teorii složitosti něco jako hledání Svatého grálu. Zatím se však nezdá, že by zde šlo dosáhnout nějakého výsledku. Problémy, o nichž se domníváme, že patří do rozdílové množiny NP\P, označujeme jako *výpočetně nezvládnutelné*. Právě o tyto problémy má eminentní zájem například současná kryptografie.

Hledání výjimek

Formulace výše uvedeného paradigmatu o univerzálnosti Turingova stroje je zároveň silnou výzvou pro hledání výjimek, které by oprávněnost tohoto přístupu vyvrátily (a tím změnily náš pohled na otázky složitosti a možná i vypočitatelnosti). Jako vodítko na této cestě lze použít předpoklad, že ono „něco“ by měl být fyzikální proces, na který lze namapovat nějaký výpočetní postup a jehož simulace na Turingově stroji není polynomiálně zvládnutelná. Čas od času se ve fyzice nějaký aspirant na sesazení Turingova stroje objeví, avšak záhy je pro „nedostatek důkazů“ od sesazování upuštěno. Jedna věc je totiž najít proces, pro který **neznáme** polynomiálně složitou simulaci na Turingově stroji, a druhá věc je dokázat, že tato simulace **neexistuje**.

Každý fyzikální proces, pro který neznáme polynomiálně složitou simulaci na klasickém Turingově stroji, může zásadně ovlivnit teorii složitosti a související oblasti, jako je kryptografie.

Během experimentování s konceptem Turingových strojů se vytvořila odnož označovaná jako *pravděpodobnostní Turingovy stroje*. Zjednodušeně řečeno jde o Turingův stroj vybavený zdrojem náhodných čísel, který je využíván jeho přechodovou funkcí. Některé přechody se tak uskutečňují jen s určitou pravděpodobností (stroj ovšem vždy s jistotou „někam“ přejde). Uznává se, že pokud jde o vypočitatelnost, jsou na tom pravděpodobnostní Turingovy stroje stejně jako jejich předchůdci (ty se v tomto kontextu označují jako *deterministické*).

Pravděpodobnostní stroje se však liší svou efektivitou, která se u některých úloh projevuje dosti podstatně. Pro účely klasifikace byly zavedeny rovněž „pravděpodobnostní“ třídy složitosti, které společně s těmi „deterministickými“ shrnuje tabulka 1. Pokud jde o případné sesazení, tak si Turingovy stroje díky svým pravděpodobnostním „potomkům“ celkem upevnily své pozice, neboť v řadě případů je efektivní převod případných konkurentů na pravděpodobnostní Turingův stroj dobře vidět (nebo naopak činí problém ukázat, že zde tento převod neexistuje).

Kvantové počítače

Z hlediska teoretické informatiky začal zájem o kvantové počítače přesně v duchu výše uvedeného doporučení a byl to právě známý fyzik (a nositel Nobelovy ceny) Richard P. Feynman, kdo patrně jako první současně poznamenal, že:

1) kvantové systémy lze použít k realizaci výpočtů;
2) simulace kvantových systémů na Turingově stroji se zdá mít exponenciální složitost.

Hon na Turingův stroj tak mohl začít. Aby bylo možné lépe studovat schopnosti kvantových počítačů v porovnání s těmi klasickými, bylo roku 1985 Davidem Deutschem formulováno paradigma ***kvantového Turingova stroje***. Jeho popis je již poněkud složitější, než byl popis deterministického či pravděpodobnostního Turingova stroje (ty budeme dále shrnovat pod označením „klasický“), takže se zde omezíme pouze na důležitou principiální odlišnost. Ta spočívá v tom, že „páska“ kvantového stroje je chápána jako *kvantový registr* (viz předchozí díl), což

Tab. 1. Klasické třídy složitosti

Označení třídy	Popis	Poznámka
P (Polynomial)	Řešitelné s nejhůře polynomiální složitostí	Příklad: násobení dvou čísel
NP (Nondeterministic Polynomial)	Řešení je ověřitelné s nejhůře polynomiální složitostí	Příklad: faktorizace celého čísla
ZPP (Zero-sided Probabilistic Polynomial)	Pravděpodobnostně řešitelné s polynomiální střední hodnotou složitosti; pravděpodobnost chyby = 0	
BPP(Bounded Error Probabilistic Polynomial)	Pravděpodobnostně řešitelné v nejhůře polynomiálním čase; pravděpodobnost chyby ≤ 1/3	Příklad: Miller-Rabinův test prvočíselnosti. Chybovost lze eliminovat nezávislými opakováními algoritmu

Tab. 2. Kvantové třídy složitosti

Označení třídy	Popis	Poznámka
QP (Quantum Polynomial)	Řešitelné s nejhůře polynomiální složitostí na kvantovém počítači	P ⊆ QP, existuje relativizovaná separace
ZQP (Zero-sided Quantum Polynomial)	Řešitelné v polynomiální střední hodnotě složitosti na kvantovém počítači; pravděpodobnost chyby = 0	ZPP ⊆ ZQP, existuje relativizovaná separace
BQP (Bounded Error Quantum Polynomial)	Řešitelné s nejhůře polynomiální složitostí na kvantovém počítači; pravděpodobnost chyby ≤ 1/3	Příklad: Shorův algoritmus

mimo jiné znamená, že po dobu koherentního výpočtu může existovat v superpozici několika vlastních stavů.

