**SVET KVANTOVEJ FYZIKY**
(seriál populárnych článkov o kvantovej fyzike uverejnených v časopise Quark v roku 2005)
Zdroj: http://www.quniverse.sk/ziman/

## I. Podivné pravdepodobnosti

*Viete, že na princípoch kvantovej teórie pracuje mnoho užitočných vecí, ako napríklad tranzistor, ktorý tvorí základ každého integrovaného obvodu, holografia či trojdimenzionálne kino? Viete, že kvantová fyzika nám pomohla vysvetliť žiarenie čierneho telesa, spektrálne čiary, supravodivosť, supratekutosť, stabilitu hmoty, periodickú tabuľku prvkov a iné? Ak nie, máte príležitosť vyplniť si túto medzeru v poznatkoch a aspoň sčasti odkryť svet, ktorý skúma kvantová teória. V ďalších častiach si ukážeme si nielen niektoré jeho podivné vlastnosti, ale aj ich potencionálne využitie.*

Na začiatok použijeme štandardnú frázu: kvantová fyzika je teória mikročastíc na úrovni atómov. Ide o svet, v ktorom zlyháva klasický popis, čo má za následok, že niektoré jej vlastnosti a dôsledky sú v príkrom rozpore s našou intuíciou. Tá je totiž do veľkej miery vybudovaná na pozorovaní vlastností makrosveta, avšak s mikrosvetom nemáme a zrejme ani nikdy nebudeme mať nejakú priamu skúsenosť.

Azda najdiskutovanejšou črtou kvantovej teórie je jej pravdepodobnostný charakter. Z bežnej praxe sme zvyknutí, že pravdepodobnosti sú iba dôsledkom istej našej „neschopnosti" a svet je v podstate deterministický. Vieme, že autobus nás z jednej zastávky na druhú odvezie za jednu minútu. Prípadný rozdiel v čase závisí od momentálnej dopravnej situácie. Ak by sme však vedeli polohu a rýchlosť všetkých áut na ceste, tak si vieme celú situáciu namodelovať a výsledný čas určíme presne. Situácia v kvantovom prípade je však úplne iná. Ak sme zaznamenali elektrón na mieste *A* a pýtame sa kedy ho spozorujeme na mieste *B*, tak nech robíme, čo robíme, výsledný čas nevieme predpovedať s určitosťou. Kvantová teória nám povie iba pravdepodobnosť zaznamenania elektrónu v nejakom čase v mieste *B*. **Dôležitý poznatok: kvantová fyzika predpovedá iba pravdepodobnosti jednotlivých udalostí**. A tie nie sú spôsobené našou neúplnou vedomosťou alebo našou lenivosťou určiť veci presne. Kvantové pravdepodobnosti sú principiálne.

### *AKO KRABICA S NÁLEPKAMI*

Pravdepodobnostný charakter má za následok, že nevieme zodpovedať také jednoduché otázky ako: **Aká je energia elektrónu? Aká je jeho poloha alebo hybnosť?** Aby sme boli presnejší, sú situácie keď niektoré z týchto otázok vieme zodpovedať, ale ide skôr o výnimky. Navyše, neexistuje situácia, keď by sme vedeli zodpovedať všetky takéto otázky súčasne. Inými slovami, objekty popísané kvantovou teóriou nemajú presne určené hodnoty energií, hybností, polôh, ... . V klasickej fyzike vieme každému objektu (či už ide o auto, loptu alebo planétu) priradiť jednoznačne hodnoty hocakých fyzikálnych veličín. Takýto objekt si potom môžeme predstaviť ako krabicu polepenú nálepkami s týmito hodnotami. V kvantovej fyzike však vieme objektom priradiť iba určité typy nálepiek. Niekedy vieme elektrónu prilepiť nálepku s hodnotou energie, inokedy s hodnotou polohy prípadne rýchlosti. Sú aj situácie, keď elektrón môže mať aj kombinácie alebo žiadnu zo spomínaných nálepiek. Nikdy však nemôže mať súčasne nálepky polohy aj rýchlosti. Tento fakt je iba iným vyjadrením nemožnosti presného určenia polohy a rýchlosti častice súčasne. Ak by sme to vedeli, tak nám nič nebráni nalepiť obe nálepky.

To, že elektrón nemá nálepku energie, ešte neznamená, že ju nemôžeme merať. Nikto nám v tom predsa nemôže zabrániť. V skutočnosti ani nie je iná možnosť, ako zistiť, či má alebo nemá danú nálepku,. Výsledkom merania je vo všeobecnosti **pravdepodobnostné rozdelenie** výsledkov. Z takéhoto rozdelenia sa spravidla zaujímame o dve čísla: **strednú hodnotu veličiny E** (v tomto prípade energie) a **strednú kvadratickú odchýlku ΔE**. Iba ak $\Delta E = 0$, tak objekt môže vlastniť nálepku energie s konkrétnou hodnotou *E*. Nulová odchýľka znamená, že výsledkom merania je vždy tá istá hodnota energie, a síce *E*. Kvantová teória dostala svoje meno preto, že na nálepkách zväčša nie sú ľubovoľné hodnoty. Príroda nám dáva k dispozícií iba niektoré zo všetkých možných hodnôt. Hovoríme, že **hodnoty fyzikálnych veličín sú kvantovan**é. V praxi to znamená, že napríklad elektrón v atóme vodíka môže mať na nálepke iba energie splňajúce vzťah $E_n = -\frac{13{,}6\,\mathrm{eV}}{n}$, kde $n = 1,2,3,...$

### *V AKOM SÚ STAVE*

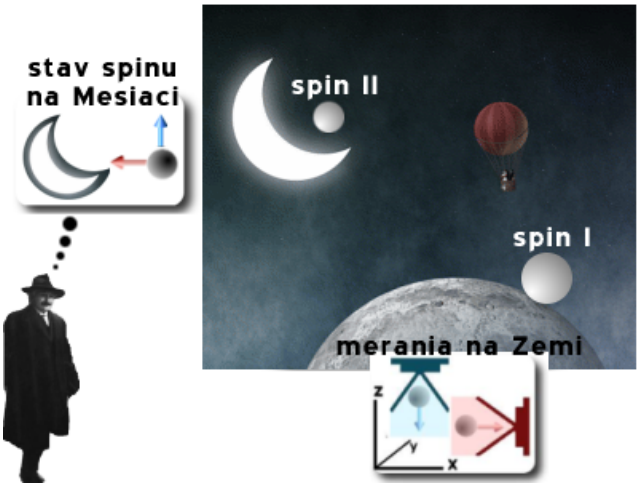
Na popísanie objektu v klasickom svete (makrosvete) nám niekedy stačí špecifikovať jeho polohu $\vec{r} = (x, y, z)$ v priestore a jeho rýchlosť $\vec{v}$. Všetky ostatné mechanické veličiny sú už iba funkciou týchto dvoch hodnôt. Napríklad energia je daná ako súčet kinetickej energie $E_k = mv^2/2$ a potenciálnej energie $E_p$, ktorá môže mať najrôznejší tvar v závislostí od síl pôsobiacich na popisovaný objekt. Klasickému objektu teda stačí nalepiť dve nálepky – polohu a rýchlosť, resp. hybnosť $\vec{p} = m\vec{v}$. Dvojicu vektorov $\vec{r}, \vec{p}$ nazývame stavom tohto klasického systému. Všeobecne môžeme povedať, že **fyzikálny stav je vlastne iba efektívne skomprimovaná informácia o systéme**. Ak poznáme stav objektu, tak hodnoty všetkých fyzikálnych veličín získame iba použitím tej správnej formuly. To však neplatí v kvantovej teórii, kde ako sme si povedali, nie všetky fyzikálne veličiny majú vždy „dobrý" zmysel. Poznanie stavu kvantového objektu nám umožňuje predpovedať iba pravdepodobnostné rozdelenia výsledkov merania, resp. stredné hodnoty. **Ako teda vlastne taký stav kvantového objektu vyzerá?**
Kvantový stav je o niečo abstraktnejší pojem ako stav klasického systému. Kvantový objekt totiž nemôžeme popísať nejakou sadou nálepiek zodpovedajúcich hodnotám fyzikálnych veličín. Nevieme zadať polohu a hybnosť súčasne, ale iba ich stredné hodnoty,

ktoré však na úplný popis stavu nestačia. Rovnako nám na určenie stavu nestačia ani pravdepodobnostné rozdelenia polôh a hybností skúmaného objektu. **Kvantová fyzika namiesto s pravdepodobnosťami narába s amplitúdami pravdepodobností**, t. j. s akýmisi odmocninami z normálnych pravdepodobností. K presnejšiemu popisu stavu sa ešte vrátime neskôr. Nateraz je dôležité si uvedomiť, že pojem stavu fyzikálneho systému má v kvantovej teórii podstatnú úlohu, oveľa dôležitejšiu než v prípade klasickom.

***SPIN 1/2***

Celkový moment hybnosti kvantových objektov (v porovnaní s klasickými) má akúsi zložku navyše. Ide o vnútorný moment hybnosti, ktorý nazývame *spin častice*. Jeho hodnota závisí od typu častice, napríklad elektróny a protóny majú spin 1/2, fotóny 1 atď. Vďaka tomu vlastnia kvantové objekty akýsi vnútorný rozmer, ktorý sa odzrkadľuje aj v popise stavu. Okrem priestorových vlastností musíme špecifikovať aj stav spinu danej častice. Niekedy sa však vieme obmedziť iba na štúdium vlastností spinu, a vtedy nepotrebujeme vedieť stav celého objektu, t. j. jeho hybnosť či energiu. Takýto popis je oveľa jednoduchší. Spin sám osebe nemá žiadnu polohu alebo hybnosť. Ide o čisto kvantovú charakteristiku objektu, ktorá nemá žiadnu klasickú obdobu. Zvyčajne si spin predstavujeme, ako akési vrtenie sa častice okolo svojej osi (podobne ako Zem), ale ide iba o analógiu a nič také sa v skutočnosti nedeje. Napriek tomu je to užitočná predstava. Stav spinu si môžeme predstaviť ako vektor (šípku), ktorý nám definuje smer tejto rotácie. To, čo vieme o spine zisťovať sú jeho priemety do jednotlivých smerov, t.j. meriame aká je hodnota spinu v každom možnom smere.

Spin ½ je ten najjednoduchší kvantový objekt, aký si vieme predstaviť. Prípadná nálepka hodnoty spinu ½ v hocakom smere má totižto iba dve rôzne hodnoty. Je v podstate na nás, ako si ich označíme. Budeme používať šípky (↑↓), čísla (±1), prípadne aj logické hodnoty (0,1). **Pre spin ½ platí, že vždy existuje iba jeden jediný smer**, v ktorom mu vieme priradiť nálepku s nejakou z týchto hodnôt. Potom vieme povedať: „toto je spin v tomto smere“. Túto vlastnosť využívame na označovanie stavov spinu. Stav spinu 1/2 v smere vektora $\vec{n}_{\theta,\varphi} = (\cos\theta\cos\varphi, \cos\theta\sin\varphi, \sin\theta)$ budeme označovať symbolom $\left|\vec{n}_{\theta,\varphi}\right\rangle$. Ide o symbol, ktorý reprezentuje akúsi “kvantovú nálepku” hovoriacu, že spin má hodnotu +1 v smere určenom vektorom $\vec{n}_{\theta,\varphi}$. Akákoľvek iná nálepka pre spin je zakázaná! Symboly $\left|\uparrow\right\rangle, \left|\downarrow\right\rangle$ budeme používať na označenie stavu spinu v smere a protismere osi *z*.




**Obr.1 Einstein-Podolsky-Rosen paradox.** *Dve častice so spinom ½ sa nachádzajú v špeciálnom stave, v ktorom je celkový spin nulový. Takúto dvojicu zvykneme nazývať EPR párom. Jedna z nich je na Mesiaci a druhá na Zemi. Výsledky merania spinu na Zemi nám okamžite hovoria, aký je stav spinu na Mesiaci. Táto vlastnosť je však v rozpore s predstavou lokálnosti a realizmu nášho popisu sveta. Na základe týchto požiadaviek prídeme k záveru, že spin na mesiaci je v stave, ktorý je v rozpore s kvantovou teóriou. Na obrázku má spin na Mesiaci určené hodnoty v dvoch smeroch (dve šípky), pričom kvantová teória povoľuje maximálne jeden smer.*

***SKRYTÉ PREMENNÉ A EPR PARADOX***

Nepozdávajú sa vám pravidlá kvantového sveta a jeho vlastnosti? Nie ste určite jediný a isté prekvapenie pri stretnutí s kvantovými pravidlami zažije zrejme každý. Skutočne sa to nedá popísať jednoduchšie? Neprehliadli sme niečo? Nie sú predsa len tie kvantové pravdepodobnosti dôsledkom našej skrytej nevedomosti? Možno sa iba pozeráme na mikrosvet cez tie nesprávne okuliare, a ak by sme si dali tie správne, tak pravdepodobnosti by zrazu zmizli a dostali by sme náš starý známy klasický svet. Podobné úvahy zrejme inšpirovali aj Alberta Einsteina, Borisa Podolského a Nathana Rosena, ktorí sformulovali tzv. *EPR paradox*. Autori argumentujú že kvantový popis stavu nie je úplný a existujú akési „skryté“ parametre, ktoré vôbec nemusíme byť schopní niekedy zistiť (sú skryté!), ale s ich pomocou by sa nám celý kvantový popis pretransformoval na klasický. Vedeli by sme presne povedať, aký výsledok bude mať každé jedno meranie a naše predpovede by už nemali iba pravdepodobnostný charakter. V tomto zmysle by bol náš popis pomocou skrytých parametrov úplný.