Tento náhled dává plně vyniknout jevu označovanému jako *kvantový paralelismus*: Mějme úsek pásky o délce n políček. U klasického stroje to znamená, že máme k dispozici n bitů, na které můžeme zakódovat například jedno z 2^n možných zadání nějaké vstupní úlohy. Jakmile stroj spustíme, rozběhne se řešení zadaného problému a po zastavení stroje (pokud k němu dojde) obdržíme k tomuto zadání příslušný výsledek.

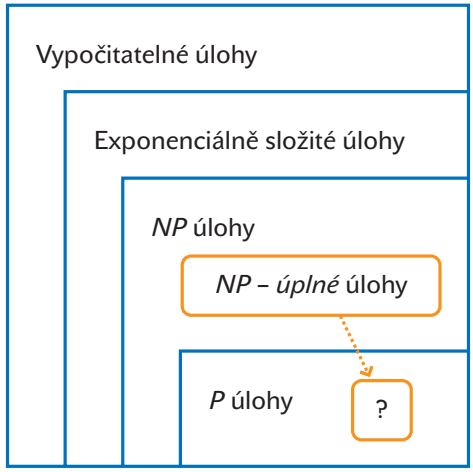
Nyní si představme situaci u stroje kvantového. Zde jedno políčko znamená jeden qubit, takže máme k dispozici pásku o n qubitech. Víme, že tato páska se může nacházet v superpozici tvořené až 2^n stavy současně. To znamená, že například všechna zadání úlohy o délce n bitů můžeme naráz uložit na pásku a po spuštění stroje je nechat všechna paralelně vyřešit tak říkajíc „jedním vrzem"! Jakmile se stroj zastaví, obdržíme stav odpovídající superpozici příslušných řešení. Celá věc má však jeden podstatný háček – víme, že měřením takového stavu obdržíme pouze jeden z vlastních stavů. Odpůrci kvantového počítání se v tomto okamžiku škodolibě usmívají a prohlašují, že stejného výsledku je možné dosáhnout použitím pravděpodobnostního Turingova stroje.

Uzavřít teorii kvantového počítání položením rovnítka mezi kvantový a pravděpodobnostní Turingův stroj by však bylo příliš ukvapené. Pokud by se kvantový registr mohl pochlubit pouze prostou existencí superponovaných stavů, pak by pravděpodobnostní stroje patrně skutečně oslavily vítězství. Avšak díky dalším jemným finesám, jako je například možnost interference stavů či existence provázaných stavů, se zdá, že kvantové stroje přece jen mají nad těmi klasickými navrch. Zjednodušeně lze říci, že díky zmíněným vlastnostem má kvantový stroj tu přednost, že všechny předložené paralelní cesty výpočtu skutečně **projde**, zatímco pravděpodobnostní si z nich jen **náhodně vybere jednu jedinou** a tou dojde až do koncového stavu.

Řešení úloh na QC

Většina studií o efektivitě výpočtů na kvantových počítačích (ve světě se pro ně začíná ujímat zkratka QC, *quantum computer,* u nás též KP) se dnes opírá o paradigma kvantového Turingova stroje, který je dobrou abstrakcí možností těchto počítačů. A podobně jako u klasických počítačů nevadí, že zatímco konstruktéři se pohybují v oblasti kvantových obvodů, teoretičtí analytici používají kvantové Turingovy stroje.

Na první pohled se zdá, že přiznání definitivní porážky klasických Turingových strojů jejich kvantovými následníky je na spadnutí. Nic podobného se však neděje, pokusme se proto alespoň zmapovat terén. Asi největším dobrodružstvím by bylo otevřít otázku kvantové versus klasické vypočitatelnosti. Na první pohled k tomu máme dobrý důvod: kvantový Turingův stroj dokáže – na rozdíl od klasického – vygenerovat **skutečně náhodné číslo**. Tato úloha se na klasických strojích považuje za nevypočitatelnou (připomeňme, že pravděpodobnostní stroj by něco takového sice dokázal, ale potřebuje k tomu dostat skutečně náhodné číslo již jako vstup).