Einstein, Podolski a Rosen prišli k paradoxu pri analyzovaní tejto situácie. Predstavme si dva elektróny, ktoré tvoria spoločne systém s celkovým spinom nulovým. Jeden z týchto elektrónov pošlime na Mesiac a druhý si necháme u seba na Zemi. Ak na

našom elektróne zmeriame spinu v akomkoľvek smere, tak automaticky vieme aj hodnotu spinu druhého elektrónu v tom istom smere (celkový spin je nulový). Ak napríklad meriame v smere *z* a dostaneme výsledok ↑, tak si môžeme byť istý, že druhý elektrón má hodnotu ↓ v smere *z*, t. j. druhý elektrón sa nachádza v stave $|\downarrow\rangle$. Takýto výsledok však platí, nech si už meranie spinu na našom elektróne zvolíme v akomkoľvek smere. Elektrón na Mesiaci má presne opačný smer spinu, aký sme namerali my. A tu narážame na problém.

Trojica autorov vo svojom zdôvodňovaní vychádza z dvoch požiadaviek na akúkoľvek fyzikálnu teóriu: **lokálnosť** a **realizmus**. Lokálnosť odzrkadľuje fakt, že akékoľvek manipulácie s jedným systémom, nemôžu nijako ovplyvňovať vlastnosti iného priestorovo vzdialeného systému. Prinajmenšom druhý systém nemôže byť ovplyvnený okamžite. Realizmus sa týka vlastnosti, že v prípade, ak vieme s určitosťou povedať o nejakom systéme výsledok merania nejakej fyzikálnej veličiny, tak musí existovať niečo ako **„element reality“,** čo znamená, že daný systém má skutočne nálepku s hodnotou tohoto výsledku aj pred meraním. Obidve tieto požiadavky sú rozumné, avšak kvantová fyzika ich akýmsi spôsobom nespĺňa.

Vráťme sa k navrhnutému experimentu. Element reality je spojený s faktom, že vieme pred uskutočnením merania na elektróne na Mesiaci povedať ako dopadne. Ak zoberieme do úvahy aj lokálnosť, tak dostávame, že tento elektrón by sa mal v tomto stave nachádzať ešte pred uskutočnením nášho merania, pretože naše meranie nijako nemôže ovplyvniť elektrón na Mesiaci. A paradox nastáva, ak si uvedomíme, že náš výber smeru merania je ľubovoľný, avšak element reality (nálepka na druhom spine) závisí od tohto výberu. Odkiaľ však elektrón môže vedieť, aké meranie si zvolíme, t.j. ktorú nálepku si má nalepiť? Ak pripustíme, že by obe požiadavky mali byť splnené, tak nutne prídeme k záveru, že spin musí mať dopredu určené výsledky meraní do všetkých smerov, t.j. musí mať nálepky s hodnotami pre všetky smery. Takéto niečo je však v kvantovej teórii neprípustné, a teda kvantový popis stavu systému je neúplný a vedie ku konfliktu s lokálnosťou a realismom. Mala by teda existovať už spomínaná teória skrytých parametrov, ktorá by bola aj lokálna, a pritom by sa splnila aj požiadavka reality.

### *BELLOVE NEROVNOSTI*

Ako však overiť nejakú teóriu lokálne-reálnych skrytých parametrov? EPR paradox bol sformulovaný v roku 1934 a s riešením, respektíve s návrhom riešenia prišiel *John Bell* až v roku 1967. Myšlienka je pritom vcelku jednoduchá: skonštruovať nejakú matematickú formulu, ktorá musí byť splnená akoukoľvek lokálne-reálnou teóriou. Johnovi Bellovi sa podarilo skonštruovať jednoduchú nerovnosť obsahujúcu stredné hodnoty meraní, a teda táto nerovnosť sa dala experimentálna overiť. Čo je pekné na tomto prístupe je to, že samotné odvodenie nepredpokladá existenciu žiadnej fyzikálnej teórie. Umožňuje nám však overiť, či naša teória je v súlade s požiadavkami lokálnosti a realizmu, alebo nie. Dokonca nám umožňuje overiť priamo experimentom, či skúmané objekty môžu byť popísané nejakým modelom lokálne-reálnych skrytých parametrov, alebo nie. Ukazuje sa, že kvantová teória nie je kompaktibilná s týmito požiadavkami. Existujú diskusie o tom, či sa naruší lokálnosť,alebo realizmus. Odpoveď nie je jasná, ale napriek tomu sa zvykne hovoriť o **nelokálnosti kvantovej teórie**.

**Bellove nerovnosti**

Začnime pozorovaním, že pre štyri čísla $a, a', b, b'$ ktoré môžu mať iba hodnoty ±1 platí nasledovná identita $(a+a')b+(a-a')b'=\pm 2$ . Stačí si uvedomiť, že vždy práve jeden z výrazov $a+a'$ alebo $a-a'$ je nulový a ten druhý sa rovná ±2. Výber hodnôt ±1 priamo súvisí s výsledkami meraní spinu v rôznych smeroch. Merania v smeroch $\vec{a}, \vec{a}'$ sa robia na elektróne na Zemi, ale merania v smeroch $\vec{b}, \vec{b}'$ na Mesiaci. Označme $p(a,a',b,b')$ pravdepodobnosť výsledkov týchto meraní na oboch elektrónoch. Pre absolútnu hodnotu strednej hodnoty spomínanej identity potom platí nasledujúca nerovnosť

$$\left|\left\langle (\vec{a}+\vec{a}')\otimes\vec{b}+(\vec{a}-\vec{a}')\otimes\vec{b}'\right\rangle\right| = \left|\sum_{a,a',b,b'} p(a,a',b,b')\left[(a+a')b+(a-a')b'\right]\right|$$
$$\leq 2\sum_{a,a',b,b'} p(a,a',b,b') = 2$$

Použili sme symbol “⊗” na vyjadrenie toho, že ide o súčin dvoch meraní na dvoch elektrónoch a nie o súčin dvoch meraní na tom istom elektróne. Ľavú stranu tejto nerovnice vieme rozpísať pomocou stredných hodnôt jednoduchších meraní, čím dostávame nerovnosť

$$\left|\left\langle \vec{a}\otimes\vec{b}\right\rangle + \left\langle \vec{a}'\otimes\vec{b}\right\rangle + \left\langle \vec{a}\otimes\vec{b}'\right\rangle - \left\langle \vec{a}'\otimes\vec{b}'\right\rangle\right| \leq 2$$

Táto nerovnosť musí byť splnená ľubovoľnou lokálne-reálnou teóriou.

Teraz si ukážeme, že táto nerovnosť je skutočne narušená v našom experimente s dvoma elektrónmi. Ak používame elektróny nachádzajúce sa v stave s celkovým spinom nulovým, tak potom stredná hodnota súčinu meraní $\vec{a}$ na elektróne na Zemi a $\vec{b}$ na elektróne na Mesiaci je daná formulkou

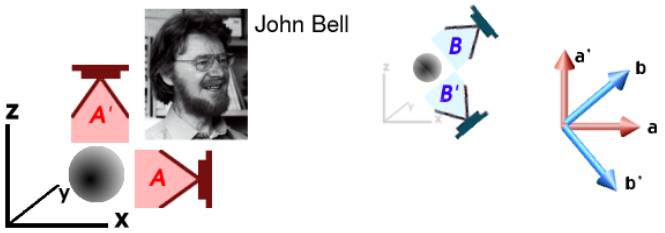
$$\left\langle \vec{a}\otimes\vec{b}\right\rangle = -\cos\omega_{ab} ,$$

kde $\omega_{ab}$ je uhol medzi vektormi $\vec{a}$ a $\vec{b}$ . Vhodným výberom smerov (viď Obr.2) merania $\omega_{ab}=\omega_{a'b}=\omega_{ab'}=45^\circ$ a $\omega_{a'b'}=135^\circ$ dokážeme uvedenú nerovnosť narušiť. Platí, že $\cos 45^\circ = -\cos 135^\circ = 1/\sqrt{2}$ a dosadením do nerovnosti dostávame

$$|-1/\sqrt{2}-1/\sqrt{2}-1/\sqrt{2}-1/\sqrt{2}| = 2\sqrt{2} \not\leq 2 .$$

Narušenie Bellových nerovností sa už overilo experimentálne vo viacerých nezávislých laboratóriách. Toto narušenie samo osebe neznamená platnosť kvantovej teórie, ale iba poukazuje na skutočnosť, že existujú systémy, ktoré nespĺňajú požiadavku lokálneho realizmu. Platnosť kvantovej teórie sa overuje samotnou veľkosťou narušenia, ktoré je v dobrej zhode s predpovedanou teoretickou

hodnotou. Existujú aj teórie, ktoré by mohli byť ešte nelokálnejšie ako kvantová fyzika, avšak otázkou zostáva, či tieto teórie popisujú aj nejaké skutočné fyzikálne systémy. Odpoveď na túto otázku však prinesie až budúcnosť.




**Obr.2 Bellove nerovnosti.** *Obrázok ukazuje ktoré merania (v ktorých smeroch) treba uskutočniť, aby Bellove nerovnosti boli narušené maximálne. Červená a modrá farba rozlišujú merania na prvej a druhej častici. Výsledkami všetkých meraní sú hodnoty plus, alebo mínus jeden.*

***BOHROVA ODPOVEĎ***

Zostáva nám odpovedať už iba na jednu otázku. Kde sme v odvodení Bellových nerovností sme urobili chybu, resp. ktorý krok nie je kompatibilný s kvantovou fyzikou? EPR paradox stimuloval jednu z najväčších vedeckých diskusií medzi *Albertom Einsteinom* a *Nielsom Bohrom*, ktorý sa pokladá za jedného z otcov kvantovej teórie. Výsledkom bola tzv. *Kodaňská interpretácia kvantovej teórie*. Bohrova obhajoba úplnosti kvantovej teórie sa, samozrejme, nezakladá na experimentoch narúšajúcich Bellove nerovnosti. V tom čase ešte tieto nerovnosti neboli na svete. Bohr argumentoval tvrdením, že podstata EPR paradoxu je vo vyjadrovaní sa o neuskutočnených experimentoch. Výber merania v smere osi *z* na Zemi skutočne znamená, že elektrón na Mesiaci bude mať nálepku obsahujúcu hodnotu tejto fyzikálnej veličiny. Avšak bez merania nevieme povedať s akou hodnotou. Výsledok merania na Zemi je úplne náhodný, a iba akt odčítania tohoto výsledku nás oprávňuje hovoriť o hodnote spinu druhého elektrónu. Bez toho nemá tvrdenie o nálepke žiadne opodstatnenie. Táto odpoveď, samozrejme, neznamená, žeby bola kvantová fyzika v súlade s podmienkami lokálneho realizmu. Skôr iba spochybňuje pojem elementu reality (po našom nálepky), ktorý existuje aj pred meraním. Kvantová teória sama osebe nevedie k EPR paradoxu, iba podmienky lokálnosti a realizmu sú v rozpore so štruktúrou kvantovej fyziky a na nich je postavený aj EPR argument o neúplnosti.

Nebudeme tu teraz hlbšie analyzovať postoje Alberta Einsteina a Nielsa Bohra, ktoré koniec koncov končia vo filozofickej rovine o tom, ako sa vlastne pozerať na svet. Ich vzájomná dišputa bola však nesmierne dôležitá, pretože naštartovala isté spriehladňovanie a snahu o hlbšie pochopenie kvantovej teórie. Zo súčasného pohľadu ponúka elegantné riešenie EPR paradoxu priamo experiment (najvyšší súd fyziky) skrz Bellove nerovnosti. A ako sme už spomenuli, experimentálna odpoveď dáva za pravdu kvantovej fyzike.

## II. Klonovanie, teleportácia a previazanie.

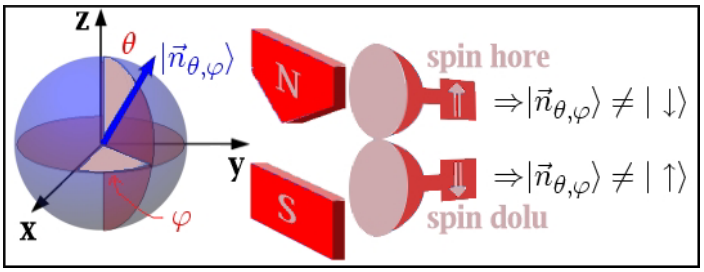
*V predošlej časti sme opísali zvláštny fenomén – kvantové stavy, vďaka ktorým celá kvantová fyzika dostala punc „nelokálnej teórie“. Tieto stavy sa ukazujú byť také dôležité, že dostali vlastné meno – previazané stavy (entangled states). Dnes si ukážeme niekoľko praktických ukážok, v ktorých tieto stavy majú hlavnú úlohu, poodhalíme závoj tajomnosti nad kvantovým klonovaním, možnosťou nadsvetelnej komunikácie a kvantovej teleportácie. Ešte jedno upozornenie: ak ste nečítali predchádzajúcu časť, bude vhodné ak to urobíte ešte pred tým, ako sa pustíte do tejto.*

V našom svete je kopírovanie úplne bežné a ani nás len nenapadne premýšľať, aké by to bolo keby sme kopírovať nemohli. Kopírovanie je aj veľmi dôležitý prostriedok našej výchovy a vzdelávania. V detstve preberáme niektoré návyky svojich najbližších, kopírujeme ich správanie, opakujeme po nich slová a vety. Aké by to bolo keby sme si stranu knihy nemohli odkopírovať, ako by fungovalo rozmnožovanie bez možnosti vytvárania replík DNA? Kvantová fyzika však napriek tomu kopírovanie zakazuje. Ak máme jediný kvantový objekt pre nás v neznámom stave, tak tento objekt nedokážeme naklonovať, namnožiť.

***KVANTOVÉ KLONOVANIE***

Aby sme pochopili kvantový zákaz klonovania, tak si musíme uvedomiť nasledovný fakt. Akékoľvek kopírovanie skrýva v sebe aj možnosť „čítania“, t.j. informáciu, ktorú kopírujeme, vždy aj poznáme, resp. máme možnosť ju spoznať. Kopírovací stroj najprv prečíta obsah papiera (pixel po pixeli) a potom vytlačí nové kópie. V kvantovej fyzike je situácia iná. Proces čítania informácie o stave je procesom merania. Meranie spinu ½ má iba dva možné výsledky, avšak počet možných stavov jedného spinu je oveľa väčší, dokonca nekonečný. Neexistuje meranie, ktorým by sme vedeli „prečítať“ úplnú informáciu o stave (ak máme iba jediný kvantový objekt). Opakovanie merania na našom spine nám tiež nepomôže. Meranie kvantového objektu totižto drasticky zmení pôvodný stav spinu a pôvodná informácia je navždy stratená. Ak chceme zistiť, o ktorý stav ide, tak potrebujeme oveľa viac spinov v tomto stave. Z jedného spinu informáciu o jeho stave nevieme prečítať, a teda ju nemôžeme vedieť ani skopírovať. Metóda „*premeraj a vyrob*“, ktorú používame pre klasické objekty, nám pri klonovaní jedinej repliky kvantového stavu veľmi nepomôže.

Je kopírovanie kvantových stavov skutočne nemožné? Stále by ešte mohla mať kvantová teória nástroj, ktorý by potrebu prečítania informácie obišiel. Situácia je však taká, že takýto nástroj neexistuje a kvantová fyzika skutočne zabraňuje kopírovaniu kvantových stavov. Kopírovanie v rámci kvantovej teórie je možné len v prípadoch, ak sa obmedzíme iba na istú podmnožinu stavov. Napríklad ak vieme, že spin je v jednom z dvoch stavov $|\uparrow\rangle, |\downarrow\rangle$, tak kopírovať vieme. Môžeme použiť metódu *premeraj a vyrob*, alebo aj procedúru pri ktorej meranie priamo nevystupuje. Ďalšou možnosťou je tzv. *aproximatívne kopírovanie*, ktoré namiesto dvoch presných kópií vytvára iba dve približné kópie. Niekedy sa môže hodiť aj takéto nedokonalé zariadenie a prísne vzaté aj pri klasickom kopírovaní je na mikroskopickej úrovni každá kópia iná. Ako najlepšie sme schopní kolnovať? Tejto otázke a možnostiam vytvárania približných kópií sa venoval aj slovenský fyzik *Vladimír Bužek* (*pozn. red.: ako prvý získal ocenenie Vedec roka SR, rozhovor s ním je v Quarku 7/1998*).




**Obr.1. Stavy spinu ½.** *Na obrázku je znázornená množina všetkých možných stavov jedného spinu ½. Každý bod na povrchu sféry zodpovedá inému kvantovému stavu* $|\vec{n}_{\theta,\varphi}\rangle$. *Vidno, že každý stav určuje smer (vektor) v trojrozmernom priestore, ktorý je definovaný dvojicou uhlov* $\theta,\varphi$. *Pravá časť obrázku zobrazuje merací prístroj, ktorý určuje hodnotu spinu v smere osi z. Po prechode medzi magnety je spin zaznamenaný v jednom z dvoch detektorov (dva výsledky merania). Horný detektor zaznamenáva zložku spinu v smere osi z a dolný detektor zaznamenáva zložku spinu v protismere osi z. Do ktorého z detektorov spin dopadne je proces úplne náhodný. Jednotlivé stavy sa odlišujú iba početnosťou (pravdepodobnosťou) koľkokrát je spin zaznamenaný v ktorom detektore. Tento rozdíl je však vidno iba pri viacnásobnom opakovaní experimentu, čo si ale vyžaduje veľké množstvo kópií toho istého stavu. My však máme spin iba jediný. V prípade ak horný z detektorov zaznamenal spin, tak určite vieme povedať, že pôvodný stav nebol spin dole v smere osi z. Nič viac o jeho pôvodnom stave povedať nevieme.*

**Množina stavov jediného spinu 1/2** je spojite nekonečná. Stavy sú reprezentované dvojicou uhlov $\theta,\varphi$, resp. smerom, a tvoria guľu (obr.1). Vďaka vlastnostiam kvantového merania z jediného spinu vieme získať iba dve hodnoty, ktoré nám veľa o uhloch $\theta,\varphi$ nepovedia. Konkrétny stav spinu zostáva prakticky rovnako záhadný ako bol pred uskutočnením merania. Paradoxne, jediné čo vieme povedať, je stav, v ktorom sa spin určite nenachádza. Spin meriame pomocou zariadení, ktoré zisťujú hodnotu spinu v určitom smere. Majú iba dva možné výsledky: spin hore (+1), alebo spin dolu (-1). Ak nameriame spin dolu, tak vieme, že spin sa nenachádzal v stave „spin hore“, a naopak. To znamená, že okrem tohoto stavu sa spin môže nachádzať v stave s ľubovoľnými hodnotami $\theta,\varphi$. Tento stav budeme označovať symbolicky ako $|\vec{n}_{\theta,\varphi}\rangle$.

***PRENOS NADSVETELNOU RÝCHLOSŤOU?***

Kvantové klonovanie síce nesúvisí priamo s nelokálnosťou kvantovej teórie, ale rôzne jeho aspekty áno. Predstavme si situáciu, že klonovanie je možné a my si z jedného spinu vieme naklonovať spinov koľko len chceme. Potom nám však nič nebráni prenášať informáciu rýchlosťou väčšou ako rýchlosť svetla. Využiť sa dá práve nelokálnosť kvantovej fyziky. Ako sme spomenuli v minulom čísle Quarku pri EPR (Einstein, Podolski a Rosen) paradoxe, po premeraní spinu na Zemi sa spin na Mesiaci nachádza v stave určenom výsledkom tohto merania. Pri meraní v smere *z* sa nachádza v jednom zo stavov $|\uparrow\rangle, |\downarrow\rangle$, avšak pri meraní v smere *x* je tento spin opísaný jedným zo stavov smerujúcich v smere, alebo protismere osi *x*. Tieto stavy budeme označovať nasledovne $|+\rangle, |-\rangle$. Voľba merania (smer *z* alebo smer *x*) je vecou experimentátora na Zemi. Ak chcem poslať odpoveď „áno“, tak zvolím meranie v smere osi *z*, a ak chcem poslať „nie“, tak premeriam v smere osi *x*. Experimentátor na Mesiaci má za úlohu zistiť aké meranie si experimentátor na Zemi zvolil, t. j. ktorý smer (*z* alebo *x*?). Potrebuje teda určiť, v ktorom zo štyroch možných stavov $|\uparrow\rangle, |\downarrow\rangle, |+\rangle, |-\rangle$ sa nachádza jeho spin. Ak sa mu to podarí, tak pozná odpoveď. Týmto spôsobom možno pomocou voľby smeru merania prenášať informáciu.

Rýchlosť prenosu je obmedzená iba rýchlosťou, s akou je experimentátor na Mesiaci schopný rozlíšiť tieto stavy, resp. smery. Kvantová fyzika však takúto možnosť nepovoľuje. Prípadná existencia merania, ktoré by nám povedalo, o ktorý zo stavov ide, by znamenala, že tento spin môže mať nálepku až so štyrmi hodnotami. Ako sme si už povedali v minulej časti, spin ½ môže mať najviac jednu nálepku s dvoma možnými hodnotami. Experimentátor by však mohol zvoliť prefíkanejšiu taktiku, a síce daný spin si naklonovať a poriadne premerať vo všetkých smeroch. Tým by získal úplnú informáciu o stave. Akokoľvek pomalý by bol tento proces, tak vždy by sme si vedeli predstaviť takú vzdialenosť medzi dvoma spinmi, že rýchlosť prenosu informácie by prevyšovala rýchlosť svetla. Namiesto na Mesiaci, byt sme experimentovali na Plute, prípadne ešte ďalej. Avšak ani klonovanie hoci len štyroch

konkrétnych stavov spinu nie je v kvantovej teórii prípustné. Nemožnosť kvantového klonovania teda „zachraňuje“ *kauzalitu udalostí*, ktorá by sa narušila nadsvetelnou rýchlosťou komunikácie.

Kvantové klonovanie, resp. jeho obmedzenie, má aj oveľa praktickejší dôsledok. Na tomto princípe je založená *kvantová kryptografia*, t. j. bezpečný prenos informácie medzi dvoma bodmi. Žiadny potencionálny špión si nemôže naklonovať posielanú informáciu. Akýkoľvek jeho pokus by bol okamžite zaznamenaný a jeho prítomnosť by bola odhalená. O kvantovej kryptografii si však povieme viac až v niektorej z ďalších častí.

***KVANTOVÁ TELEPORTÁCIA***

O kvantovej teleportácii sa už v Quarku neraz písalo. My neurobíme výnimku. Pri slove teleportácia sa okamžite aj tým, čo nesledujú seriál StarTrek, vybaví predstava extrémne rýchleho presunu hmoty na diaľku. Nadšencom science fiction sa od vzrušenia objavia zimomriavky, že konečne prišiel ten čas a neskutočné sa stáva realitou. Hneď na začiatku však musím všetkých sklamať. Pri kvantovej teleportácii nejde o žiadny okamžitý presun hmoty.

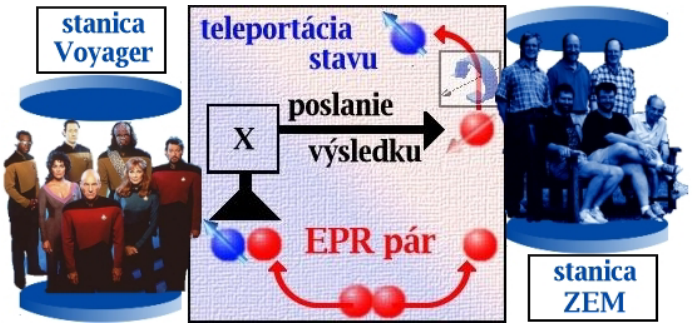
**Teleportácia.** Pozrime sa teraz bližšie na to, ako to celé funguje. V hre máme tri spiny 1/2. Dva z nich má experimentátor na Zemi a jeden sa nachádza na Plute. Spin na Plute spolu s jedným so spinov na Zemi je v špeciálnom stave a tvoria tzv. *EPR pár*. Zostávajúci spin na Zemi (ten, ktorý chceme teleportovať) je v neznámom stave určenom vektorom $\vec{n}_{\theta,\varphi}$, t.j. dvomi uhlami $\theta,\varphi$. Experimentátor na Zemi uskutočňuje *Bellovo meranie* na oboch svojich spinoch. Označme si jeho výsledky symbolmi *0,x,y,z*. Jeden z týchto symbolov ako výsledok posielame na Pluto, kde experimentátor uskutoční jednu zo štyroch transformácií *I,X,Y,Z* v závislosti od prijatej informácie. O aké transformácie vlastne ide? Uskutočnením Bellovho merania na spinoch na Zemi sa spin na Plute ocitne v jednom zo štyroch stavov v tejto tabuľke:

| | | |
|---|---|---|
| $\vec{m}_0$ | $\theta' = \theta, \varphi' = \varphi$ | Nulové otočenie |
| $\vec{m}_x$ | $\theta' = -\theta, \varphi' = -\varphi$ | *180°* otočenie okolo *x* |
| $\vec{m}_y$ | $\theta' = -\theta, \varphi' = \varphi + \pi$ | *180°* otočenie okolo *y* |
| $\vec{m}_z$ | $\theta' = \theta, \varphi' = \varphi + \pi$ | *180°* otočenie okolo *z* |

V poslednom stĺpci tabuľky je operácia, ktorú treba vykonať, aby sme dostali pôvodný stav daný uhlami $\theta,\varphi$. Opäť pripomíname, že nepotrebujeme vôbec poznať konkrétne hodnoty $\theta,\varphi$. Stačí nám vhodne (podľa tabuľky) spin na Plute pootočiť a teleportáciu máme úspešne za sebou. Pootočenie spinu sa v laboratóriu realizuje pomocou vhodne zvoleného magnetického poľa, ale nepôjdeme teraz do hlbších detailov. Ako vidieť, označenie výsledkov merania nebolo zvolené náhodou, ale indikuje, akú transformáciu treba na Plute vykonať, resp. okolo ktorej osi treba spin pootočiť.

Kvantová teleportácia napriek tomu rieši veľmi dôležitý problém. Predstavme si, že máme spin v nejakom stave (nevieme v akom) a chceme ho poslať na Pluto alebo ešte niekde ďalej. Ako to urobiť, čo najrýchlejšie, a najefektívnejšie? Priama metóda spočívajúca v jednoduchom poslaní nášho spinu nemusí uspieť. Kvantový stav spinu je veľmi krehký náklad, a bola by to vskutku veľká náhoda, ak by bol tento spin dopravený na Pluto (či už bežnou poštou alebo cez iné špecializované
doručovateľské firmy) nepoškodený. V prípade, ak máme viac kópií nášho spinu, tak je situácia o niečo jednoduchšia. Môžeme sa pokúsiť pomocou rôznych meraní stav spinu odhadnúť, t. j. zistiť hodnoty uhlov $\theta,\varphi$. Posielať obyčajnú informáciu (v tomto prípade dva uhly) o stave spinu je pomerne jednoduchá a bežná záležitosť. Príjemca na Plute si chvíľku počká a po prijatí správy si jednoducho posielaný stav pripraví vo svojom vlastnom laboratóriu. Jediný problém je množstvo kópií stavu, ktoré potrebujeme na zisteniu stavu. Je veľmi veľký – v princípe nekonečný a, nanešťastie kvantové stavy nevieme klonovať.