Obr. 2. Základní uspořádání tříd složitosti

Otázkou ovšem je, co termín „skutečně náhodné číslo" formálně znamená. Dokud si to teorie řádně neujasní, nelze touto schopností kvantových počítačů dost pádně argumentovat. Jakmile se však do tohoto problému hlouběji ponoříme, zjistíme, že se chystáme otevřít nefalšovanou

Za kvantové počítače hovoří hlavně (předpokládané) činy. Pádné teoretické důkazy jejich nadvlády nad klasickými stroji však zatím nemáme.

Pandořinu skříňku. Cesta tímto směrem totiž může vést až za hranice vymezené Gödelovou větou o nerozhodnutelnosti, tedy tam, kde dnes končí formální věda a začíná takzvaná metavěda. Možnosti, které by se zde před námi otevřely, jsou v současné chvíli stejně fascinující jako nedostupné. Tuto oblast proto zatím přenecháme spisovatelům vědecko-fantastické literatury.

Bude to s dokazováním prvenství kvantových počítačů lepší alespoň v otázkách efektivity výpočtů? Bohužel, ani zde to není příliš slavné. V tabulce 2 jsou uvedeny hlavní třídy složitosti výpočtů pro kvantové Turingovy stroje, včetně jejich známých souvislostí s klasickými třídami složitosti. Snahou vědců je provést takzvanou *separaci,* tedy ukázat, že kvantové třídy složitosti zahrnují více problémů než ty klasické. Přitom dosud není dokázána ani separace množin P a QP (tedy že $P \neq QP$). Podařilo se však dokázat relativizovanou a podmíněnou podobu této separace ([2]), což dává jistou naději, že tato separace platí, avšak na konečný důkaz si ještě budeme muset počkat.

Pro kvantové počítače tak v současné době hovoří především jejich činy – známe úlohy, které jsou na nich zatím řešitelné efektivněji než na klasických počítačích. Slůvkem „efektivněji" zde nejčastěji vyjadřujeme fakt, že na kvantových počítačích existuje řešení náležející do polynomiální kategorie, zatímco na klasických strojích známe nejlépe subexponenciální řešení. Příkladem takové úlohy je právě faktorizace a s ní spojený Shorův faktorizační algoritmus – tomu se budeme podrobněji věnovat v celém příštím dílu. Půjde o pozornost zaslouženou – lze totiž bez nadsázky prohlásit, že právě díky Shorovu algoritmu se zvyšuje zájem o oblast kvantových počítačů. Nebýt tohoto algoritmu, bylo by asi jejich přijetí (vzhledem k táhnoucím se pokusům o separace) mnohem chladnější. Shorův algoritmus se tak nejspíš zapíše do dějin fyziky mnohem tučnějším písmem nežli do kryptologie.

Pro vědce hledající nové principiální možnosti práce počítačů vždy lepší, když zároveň s novým modelem přijdou také se znalostí konkrétního (a nejlépe zásadního) problému, který jejich konstrukce dokáže vyřešit efektivněji, měřeno řádem složitosti, nežli klasický stroj. Od takového přístupu pak lze očekávat, že vyburcuje všeobecnou pozornost. Právě touto cestou se vydala teorie kvantových počítačů.

Teoretičtí informatici možná úplnou porážku Turingova stroje nepřiznají ani v době, kdy už budou kvantové počítače rutinně luštit RSA...

Shrnutí

Představili jsme si základní aspekty teorie složitosti a ukázali jsme, jak se tato disciplína zvolna vyrovnává s možností využití počítačů pracujících na principech kvantové mechaniky. Snažili jsme se ukázat, že tato teorie je schopna akceptovat nové matematické modely fyzikálních procesů vhodných pro realizaci výpočetních postupů a že obsahuje také nástroje k vyhodnocení přínosu těchto modelů. Nástup kvantových počítačů tedy neznamená konec teorie složitosti, ale spíše její rozšíření. Bohužel však tato vědní disciplína postrádá (alespoň zatím) potřebnou dynamiku, takže na definitivní důkazy o přínosu nových modelů je třeba čekat, možná velmi, velmi dlouho...

V příštím pokračování už se pustíme do výkladu Shorova faktorizačního algoritmu a jistou pozornost věnujeme také Groverovu vyhledávacímu algoritmu.

■ ■ ■ Tomáš Rosa, *autor@chip.cz*

Literatura:

[1] Archiv vědeckých článků arXiv, *http://arxiv.org/*
[2] Berthiaume, A. and Brassard, G.: The Quantum Challenge to Structural Complexity Theory, Proc. of the 7th IEEE Conference on Structure in Complexity Theory, pp. 132-137, 1992
[3] Papadimitriou, CH.-H.: Computational Complexity, Addison-Wesley, 1994
[4] Shor, P. W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, extended article, 25 Jan 96, arXiv: quant-ph/9508027 v2
[5] Williams, C.-P. and Clearwater, S.-H.: Explorations in Quantum Computing, Springer-Verlag, 1998