Kvantová fyzika nám v tomto prípade ponúka aj iné riešenie – *teleportáciu*. Bude nám stačiť iba jediná kópia spinového stavu, avšak budeme požadovať zdieľanie špeciálneho stavu dvoch ďalších spinov. Jeden zo spinov vlastní príjemca na Plute, a druhý vlastníme my. Tento špeciálny stav je presne ten istý stav použitý na narušenie Bellových nerovností, t. j. stav dvoch spinov s celkovým nulovým spinom. Pri Bellových nerovnostiach bol využitý ten fakt, že meranie na jednom spine nám okamžite prezrádza stav druhého spinu. Kvantová teleportácia využíva podobný princíp. Špeciálne meranie na našej strane nám povie, čo má príjemca na Plute vykonať, aby bol jeho spin popísaný stavom, ktorý sme chceli teleportovať.
Naše meranie je tzv. *Bellove meranie*, ktoré je uskutočnené na oboch spinoch, ku ktorým máme prístup, t.j. na spine, ktorého stav chceme poslať na Pluto, a na spine, ktorý patrí do EPR páru (t. j. stavu použitého pri EPR paradoxe). Toto meranie má štyri rôzne výsledky (meriame dva spiny súčasne) a každý z nich definuje iný stav spinu na Plute. Našťastie však vždy existuje transformácia, ktorá s úplnou presnosťou pretransformuje tento stav na stav, ktorý posielame. Dôležité je, že táto transformácia vôbec nezávisí na teleportovanom stave, t.j. tento stav nemusíme poznať. Po uskutočnení tejto opravnej operácie dosiahneme teleportovanie stavu z jedného spinu na druhý spin, ktorý je ľubovoľne ďaleko. Bolo by možno lepšie, a zrejme aj správnejšie, hovoriť o *teleportácii kvantového stavu*, než o kvantovej teleportácii.




**Obr.2. Teleportácia kvantového stavu.** *V ľavej časti obrázku sú postavy zo seriálu Star Trek, vďaka ktorým sa cestovanie pomocou teleportácie dostalo do širšieho povedomia. V pravej časti je skupina šieštich fyzikov (Charles Bennett, Gilles Brassard, Asher Perez, William Wootters, Richard Jozsa, Claude Crepeau), ktorá vymyslela kvantovú verziu teleportácie. V strede sa nachádza schematický obrázok teleportácie, ktorá je popísaná v texte a aj v rámčeku 2. V zakreslenom príklade bola v Bellovom meraní nameraná hodnota x, ktorá znamená, že druhý experimentátor vykoná rotáciu svojho spinu okolo osi x. Po tejto operácií je proces teleportácie ukončený.*

K uskutočneniu teleportácie je nutné poslať informáciu o výsledku merania na Pluto, aby tamojší experimentátor vedel presne, čo má so svojím spinom urobiť a zavŕšiť tak celý proces. Naša schopnosť posielania tejto informácie ohraničuje rýchlosť celej teleportácie. Teória relativity definuje ako hornú hranicu dosiahnuteľnej rýchlosti rýchlosť šírenia sa svetla vo vákuu, asi *300 000* km/s. Z tohto faktu vyplýva, že pri teleportácii kvantového stavu nielenže nejde o presun hmoty, ale ani rýchlosť nie je okamžitá.

Pozor na nasledovnú úvahu! Kvantová teleportácia prenáša stav jedného spinu na iný spin. Nakoniec teda máme dva spiny v tom istom stave. Ako je to však potom s nemožnosťou kvantového klonovania? Ubezpečujem vás, že všetko je v poriadku a k žiadnemu klonovaniu neprichádza. Finta je v tom, že pôvodný spin (ktorého stav teleportujeme) sa po teleportácii už viac v tomto stave nenachádza, a teda nemáme žiadne dve kópie toho istého stavu. Nezabúdajme, že na pôvodnom spine bolo uskutočnené meranie, ktoré stav tohoto spinu úplne zmenilo. Teleportácia kvantového stavu už bola zrealizovaná aj experimentálne v niekoľkých nezávislých pokusoch.

***KVANTOVÉ PREVIAZANIE***

*Kvantové previazanie* je špecifická vlastnosť stavov kvantových systémov, ktorá nám hovorí, že vlastnosti dvoch kvantových objektov, aj keď sú navzájom veľmi vzdialené, veľmi úzko spolu súvisia. Prvý, kto pomenoval tento jav, nebol nikto iný ako *Erwin Schrodinger*. Stalo sa to približne v tom istom čase, ako sa na svete objavil aj EPR paradox, ktorý poukázal na *nelokálnosť* kvantovej teórie. Pojmy nelokálnosti a kvantového previazania spolu súvisia, avšak neznamenajú úplne to isté (ako sa kedysi predpokladalo). Kvantové previazanie má svoju presnú matematickú definíciu a nelokálnosť je definovaná pomocou Bellových nerovností. V posledných rokoch sa vedcom podarilo zistiť, že nie všetky previazané stavy narúšajú Bellove nerovnosti, t. j. tieto dve definície neznamenajú úplne to isté.

Obe tieto vlastnosti (nelokálnosť a previazanie) sa prejavujú v experimentoch ako *neklasické vzťahy* medzi fyzikálnymi pozorovaniami, ktoré na prvý podhľad odporujú našim (klasickým) intuitívnym predstavám. Iba nedávno bolo odhalené, že kvantové previazanie je veľmi užitočný informatický zdroj, ktorý sa dá využiť v teórii informácie. Umožňuje rýchlejšie vyriešenie klasických problémov. Na tzv. *kvantových počítačoch* by sme boli schopní rýchlejšie rozložiť prirodzené čísla na prvočísla. Práve nemožnosť efektívneho vyriešenia tejto úlohy je základom niekoľkých kryptografických komunikačných protokolov, napr. internetom bežne používané RSA kódovanie by prestalo byť bezpečným spôsobom utajenia komunikácie. Na druhej strane je spôsob, ako kvantové previazanie využiť na úplne bezpečný prenos informácií. O kvantovom počítaní a kvantovej kryptografii si povieme viac v niektorej z nasledujúcich častí. V súčasnosti sa fenomén kvantového previazania skúma zo všetkých strán a stále zostáva ešte veľa nezodpovedaných otázok. Úplné pochopenie potenciálu kvantového previazania je výzvou, a riešenie nám možno umožní lepšie pochopiť zákonitosti kvantovej teórie samotnej.

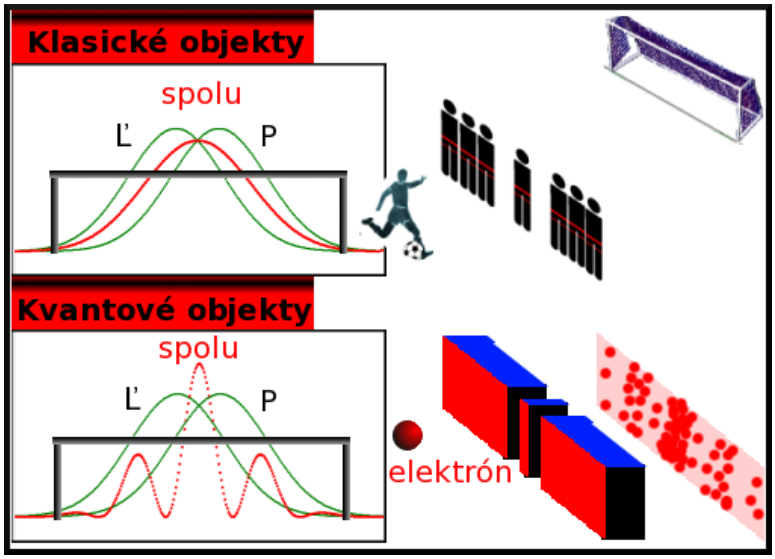
## III. Hranica medzi kvantovým a klasickým svetom

*Kvantová fyzika je veľmi úspešnou fyzikálnou teóriou, ktorú používame hlavne na popis mikrosveta. Prečo však aj na úrovni makrosveta, ktorý sme schopní priamo vnímať, nepozorujeme kvantové efekty? Akým spôsobom a prečo sa objekty prestávajú správať podľa kvantových zákonov? Kde je hranica medzi kvantovým a klasickým svetom? Existuje vôbec takáto hranica? V tejto časti si povieme, čím sa vlastne tieto dve teórie líšia.*

### Dvojštrbinový experiment

Ešte základnejšou črtou kvantovej teórie, ako kvantové previazanie, je *kvantová interferencia*, resp. *superpozícia kvantových stavov*. Teraz sa pokúsime tento čisto kvantový jav vysvetliť. Predstavme si futbalistu, ktorého úlohou je kopnúť loptu do brány a v ceste mu stojí múr postavený z hráčou súperovho tímu. Aktér tohoto priameho kopu je veľmi všímavý a postrehol, že jeden z hráčov chýba, t.j. v múre je úzka „trhlina“. Rozhodne sa využiť situáciu a loptu kopne cez túto dieru v múre. Kam takto kopnutá lopta

dopadne? Predstavte si, že ste na mieste brankára, ktorý si včas všimol prázdne miesto v múre. Kam by ste sa postavili? Prirodzene do stredu brány, resp. na miesto, kde pomyselná spojnica lopty a stredu trhliny pretína bránkovú čiaru. Skutočne, ak (ideálny) futbalista opakuje priamy kop z toho istého miesta viackrát, tak, použijúc práve popísanú stratégiu, najviackrát trafí práve do stredu bránky. *Pravdepodobnosť* je pre stred brány najväčšia.




**Obr. 1. Dvojštrbinový experiment.** *Na obrázku je znázornený dvojštrbinový experiment s klasickým telesom (futbalová lopta) a kvantovou časticou (elektrónom). Naľavo v obrázku je zobrazená pravdepodobnosť v oboch prípadoch (červená farba) a pre porovnanie sú zobrazené aj pravdepodobnosti v prípade, že jedna zo štrbín je uzavretá (zelená farba). Na spodnom grafe (v kvantovom prípade) vidno interferenčný obrazec.*

Teraz si situáciu skomplikujme. Povedzme, že múr má trhliny dve: jednu naľavo, a druhú napravo od stredu múru. Kam bude lopta kopnutá v takomto prípade? Ak tieto trhliny nie sú veľmi ďaleko od seba (napr. ich oddeluje iba jediný hráč), tak najpravdepodobnejšie bude lopta kopnutá opäť do stredu bránky. Ak však ľavú (pravú) trhlinu „zaplátame“ ďalším hráčom, tak lopta bude dopadať viac doľava (doprava). Funkcia $p_L(x)$ (resp. $p_R(x)$) označuje pravdepodobnosť toho, že lopta dopadne do miesta $x$ v bránke, keď ľavá (resp. pravá) trhlina je zaplátaná. O každej z dopadajúcich lôpt vieme samozrejme povedať, ktorou z trhlín prišla. Potom pravdepodobnosť dopadu lopty do miesta $x$ v bráne, ak obe trhliny sú odkryté, je rovná súčtu jednotlivých pravdepodobností, t.j. $p(x)=\frac{1}{2}\left(p_L(x)+p_R(x)\right)$. Faktor ½ vo vzťahu pre výslednú pravdepodobnosť znamená, že futbalista triafa loptu cez ľavú a cez pravú trhlinu rovnako často.

Zoberme teraz namiesto lopty elektróny (fotóny) vystrelované z elektrónového dela a namiesto hráčov tvoriacich múr uvažujme tienidlo s dvoma štrbinami. Hráčmi sú v tomto prípade atómy tvoriace tienidlo a štrbiny predstavujú miesta, kde títo atómoví futbalisti chýbajú. Ak zopakujeme ten istý experiment, tak spomínaný súčet jednotlivých pravdepodobností je v príkrom rozpore s experimentálnou realitou, ktorú pozorujeme v prírode, t.j. $p(x)\neq\frac{1}{2}\left(p_L(x)+p_R(x)\right)$. Namiesto toho pozorujeme tzv. *interferenčný obrazec*, ktorý pozostáva zo striedania pravdepodobnejších, a menej pravdepodobných oblastí dopadu elektrónu do „bránky“. Zhruba povedané „kvantová lopta“ dopadá veľmi pravdepodobne do stredu a na okraje bránky, ale pravdepodobnosť dopadnúť kúsok naľavo, alebo napravo od stredu je zanedbateľná. Z pohľadu brankára ide o nerozriešiteľnú dilemu kam sa postaviť, aby loptu chytil.

Naviac pri tomto experimente nemáme absolútne žiadnu vedomosť o tom, ktorou štrbinou k nám elektrón priletel. Klasicky to vieme určiť na základe určenia smeru rýchlosti, ktorá nám presne hovorí odkiaľ elektrón priletel. Avšak kvantový objekt (pozri prvú časť tejto série uverejnenej v *Quarku 2005/1*) nemôže mať súčasne aj „nálepku“ polohy ($x$), a aj „nálepku“ rýchlosti ($v$). Túto vlastnosť nazývame *Heisenbergovým princípom neurčitosti*. Vďaka nemu, alebo práve preto, nevieme o smere rýchlosti prilietajúcej kvantovej lopty povedať vôbec nič. Tým, že zaznamenáme jej aktuálnu polohu, úplne zničíme informáciu o jej pôvodnej rýchlosti. Preto aj štrbina, ktorou elektrón letel, zostáva neurčenou. Snažiť sa špecifikovať dráhu, ktorú kvantová lopta vykonala, kým dopadla do bránky, v kvantovej teórii všeobecne nemá veľký zmysel. Prichádzme k zaujímavému poznatku, že dráhu pohybu kvantových objektov nevieme sledovať.

Teraz si predstavme, že sa niekto predsa len snaží zistiť, ktorou štrbinou elektrón preletel. Napríklad môžeme štrbiny mierne osvetliť. Aký bude výsledok? Kupodivu v tomto prípade opäť dostaneme, že výsledné pravdepodobnostné rozdelenie je v zhode

s klasickým výrazom $p(x)=\frac{1}{2}\left(p_L(x)+p_R(x)\right)$. Ako tomu rozumieť? Čo spôsobuje, že elektrón (kvantový objekt) nám zrazu dá klasický výsledok? Odpoveďou je *kvantové meranie,* ktoré narozdiel od klasického, veľmi dramaticky mení stav celého kvantového objektu. Dá sa povedať, že kvantový objekt je veľmi citlivý na akúkoľvek našu snahu niečo o ňom zistiť. Každý náš nový poznatok je zaplatený úplnou zmenou stavu kvantového objektu a pôvodný stav je nenávratne preč.

Vždy keď zistíme, ktorou štrbinou elektrón preletel, tak na prítomnosť druhej štrbiny môžeme úplne zabudnúť. Vieme, že elektrón ju nepoužil. Inými slovami elektrón, ktorý nám dopadne do detektora, má známu minulosť. Všetky dopadnuvšie elektróny vieme potom zaradiť do dvoch skupín podľa toho, odkiaľ pochádzajú. Naviac pre tieto skupiny samostatne musí platiť, že pravdepodobnostné rozdelenie príslušných elektrónov je určené funkciamu $p_L(x)$ a $p_R(x)$. V polovici prípadov elektrón prešiel cez ľavú štrbinu a v polovici cez pravú. Výsledná pravdepodobnosť je preto súčtom týchto pravdepodobností, t.j. $p(x)=\frac{1}{2}\left(p_L(x)+p_R(x)\right)$. Ak nemáme informáciu o tom, cez ktorú štrbinu elektón preletel, tak nameriame úplne iné $p(x)$ a pravdepodobnosti $p_L(x)$, $p_R(x)$ vôbec nepoznáme. Aby sme ich poznali, museli by sme uskutočniť nové experimenty, v ktorých ponecháme pootvorenú iba jednu zo štrbín. A keďže porovnávame pravdepodobnosti získané v dvoch úplne odlišných meraniach, tak možno už nie je takým prekvapujúcim fakt, že $p(x)\neq\frac{1}{2}\left(p_L(x)+p_R(x)\right)$.

Dôležité je si uvedomiť, že v klasickom prípade (s futbalovou loptou) sú dva jednoštrbinové experimenty obsiahnuté v jedinom experimente s oboma štrbinami otvorenými. Naviac však zisťujeme, ktorou zo štrbín elektrón preletel. Klasický experiment, v ktorom sú otvorené obe štrbiny a nezisťujeme, ktorou štrbinou teleso letelo, je ekvivalentný experimentu, pri ktorom túto informáciu zisťujeme predtým, než teleso dopadlo do bránky. Je nám jedno, či informáciu o dráhe zisťujeme, alebo nie. V kvantovom prípade je však situácia odlišná. Kvantový dvojštrbinový experiment nemôžeme chápať ako zloženie dvoch jednoštrbinových. Takáto úvaha, ktorá nás automaticky vedie k tomu, že máme sčitovať jednotlivé pravdepodobnosti, je nesprávna. Argument je založený na našej skúsenosti hovoriacej, že teleso predsa muselo ísť iba jednou zo štrbín. Nič nás však neoprávňuje používať takúto skúsenosť aj pre kvantové objekty. Kvantová fyzika túto vlastnosť popiera a nevieme povedať, ktorú zo štrbín si elektrón vybral, resp. vyzerá to, akoby elektrón preletel cez obidve štrbiny súčasne.

Popísanému javu hovoríme *kvantová interferencia*. Pozor však na to, že táto interferencia nie je dôsledkom akejsi interakcie medzi elektrónmi, ktoré prechádzajú jednou, alebo druhou štrbinou. V našich experimentoch neuvažujeme o akomsi prúde elektrónov, ale vždy predpokladáme, že elektrón je v hre iba jeden jediný. Aby sme dostali pravdepodobnosti, tak experiment opakujeme viackrát, ale vždy iba s jedným elektrónom. Existencia *interferenčného obrazca* pre výslednú pravdepodobnosť $p(x)$ je prejavom tzv. *vlnových vlastností* častíc. Interferencia je vo fyzike dobre známy pojem, ktorý je charakteristický práve pre vlnenie (napr. vlny na vode, zvuk, svetlo, atď.). V nedávnej ankete o najkrajší fyzikálny experiment, ktorej výsledky boli zverejnené v *New York Times*, sa na prvom mieste umiestnil práve popísaný *dvojštrbinový experiment*.

**Princíp superpozície**

Pozorovanie interferenčného obrazca je jedným zo základných príznakov *kvantovosti* pozorovaného objektu. Interferencia je dôsledkom tzv. *princípu superpozície*, ktorý je jedným zo základných matematických pravidiel kvantového sveta. Je veľmi jednoducho sformulovateľný v reči matematiky a ako to už býva, len veľmi ťažko vysvetliteľný bez jej použitia. Dôležité je vedieť, že tento princíp stojí v pozadí všetkých odlišností kvantového popisu sveta od klasického. Ak pochopíte tejto základnej črte kvantovej teórie, tak ste na najlepšej ceste odkryť všetky ostatné tajomstvá kvantového sveta.

*Princíp superpozície* sa týka kvantových stavov. Ak vieme, že systém sa môže nachádzať v dvoch rôznych stavoch $|\psi\rangle,|\varphi\rangle$, tak princíp superpozície nám zaručuje aj existenciu stavov, ktoré sú *superpozíciou* týchto dvoch. Zapisujeme to ako súčet, napr. $a|\psi\rangle+b|\varphi\rangle$, kde *a,b* sú ľubovoľné, dokonca komplexné, čísla. V skutočnosti existuje isté obmedzenie na prípustné hodnoty *a,b*, ale pre nás a ani pre samotnú logiku superpozície nie je potrebné ho špecifikovať. Pripomíname, že symboly $|\psi\rangle,|\varphi\rangle$ označujú iba rôzne stavy kvantového systému a netreba za týmito symbolmi vidieť niečo komplikované. Ide iba o štandardne používané značky, pomenovania. Prehnane si môžeme predstaviť, že $|\psi\rangle,|\varphi\rangle$ sú symboly označujúce značku auta, napr. trabant a mercedes. Pre nás bude podstatné povedať si, aký je vťah superpozície týchto stavov $a|\psi\rangle+b|\varphi\rangle$ k samotným stavom $|\psi\rangle,|\varphi\rangle$. Zhruba povedané, samotné stavy sa prejavujú istými vlastnosťami (nálepkami). Ich superpozícia však už nemá žiadnu z týchto charakteristík úplne presne. V podstate má úplne inú nálepku, ktorú jej vieme priradiť. Ako príklad si uveďme dvojštrbinový experiment. Častice ktoré prejdú pravou štrbinou sa na tienidle nachádzajú v stave $\psi_R$, kdežto tie čo prešli ľavou štrbinou sú v stave $\psi_L$. Takáto je sitácia ak máme otvorenú iba jednu zo štrbín. Ak ponecháme otvorené obidve, tak prechádzajúca častica sa nachádza v superpozícii $\psi_R+\psi_L$, ktorá obsahuje informáciu o štrbine iba čiastočne, resp. nám povie, že častica si vyberala štrbiny s rovnakou pravdepodobnosťou. Nevieme však, ktorú si vybrala kedy.

**Superpozícia a štatistická zmes**

Označme si ako $p_\psi(x)$ pravdepodobnosť, že pri nejakom meraní *X* nameriame výsledok *x*, pričom meraný objekt je popísaný stavom $|\psi\rangle$. Podobne si nadefinujme pravdepodobnosť $p_\varphi(x)$. Pri tom istom meraní uskutočnenom na časticiach v superpozícii $a|\psi\rangle + b|\varphi\rangle$, je výsledná pravdepodobnosť daná nasledovne

$$p(x) = |a|^2\, p_\psi(x) + |b|^2\, p_\varphi(x) + I(x)$$

Posledný výraz v tejto rovnici *I(x)* je tzv. *interferenčný člen* a závisí od merania. Jeho hodnota môže byť aj kladná, aj záporná. Dokonca existujú merania, pre ktoré je táto hodnota nulová. V týchto prípadoch je potom výsledná pravdepodobnosť „klasická“, t.j. stav sa pre tieto merania javí ako *štatistická zmes* dvoch stavov $|\psi\rangle, |\varphi\rangle$ s váhami $|a|^2$ a $|b|^2$. Pre superpozíciu sú však zaujímavé tie prípady, keď je interferenčný člen nenulový a týchto je zdrvujúca väčšina. Interferenčný člen opäť nie je ľubovoľnou funkciou. Nebudeme sa však snažiť špecifikovať príslušné technické detaily, pretože ich nebudeme potrebovať a pre logiku veci nie sú podstatné.

*Štatistická zmes* dvoch stavov $|\psi\rangle, |\varphi\rangle$ je špeciálny stav, ktorý je výsledkom nasledovnej procedúry. Pre prípravu *N* častíc v zmesi zoberieme $Nq_1$ častíc v stave $|\psi\rangle$, $Nq_2$ častíc v stave $|\varphi\rangle$ a zamiešame ($q_1 + q_2 = 1$). Výsledky merania veličiny *X* pre takto pripravenú štatistickú zmes sú dané pravdepodobnosťami

$$p(x) = q_1 p_\psi(x) + q_2 p_\varphi(x)$$

Ak položíme $q_1 = |a|^2$ a $q_2 = |b|^2$, tak dostaneme pre výslednú pravdepodobnosť ten istý výraz, ako pri superpozícii s nulovým interferenčným členom. Rozdiel nastáva pri meraniach s nenulovým interferenčným členom. Štatistická zmes, narozdiel od superpozície, existuje aj v klasickej teórii.

Vieme ako vyrobiť štatistickú zmes, ale ako vlastne vyrobiť superpozíciu? Princíp superpozície nám nehovorí nič o tom, ako superpozičný stav vyrobiť. Hovorí iba o jeho existencii. Čo je to teda vlastne ten princíp superpozície? Ide o tvrdenie, ktoré hovorí o existencii istého štatistického vzťahu medzi kvantovými stavmi. Pravdepodobnosti, ktoré sú dôsledkom štatistickej zmesi, sú „klasické“. Ide o náhodnosť spôsobenú zmiešavaním, ktorá sa vyskytuje aj v klasickej fyzike. Avšak náhodnosť, ktorá je dôsledkom superpozície má úplne iný charakter, ktorý vedie k pozorovaniu interferenčných obrazcov pre výsledné pravdepodobnosti. Ďalšou otázkou môže byť, ktoré stavy sú „zakladné“, resp. ako nájsť stavy, ktorých superpozíciou sú všetky ostatné? Odpoveďou je, že žiadne takéto význačné stavy neexistujú. Každý jeden stav môžeme vybrať ako „základný“, a naopak, každý jeden stav je iba superpozíciou iných stavov. Aj to je jeden z dôvodov, prečo neexistuje jednoduchý návod ako superpozíciu vyrobiť. V istom zmysle je superpozícia zabudovaná v každom stave a iba čaká na svoje odhalenie. Otázka, ktorá sa dá zodpovedať je, či stav, ktorý mám, je alebo nie je superpozíciou nejakej danej množiny stavov. Odpovedať na túto otázku sa dá spôsobom, že nájdeme interferenčný člen *I(x)* ako jednoduchý rozdiel pravdepodobností, a potom overíme, či takto získaný výraz spĺňa všetky potrebné vlastnosti, alebo nie.

**Vzťahy neurčitosti.**

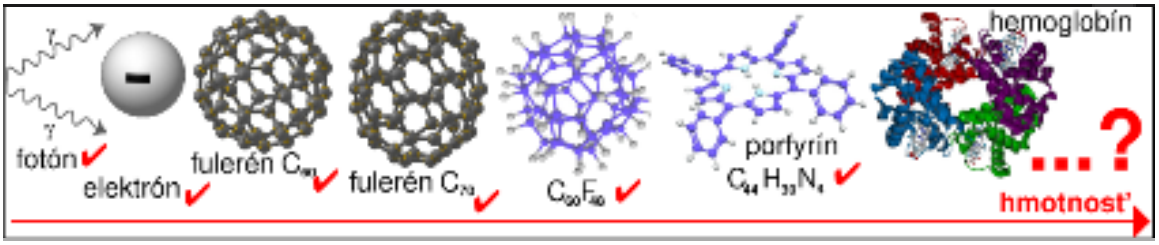
Už niekoľkokrát sme si spomenuli, že „obyvatelia“ kvantového sveta nemajú súčasne presne určenú svoju polohu a rýchlosť, resp. že niektoré fyzikálne veličiny sú nazvájom *nekompaktibilné*. Presné určenie polohy znamená úplnú *neurčitosť* o rýchlosti a naopak. Pri neurčitosti je náša vedomosť je vyjadrená nie jednou hodnotou, ale celým intervalom (štatisticky). Napríklad uvedieme hodnotu 10 plus/mínus 45, t.j. 10±45. Číslo 45 charakterizuje našu neurčitosť. Čím je väčšie, tým je aj naša neurčitosť vyššia, a naša znalosť o hodnote je menšia. Tento interval (10±45) nám ohraničuje možné hodnoty výsledkov pri meraní danej veličiny (napr. rýchlosti). Kvantová teória pomocou vzťahov neurčitosti spája neurčitosti, ktoré sa týkajú dvoch meraní. Napríklad neurčitosti pre polohu ($\sigma_x$) a pre rýchlosť ($\sigma_v$) sú zviazané tzv. Heisenbergovým vzťahom neurčitosti

$$\sigma_x \cdot \sigma_v \geq \hbar / m \quad ,$$

kde $\hbar$ = 1,054.10$^{-34}$ J s je *Planckova konštanta* (základná konštanta kvantového sveta) a *m* je hmotnosť častice. Teraz poľahky overíme naše predchádzajúc tvrdenie. Ak zmeriame polohu ideálne, t.j. $\sigma_x = 0$, tak neurčitosť pre rýchlosť musí byť nekonečná. Inak by uvedený vzťah neplatil, pretože nula vynásobená konečným číslom je stále nula, kdežto na pravej strane máme síce malú, ale stále nenulovú hodnotu. Preto hovoríme, že naša neurčitosť je v tomto prípade maximálna a o hodnote rýchlosti nám ani merania nepovedia nič konkrétnejšie. Pri reálnych experimentoch však nikdy polohu nezmeriame úplne presne a naše meranie je zaťažené istou neurčitosťou, t.j. $\sigma_x$ je vždy nenulové. Neurčitosť v rýchlosti ($\sigma_v$) je potom síce konečná, ale stále veľmi veľká.

Heisenbergov vzťah neurčitosti nám umožňuje povedať, nakoľko sa kvantová vlastnosť nekompaktibility prejavuje. Pre veľké hmotnosti je totižto pravá strana nerovnosti malá v porovnaní s mikroskopickými časticami. Napríklad pre elektrón $\hbar/m = 1{,}157.10^{-4}$ a pre 1kg teleso $\hbar/m = 1{,}054.10^{-34}$. Povedzme, že polohu a rýchlosť meriame s presnosťou na 10 desatinných miest, t.j. $\sigma_x \approx \sigma_v \approx 10^{-10}$. Pro zmeraní polohy s takouto presnosťou je v prípade elektrónu neurčitosť pre rýchlosť $\sigma_v \geq$ milión. Pre 1kg teleso (pri tej istej neurčitosti v meraní polohy) je podľa Heisenbergovho vzťahu neurčitosť pre rýchlosť $\sigma_v \geq 10^{-24}$, čo je oveľa menšie obmedzenie, ako je dané našim experimentálnym zariadením. V tomto prípade nie sme schopní vzťah neurčitosť overiť. Pre hmotnejšie telesá je obmedzenie dané vzťahom neurčitosti prakticky zanedbateľné, a preto efekty s ním spojené v klasickom svete nepozorujeme. V istom zmysle klasická fyzika je priblížením kvantovej fyziky. S narastajúcou hmotnosťou skúmaných objektov sú kvantové vlastnosti zanedbateľné a na klasickej úrovni sú všetky veličiny kompaktibilné.

**Ktorý kvantový objekt je najväčší?**
Kvantová fyzika je všeobecne chápaná ako teória popisujúca svet veľmi malých rozmerov – mikrosvet. Je zrejmé, že bežné objekty sa nesprávajú kvantovo. Napriek tomu všetky objekty sú zložené z molekúl, atómov, atď, t.j. práve z malých kvantových objektov. Čím to je, že zoskupovaním kvantových objektov sa kvantové vlastnosti akosi vytrácajú až nakoniec dostávame dokonale klasický svet? Kde je tá hranica, prípadne, ktorá vlastnosť ovlyvňuje „kvantovosť" najviac? Poznáme totižto aj výnimky. Existujú aj makroskopické systémy, ktoré vykazujú kvantové vlastnosti. Napríklad javy supravodivosti a supratekutosti sú makroskopické a kvantové súčasne. Sú fyzici, ktorí takúto hranicu takmer bez váhania napíšu a oddelia klasický svet od kvantového, ale sú aj takí, ktorí v žiadnu hranicu neveria.




**Obr.2. Kvantové vlastnosti molekúl.** *Na obrázku sú znázornené objekty, s ktorými bol uskutočnený dvojštrbinový experiment. Prvé experimenty boli tohoto typu boli uskutočnené ešte pred vznikom kvantovej teórie v oblasti optiky, kde bol jav interferencie veľmi dobre známy a prisudzoval sa vlnovej podstate svetla. V experimente s elektrónmi bolo po prvýkrát demonštrované, že aj častice (nielen vlny) sú schopné interferovať. V posledných rokoch boli uskutočnené interferenčné experimenty s molekulami fulerénu a porfyrínu, ktorý je momentálne najhmotnejším kvantovým objektom. Vedci v susednom Rakúsku majú za cieľ pokračovať v zvyšovaní hmotnosti kvantových objektov. Momentálne sa venujú molekulám hemoglobínu a malým vírusom.*

Podobný názor zdiela aj Anton Zeilinger zo susedného Rakúska, ktorého skupina (okrem iného) experimentálne testuje kvantovú interferenciu pre čoraz väčšie objekty. Vo svojich laboratóriách uskutočnili dvojštrbinový experiment s molekulami fulerénu $C_{60}$ (molekulové lopty) a $C_{70}$, fluórom obohateného fulerénu $C_{60}F_{48}$, a s biomolekulami porfyrínu (presnejšie meso-tetrafenylporfyrínu) $C_{44}H_{30}N_4$, ktoré sú napríklad súčasťou farebných centier chlorofylu. Ich ďalším cieľom je preukázať kvantové vlastnosti (interferenciu) enzýmov a vírusov, t.j. látok, ktoré možno ešte nepovažujeme za makroskopické, ale určite za klasické. Aspoň zatiaľ. Zaujímavou je aj otázka, či živé bunky majú kvantové vlastnosti, alebo nie. Otázka spojenia živých organizmov a kvantových vlastností je vzrušujúcou výzvou nielen pre fyzikov.

**K čomu je superpozícia dobrá?**
Hoci už od vzniku kvantovej teórie bol princíp superpozície akceptovaný ako jej základný princíp, jeho využitie pre praktické účely nebolo hlavným cieľom výskumu. Až v posledných rokoch s rozvojom tzv. kvantovej teórie informácie sa začal proces snahy o hlbšie pochopenie tohoto princípu. Celá mágia kvantového sveta je totižto ukrytá v tomto princípe a otázka prechodu z kvantového do klasického sveta je stále otvorená. Ukazuje sa, že práve z pohľadu informácie je princíp superpozície takmer prevratným javom, ktorý poskytuje riešenia pre niektoré úlohy a naviac, formuluje nové. V ďalších častiach si ukážeme ako princíp superpozície umožňuje vytvorenie kryptografického kľúča (kvantová kryptografia), pomáha rýchlejšie vyriešiť niektoré ťažké problémy (kvantové počítanie), a iné.

## IV. Kvantová kryptografia

*Snaha človeka skrývať svoje tajomstvá je tu od nepamäti. Je jedno, či ide o zlato, šperky, zbrane, alebo o tajné recepty, technológie, vynálezy, či myšlienky. Kryptografia sa venuje problémom, s ktorými sa stretne každý, kto sa pokúsi svoje tajomstvá prenášať z jedného miesta na iné, prípadne sa chce s nimi s niekým podeliť. V tejto časti si priblížime ako sa zákony kvantovej fyziky dajú využiť k zlepšeniu bezpečnosti komunikácie.*

Iba perfektné zvládnutie komunikácie medzi jednotlivými časťami královstiev, impérií, alebo armád pomáhalo králom a cisárom udržať a riadiť svoje krajiny po celé stáročia, vyhrávať dôležité vojny, predchádzať domácim aj vonkajším útokom. Všetci si pritom uvedomovali potenciálne nebezpečenstvo, keby sa tajné príkazy, alebo depeše, dostali do tých nesprávnych rúk. Snaha o zabezpečenie citlivých informácií motivovala a stále motivuje vypracovávanie najrôznejších techník, vytváranie špecializovaných tímov, ktorých úlohov je zaistiť bezpečnosť komunikácie. Súčasne s tým však vznikala a rozvíjala sa aj potreba odhaľovania tajných správ, ktorej prínos je zrejmý: vedieť o zámeroch nepriateľa a byť o krok pred ním. Kdesi na pozadí celej histórie je skrytý súboj medzi tými, čo tajné šifry vytvárajú, a tými, čo tieto šifry lúštia. Boli obdobia keď mali navrch jedny, ale aj obdobia, keď mali navrch druhí. Tento súboj možno badať aj dnes a z tohoto pohľadu sa dá povedať, že internet je jedným veľkým bojiskom.

História kryptografie (t.j. umenia skrývania, utajovania a následného odhaľovania informácie) je nemenej zaujímavá ako história samotná. Bohužiaľ tu nemáme priestor, čo i len veľmi povrchne naznačiť, čo všetko bolo priamo, či nepriamo spojené s kryptografiou. Jej úlohou je premeniť ľubovoľný text na zmes symbolov, ktoré na prvý pohľad nič neznamenajú. Tento proces sa nazýva *zakódovanie*. Šifra je akýsi predpis (recept), ktorý nám umožňuje správu zakódovať. Rozlišujeme dva základné prístupy k šifrovaniu správ: *prehodenie písmen* (permutácia) a *nahradenie písmen* (substitúcia) inými písmenami, prípadne úplne novými

symbolmi. Napríklad po zakódovaní jedného slova dostaneme RKUAQ (permutácia), alebo RVBSL (substitúcia). Viete uhádnuť pôvodné slovo? Nie je to zložité. Ide o slovo QUARK. V prvom prípade sme najprv slovo napísali odzadu a potom poprehadzovali dvojice písmen. V druhom prípade sme každé písmeno nahradili písmenom, ktoré stojí v abecede hneď za ním. Obidve tieto šifry je veľmi ľahké odhaliť. Typom šifry, ktorá nahrádza písmená novými znakmi, je napríklad *Morseova abeceda*. Namiesto písmen používa bodky a čiarky (krátke a dlhé signály). V tomto prípade však nie je cieľom správu utajiť, ale iba efektívne sprostredkovať, t.j. šifrovanie nie je vždy nutne motivované iba snahou informáciu utajiť.

Svätým grálom kryptografie sa stalo hladanie úplne bezpečnej šifry, t.j. takej, ktorú nikto a nikdy nebude vedieť rozlúštiť. Predtým ako si ju ukážeme, si povedzme niečo o tom, ako vlastne jednotlivé šifry odhaľovať, t.j. ako rozšifrovávať. Namiesto nahradenia písmenom, ktoré stojí v abecede posunuté o jedno miesto doprava, môžeme nahradiť písmenom, ktoré je posunuté o $N$ miest. Takýto spôsob kódovania sa nazýva *Cézarova šifra* podľa rímskeho cisára, ktorý ju používal pri riadení svojich légií. Kľúčom k dešifrovaniu je nájsť, ktorý symbol, čo znamená, t.j. odhaliť, že B je namiesto A, C je namiesto B, atď. Ako však zistiť veľkosť posunutia? Môžeme skúsiť všetky možnosti posunutí, ktorých nie je až tak veľa. Ale, čo v prípade ak je abeceda usporiadaná nejakým neznámym spôsobom? Takýto prípad nemôžeme vylúčiť. Skúšať všetky možnosti v takomto prípade by už zabralo veľmi dlhý čas.

Existuje však aj iný spôsob. Pre slovenčinu (podobne aj pre iné jazyky) platí, že jednotlivé písmena sa v bežných textoch nevyskytujú rovnako často. Napríklad v tomto texte bolo písmeno A použité zhruba 1800 krát, kdežto písmeno G ani nie 10 krát. Vieme povedať, ktoré písmeno používame v ktorom jazyku najviac, a ktoré najmenej. Ak teda máme dostatočne dlhý zašifrovaný slovenský text, tak symbol, ktorý sa najviackrát opakuje, bude s veľkou pravdepodobnosťou nahradzovať písmeno A, alebo E. Takto môžeme odhadnúť niekoľko písmen a zvyšok poväčšine poľahky doplníme. Niekedy je potrebné si všímať aj dvojice, trojice, atď. Vieme napríklad, že písmená JG vedľa seba nebývajú. Využitie všetkých takýchto štatistických znalostí o používaní písmen v našom jazyku nám umožní nakoniec šifru pomerne veľmi rýchlo odhaliť. Cézarova šifra teda nie je úplne vhodná na posielanie utajených správ.

**Vernamova šifra.**

Úplne bezpečnú šifru dostaneme, ak iba trochu skomplikujeme šifru Cézarovu. Namiesto toho, aby sme posunutie zafixovali pre celú správu, prípadne pre nejaké bloky písmen zo správy, tak nadefinujeme iný (náhodný) posun pre každé jedno písmeno správy. Tieto posuny sú špecifikované tzv. *šifrovacím kľúčom*, ktorým správu akoby uzamkneme. Vďaka takémuto postupu dosiahneme to, že každý symbol sa nám v zašifrovanom texte vyskytuje zhruba rovnako často. Preto popísaný spôsob lúštenia šifry fungovať nebude. Výsledná správa je úplne náhodným zoskupením znakov, ktoré bez znalosti jednotlivých posunutí neobsahujú vôbec žiadnu informáciu (pozri obrázok 1). Tento spôsob šifrovania nazývame *Vernamova šifra*, ktorá je jedinou úplne bezpečnou šifrou. Jej drobnou nevýhodou je, že na používanie je trochu náročná. V prvom rade odosielateľ a aj adresát musia poznať dopredu hodnoty jednotlivých posunutí t.j. pred tým než začnú komunikovať, obidvaja poznajú šifrovací kľúč. Pri dekódovaní treba jednotlivé písmená podľa toho istého kľúča poposúvať späť, t.j. tentokrát v abecede doľava. Aby sme dosiahli úplnú bezpečnosť, tak dĺžka šifrovacieho kľúča musí byť rovnako dlhá ako dĺžka celého zakódovaného textu. Naviac kľúč nemôžeme používať opakovane. Existujú totiž spôsoby ako v takomto prípade šifru odhaliť.

Proces bezpečnej komunikácie si môžeme predstaviť nasledovne. Šifrovanie nie je ničím iným ako ukladaním správ do pevnej krabice, ktorú zatvoríme a zámok uzamkneme kľúčom. Bezpečnosť znamená, že krabica, a aj zámok, sú neotvoriteľné nech použijeme akékoľvek prostriedky. Ani kladivom, ani pílkou sa do krabice nedostaneme. Jediným spôsobom ako zistiť obsah krabice, je použiť kľúč a zámku odomknúť. Bohužiaľ, žiadnu úplne odolnú krabicu nemáme a nepoznáme. V skutočnosti ju ani nepotrebujeme, pretože našim cieľom nie je ukryť niečo hmatateľné (papier), ale niečo viac abstraktné, t.j. informáciu zapísanú na papieri. Idea šifrovania je taká, že žiadna sila nám nepomôže dostať sa k obsahu. Práve naopak, použitie hrubej sily nie je vôbec potrebné. Zašifrovaná správa nemusí byť skrytá v krabici a každý si ju môže pozrieť. Avšak iba ten, kto má „kľúč“ môže skrytý obsah aj otvoriť a text odkódovať.

Pozrime sa teraz detailne na to ako Vernamova šifra funguje v prípade, že abeceda je zložená iba z dvoch „písmen“ 0,1. Hocijaký skutočný text vieme zapísať ako postupnosť núl a jednotiek. Nebudeme sa teraz zaujímať o nejakú konkrétnu správu a našou úlohou bude zašifrovať text 0011001100110011, nech už znamená čokoľvek. Na posunutia v takejto dvojprvkovej abecede nemáme veľa možností: alebo neposúvame písmená vôbec, alebo namiesto nuly píšeme jednotku a naopak. Suma sumárum máme k dispozícii dve rôzne Cézarove šifry: posunutie o $N$=0 a posunutie o $N$=1. Vernamova šifra (kľúč) je opäť iba postupnosťou núl a jednotiek, ktoré špecifikujú posunutie daného písmena v pôvodnej správe, napr. 0010111010111000. Výsledkom šifrovanie bude postupnosť 0001110110001011. Táto správa príde k adresátovi, ktorý použije ten istý kľúč na dešifrovanie, t.j. v prípade $N$=0 písmeno ponechá bez zmeny a v prípade $N$=1 písmeno nahradí jedným písmenom naľavo, t.j. nulu nahradí jednotkou a naopak. V tomto prípade je šifrovanie (posunutie doprava) a dešifrovanie (posunutie doľava) tou istou operáciou. Overte si, že ak použijete ten istý kľúč na zašifrovaný text, tak dostanete pôvodnú postupnosť núl a jednotiek.

**Vernamova šifra z pohľadu fyzika**

Na poslanie hodnoty bitu informácie z jedného miesta na druhé bezpochyby potrebujeme nejaký fyzikálny objekt, ktorý hrá úlohu kuriéra (nosiča) informácie. Informácia samotná je zakódovaná práve do stavu tohoto fyzikálneho objektu. Položme si otázku, či je nejaký rozdiel ak informácia je zapísaná na kuse papiera, uložená v elektronickom čipe, alebo zakódovaná do jediného elektrónu.

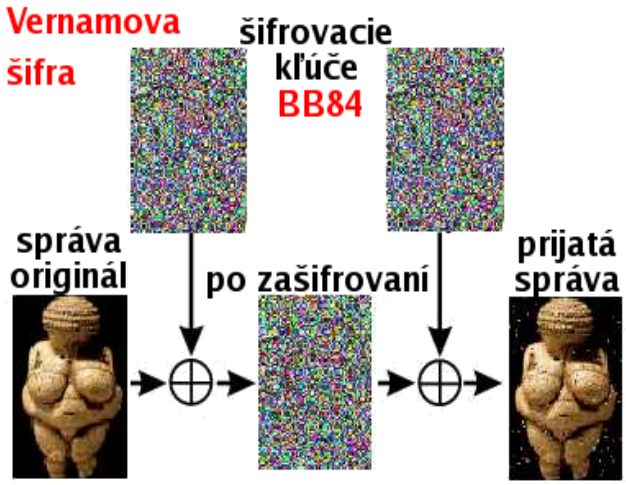
V prípade, že používame dvojprvkovú abecedu, tak kuriéra nazývame *klasickým bitom*. Ide o ľubovoľný fyzikálny systém, ktorý sa nachádza v dvoch rôznych stavoch, ktoré si pomenujeme ako stav 0 a stav 1. K uskutočneniu Vernamovej šifry potrebujeme aspoň dva klasické bity, ktoré pripadajú na prenos jedného bitu informácie, t.j. písmena 0, alebo 1. Prvým krokom Vernamovej šifry je *distribúcia kľúča*. V tomto kroku odosielateľ a aj adresát obdržia každý po *K* klasických bitoch, pričom *x*-tý bit oboch je vždy v rovnakom stave (pre každé *x*). Poslanie správy budeme vykonávať pomocou fyzikálnej transformácie uskutočnenej na klasických bitoch tvoriacich kľúč. Ak chceme poslať nulu, tak nevykonáme žiadnu operáciu a stav klasického bitu necháme nezmenený. Ak však posielame jednotku, tak stav klasického bitu zmeníme. Táto operácia spôsobuje, že hodnota klasického bitu sa zmení na opačnú (z nuly na jednotku a naopak), čo zodpovedá logickej operácii negácie. Hovoríme, že aplikujeme operáciu NOT. Po vykonaní príslušnej operácie pošleme klasický bit adresátovi. Dešifrovanie uskutočníme porovnaním stavov, resp. hodnôt, oboch klasických bitov. V prípade, ak sú stavy rovnaké, tak odosielateľ nevykonal žiadnu operáciu a posiela nám písmeno 0, kdežto ak sú rôzne, tak odosielateľ vykonal operáciu NOT, čím poslal písmeno 1. Treba si dobre rozmyslieť, že popísaný spôsob komunikácie je presne to isté ako Vernamova šifra popísaná v predošlom odstavci, t.j. správa je zašifrovaná tým istým spôsobom.

Aby sme zabezpečili bezpečnosť prenosu, tak distribuovaný kľúč musí byť úplne náhodný, t.j. nesmú sa v ňom opakovať nejaké reťazce núl a jednotiek. Napríklad kľúčom 00010001000100010001 nie je príliš bezpečné uzamykať. V podstate ide o opakované použitie tej istej Vernamovej šifry 0001 pre správy s dĺžkou 4 bity. V ideálnom prípade sa nuly a jednotky vyskytujú v šifrovacom kľúči rovnako často. Z pohľadu fyziky to znamená, že odosielateľ a adresát zdieľajú dva klasické bity, ktoré sa nachádzajú v tzv. *maximálne korelovanom stave*.

**Superhusté kódovanie – dva v jednom**

Pri prenesení jedného klasického bitu prenesieme jeden bit informácie. Je to však maximum, čo môžeme dosiahnuť? Všeobecne platí, že do jediného klasického bitu vieme zakódovať maximálne jeden bit informácie. Pri Vernamovej šifre však máme v hre spolu až dva klasické bity, ktoré potencionálne môžu obsahovať až dva bity informácie. Vieme ich plne využiť? Bohužiaľ nie, pretože na jednom klasickom bite nevieme vykonať viac ako dve rôzne operácie (nerobiť nič, alebo NOT), t.j. poslať vieme najviac dve hodnoty, ktoré predstavujú jeden bit informácie.

Predstavme si však situáciu, že namiesto klasických bitov používame bity kvantové. Z jedného kvantového bitu vieme takisto získať najviac jeden bit informácie. Z tohoto pohľadu sa klasické a kvantové bity vôbec nelíšia. V kvantovom prípade však odosielateľ môže vykonať oveľa viac operácii ako v prípade klasickom, kde máme transformácie iba dve. Inými slovami, v kvantovom prípade sa môžeme pokúsiť odoslať viac písmen a použiť tak viacpísmenovú abecedu. V prípade, ak odosielateľ a adresát zdieľajú *maximálne previazaný stav* (napr. stav s nulovým celkovým spinom), tak vieme vykonať štyri také operácie, že celkové stavy oboch kvantových bitov budú navzájom perfektne rozlíšiteľné. Jediným meraním potom vieme zistiť o ktorý z týchto štyroch stavov ide. Meranie je nám už známe Bellove meranie, ktoré bolo napríklad použité aj pri teleportácii (pozri Quark 2005/2). Adresát po prijatí kvantového bitu bude teda schopný jednoznačne určiť iba jediným meraním, ktorú zo štyroch operácií si odosielateľ zvolil, t.j. ktoré písmeno (jedno zo štyroch) poslal. Štyri písmená zodpovedajú dvom bitom prenesenej informácie. V kvantovom prípade teda dokážeme potenciál dvoch kvantových bitov využiť naplno a preniesť dva bity informácie pri poslaní jediného kvantového bitu (dva v jednom). Samozrejme poslaný kvantový bit môže niesť najviac jeden bit informácie. Inak by sme si odporovali s tým, čo sme už povedali predtým. V tomto prípade ale paradoxne kuriér nenesie vôbec žiadny bit informácie. Hocikto, kto zachytí poslanú časticu nezíska žiadnu informáciu. Druhý kvantový bit slúži na odomknutie správy. Celá informácia je skrytá v počiatočných koreláciach medzi kvantovými (ak klasickými) bitmi. Ako však vieme korelácie (pozri Quark 2005/1,2) kvantových systémov sú silnejšie a divnejšie ako systémov klasických. Kvantový analóg Vernamovej šifry je príkladom tejto sily kvantových korelácií, ktoré zdvojnásobujú prenosovú kapacitu. Kvantovej verzii sa zvykne hovoriť *superhusté kódovanie*.




**Obr. 1.** *Na obrázku je znázornená ideaVernamovej šifry. Išlo o skutočný experiment, v ktorom bol pomocou kvantovej fyziky rozdistribuovaný šifrovací kľúč a následne bola prenesená fotografia sošky Venuše. Kľúč je definovaný farbou pixela, ktorá definuje „posunutie“ v abecede farieb. Ako vidno chybovosť prenosu bola veľmi malá.*

**Kvantová distribúcia kľúča**

Vernamova šifra je založená na existencii šifrovacieho kľúča, ktorý je známy iba odosielateľovi a adresátovi. Ako však zabezpečiť existenciu takéhoto kľúča? Kľúč nemôže byť jednoducho poslaný z jedného miesta na druhé. Každý by ho mohol prečítať. Na druhej strane zašifrovať ho nie je možné, lebo k zašifrovaniu potrebujeme kľúč, ktorý ešte nemáme. Distribúcia kľúča je najvážnejším problémom a nedostatkom Vernamovej šifry. Dokonca takým vážnym, že Vernamova šifra sa prakticky nepoužíva. Bezpečná distribúcia je klasicky neriešiteľný problém. Kvantová fyzika však ponúka riešenie aj v tejto oblasti. Bude nám stačiť posielať jediný kvantový bit a žiaden iný okrem tohoto nebudeme potrebovať.

V roku 1984 Charles Bennett a Gill Brassard navrhli kvantový protokol určený na distribúciu kľúča, ktorý dnes označujeme ako BB84. Pre lepšiu predstavu si tento protokol popíšeme na konkrétnom príklade. *Polarizácia fotónu* je (podobne ako spin 1/2) vhodným kandidátom na realizáciu kvantového bitu. Zhruba povedané, polarizácia predstavuje akýsi smer priradený každému fotónu, smer v ktorom kmitá „jeho“ elektrické pole. Perfektne rozlíšiť sa dá iba medzi tými dvoma smermi polarizácie, ktoré zvierajú pravý uhol, napríklad medzi *horizontálne* a *vertikálne* polarizovaným fotónom. K tomuto slúžia zariadenia zvané polarizátory, ktoré majú tú vlastnosť, že fotóny s istou polarizáciou neprepúšťajú vôbec. Naviac fotóny, ktorým sa podarí prejsť, sa vždy nachádzajú v smere kolmom na tento smer. Hovoríme, že svetlo (tvorené fotónmi) je po prechode polarizátorom polarizované v istom smere. Pre polarizáciu platí princíp neurčitosti, ktorý zaručuje bezpečnosť prenosu kľúča. O fotóne vieme zistiť hodnotu polarizácie iba v jedinom smere, t.j. nevieme súčasne presne zmerať veľkosť polarizácie v dvoch rôznych (nekolmých) smeroch.

**BB84**

Budeme potrebovať fotóny v štyroch rôznych stavoch: horizontálne polarizované $|H\rangle$ (t.j. pod uhlom 0 stupňov), vertikálne polarizované $|V\rangle$ (t.j. pod uhlom 90 stupňov), diagonálne polarizované pod uhlom 45 stupňov $|+\rangle$ a diagonálne polarizované pod uhlom 135 stupňov $|-\rangle$. Tieto stavy predstavujú dvojice navzájom kolmých polarizácií, t.j. dve bázy H/V a +/–. Odosielateľ určuje hodnotu bitu výberom stavu: hodnotu 1, ak vyberie $|H\rangle$, alebo $|+\rangle$, a hodnotu 0, ak vyberie stavy $|V\rangle$, alebo $|-\rangle$. Výbery stavov a aj báz robíme pre každý bit úplne náhodne. Úlohou adresáta je určiť, ktorý stav sme si vybrali. Kvôli princípu neurčitosti neexistuje meranie, ktorým by sme to vedeli určiť. Adresát preto strieda náhodne dve rôzne merania a zisťuje hodnoty polarizácie v dvoch rôznych bázach H/V, alebo +/–. Používa polarizátor v smere H, alebo polarizátor v smere +. Má dve možnosti: alebo tipne bázu správne, alebo nie. Správne tipnutie bázy znamená výber polarizátora H ak bol poslaný stav $|H\rangle$ (ako bit 1), alebo stav $|V\rangle$ (ako bit 0). Podobne pre výber polarizátora v smere +. Ak správne tipne adresát bázu, tak vie určiť ktorý bit bol poslaný. Ak fotón polarizátorom neprejde, tak poslaný bit má hodnotu 0, a ak fotón prejde, tak bol poslaný bit 1. V prípade, ak sa voľba polarizátora nezhoduje s výberom bázy odosielateľa, tak adresát nevie povedať o hodnote poslaného bitu informácie vôbec nič. V takomto prípade je šanca fotónu prejsť a nepresť polarizátorom jedna k jednej. Preto, ani keď fotón prejde a ani keď neprejde, nevieme povedať o fotón v akom stave išlo.

Zistili sme, že bit informácie sa nám podarí preniesť vždy, keď sa voľba polarizátora zhoduje s voľbou bázy. Bohužiaľ adresát nevie, či zvolil to správn nastavenie polarizátora, alebo nie. Riešenie je našťastie jednoduché. Odosielateľ zverejní, ktorú bázu kedy vybral a adresát zverejní, v ktorom smere polarizáciu meral. Napríklad si zatelefonujú a budú vedieť kedy sa zhodli a kedy nie. Vďaka tomu oddelia plevel od zrna a vyhodia tie výsledky, kedy sa nezhodli. Zvyšné hodnoty bitov sú potom presne také isté, t.j. majú k dispozícii ten istý kľúč, ktorý môžu použiť pri šifrovaní a dešifrovaní. Vôbec nevadí, že informácia o tom kedy sa zhodli je verejná a prístupná každému. Dôležité je, že nikto okrem nich nepozná konkrétnu voľbu stavu (teraz už zo známej bázy) a ani výsledky meraní. A práve v nich je skrytý kľúč.

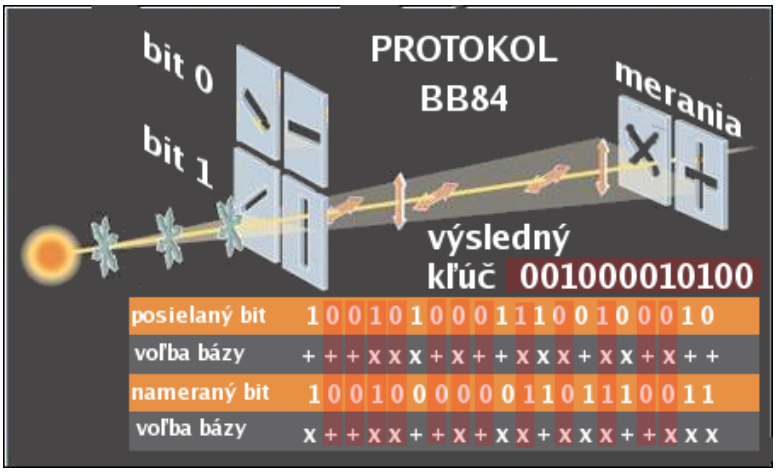
Distribúcia kľúča sa teda skladá z troch fáz. V pvej fáze odosielateľ, aj adresát ľubovoľne volia bázy a merania. Každý u seba zhromaždí postupnosť núl a jednotiek. V druhej fáze si oznámia voľby báz a meraní. To im umožní povyhadzovať zo získanej postupnosti tie nuly a jednotky, ktoré zodpovedajú prípadom keď sa nezhodli. Tieto dve fázy samozrejme nie možné zameniť. V priemere sa obidvaja zhodnú zhruba v polovici prípadov. Aby si boli istí, že majú skutočne rovnaký kľúč, tak zverejnia aj niektoré bity zo získaného kľúča. Ak pri porovnaní zistia nejaké chyby, tak vedia, že niekto sa snažil ich komunikáciu rušiť, nebodaj odpočúvať. Nepriateľ môže posielané kvantové bity zachytávať a posielať adresátovi úplne vymyslené stavy. Našťastie neexistuje spôsob ako by mohol zistiť, ktorý stav bol poslaný. Klonovanie kvantových stavov tiež nefunguje. Strategicky môže počkať na fázu, v ktorej sa zverejnia bázy, aby mohol uskutočniť merania. Jeho prítomnosť sa však nutne prejaví ako istá chybovosť výsledného reťazca bitov, t.j. kľúča. Adresátovi totižto nepriateľ podhadzoval vymyslené stavy, ktoré sú iba so štvrtinovou šancou správne. Aby sme ho skutočne odhalili, tak potrebujeme zverejniť zhruba polovicu svojich „správnych“ bitov. V tretej fáze teda overujeme bezpečnosť kľúča.

**Kryptografia v praxi**

Ako to už býva, v praxi sa stretávame s „drobnými“ problémami. Ako zabezpečiť prenos fotónu z jedného miesta na druhé spôsobom, aby ho neustále interakcie s prostredím, čo namenej zmenili, t.j. minimalizovať šum? Ako pripraviť jeden jediný fotón? Ako postaviť detektor, ktorý vždy detekuje prítomnosť, alebo neprítomnosť fotónu? Jednou z možností, ako vyriešiť tieto problémy, je jednoducho sa vykašlať na fotóny a skúsiť iné kvantové systémy. Fotóny sú však veľmi lákavé objekty, najmä vďaka svojej rýchlosti. Chceme predsa komunikovať čo najrýchlejšie. Na krátku vzdialenosť protokol BB84 nie je veľmi zložité zrealizovať priamo s polarizáciami fotónu. Dokonca by to išlo aj u Vás v škole. Postačí laserové ukazovátko, polarizačné okuliare,

prípadne polarizačné filtre používané pri fotografovaní. Tento experiment nespĺňa síce všetky požiadavky bezpečnosti, ale to by Vás nemalo odradiť.

Druhou nevýhodou polarizácie je, že pri prenose na trochu dlhšie vzdialenosti je šum už príliš veľký. Ani pri prenose optickými vláknami, v ktorých je šum menší, zmenu polarizácie nevieme kontrolovať. Preto namiesto polarizačných stavov sa v reálnych experimentoch používajú iné kvantové stavy fotónu, ktoré sú na vplyvy prostredia menej citlivé. Svojimi experimentami v oblasti kvantovej kryptografie sa preslávila v Európe najmä skupina *prof. Nicolasa Gisina* v Ženeve. Okolo Ženevského jazera sa im podarilo preniesť šifrovací kľúč pomocou optických vlákien na vzdialenosť zhruba 67 km, čo bolo svojho času rekordom v tejto oblasti. Dokonca tam funguje malá firma s názvom *Id Optique*, ktorá predáva „plug and play“ zariadenie realizujúce protokol BB84.




**Obr.2.** *Na obrázku sú znázornené prvé dve fázy protokolu BB84, t.j. fáza vygenerovania núl a jednotiek na oboch stranách a spracovanie podľa následného zverejnenia báz, resp. nastavení polarizátora. Symbolom + označujeme bázu horizontánej a vertikálnej polarizácie. Diagonálna báza je označená ako x.*

V dnešnej dobe niektorí experimentátori prakticky po celom svete vedia preniesť šifrovací kľúč na vzdialenosti zhruba 100 km. Bohužiaľ, táto hranica je už na úrovni technologických možností dnešných optických káblov. Aj preto sa stále venuje pozornosť možnostiam prenosu fotónov vo vzduchu. Šum je v porovnaní s optickými vláknami síce oveľa väčší, ale ideou je prekonať iba asi 15km vzdialenosť smerom k najbližším sondám a potom pokračovať v prenose v tejto výške nad povrchom Zeme. V tejto výške je už atmosféra natoľko riedka (de facto už nie je), že aj šum pri prenose by bol oveľa menší a fotóny by neporušené mohli prekonať veľké vzdialenosti. Prvé experimenty tohoto typu sa uskutočňovali v Spojených štátoch americkým, ale aj napríklad v prostredí európskych Álp, kde nie sú rušivé vplyvy mestského prostredia. Pred zhruba dvoma rokmi experimentátori zo susednej Viedne uskutočnili prenos vzduchom ponad Dunaj. Nedávno bola kvantová kryptografia využitá aj na zabezpečenie prevodu peňazí medzi bankami. Zdá sa, že kvantová kryptografia si pomaly hľadá svoje uplatnenie aj v praktickom živote.

Protokol BB84 neslúži priamo na prenos informácie, ale rieši problém bezpečnej distribúcie šifrovacieho kľúča potrebného pre realizáciu Vernamovej šifry. Jediné, čo využívame je princíp superpozície (stavy $|+\rangle, |-\rangle$ sú superpozíciami stavov horizontálne a vertikálne polarizovaných fotónov) a princíp neurčitosti, ktorý zabraňuje nepriateľovi zakódovanú informáciu odhaliť. Poprvýkrát v histórii kryptografie je bezpečnosť zaručená fyzikálnymi zákonmi a princípmi. Všetky známe a používané šifry využívajú zložitosť tzv. jednosmerných matematických úloh. Príkladom takejto úlohy je rozklad na prvočísla. Každý ľahko určí výsledok násobenia dvoch prvočísiel 17x29, ale viete súčinom akých prvočísiel je 1643? Skúste obidve tieto úlohy vyriešiť a porovnajte si čas, ktorý ste na riešenie potrebovali. Jedným smerom (súčin) je úloha ľahká, kdežto pri opačnej úlohe už hovoríme o probléme. Práve na tomto princípe je založené aj známa tzv. *RSA šifra*. Problém je tak zložitý, že ani použijúc tie najlepšie metódy, ktoré poznáme, nevyriešime faktorizáciu veľkých čísiel v rozumnom čase. Aj na tých najlepších počítačoch by sme potrebovali čas, ktorý presahuje vek vesmíru. Na druhej strane súčin aj pre takto veľké čísla je pomerne jednoduchou záležitosťou. Hlavne pre najnovšie počítače. Naša bezpečnosť v istom zmysle závisí na našej neschopnosti a nie je ani jasné, či táto neschopnosť je principiálna, alebo nie. Nech je to už akokoľvek, okrem toho, že kvantová teória ponúka vlastné riešenia pre kryptografiu, tak tzv. kvantový počítač by bol schpný súčasnú bezpečnosť do istej miery narušiť. Napríklad, by nám umožnil rozfaktorizovať zhruba rovnakou, alebo aspoň rádovo porovateľnou, rýchlosťou ako násobiť. O kvantovom počítači si povieme niečo nabudúce.

**V. Kvantové počítače**

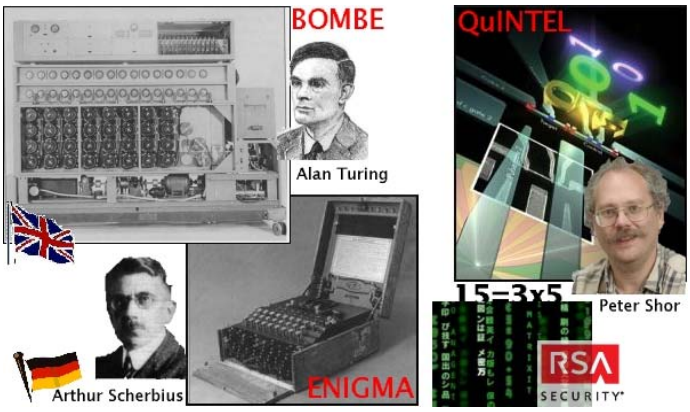
*Nie každý si uvedomuje, že pomenovanie počítača nie je odvodené od slova počítať náhodou. Či už ide o hru, alebo o bežné písanie, počítač na našom stole vykonáva výpočty. V zlomku sekundy zvládne milióny jednoduchých matematických operácií, ktoré by nám trvali niekoľko rokov. Napriek tomu však na niektoré úlohy nestačí, resp. čas, ktorý by potreboval presahuje nielen dobu jeho funkčnosti, ale aj vek vesmíru. V tejto časti si povieme niečo o tom, ako využitie kvantových vlastností môže pomôcť pri rýchlejšom riešení problémov.*

Za pohodlnosťou, ktorú nám ponúka obyčajná kalkulačka, je skrytý pomerne dlhý vývoj. Ľuďom bolo už dávnejšie jasné, že základné operácie ako sčítanie, násobenie, atď. sa dajú rozložiť do jednoduchších procedúr. V škole sa naučíme konkrétne postupy ako sčitovať, násobiť a deliť ľubovolne veľké čísla. Ide viac-menej o zautomatizované činnosti, ktoré nepotrebujú príliš veľké premýšľanie. A naviac dajú sa zrealizovať pomocou fyzikálnych procesov. Inými slovami, aj obyčajné fyzikálne objekty (nielen človek) sú správnym používaním schopné vykonávať výpočty. Všetci poznáme vzťah *dráha = čas* x *rýchlosť*. Ak chceme vypočítať 45x200, tak nám stačí udeliť napr. autíčku počiatočnú rýchlosť 200 mm/s a počkať 45 sekúnd. Zmeraním prejdenej dráhy v milimetroch získame výsledok násobenia. Autíčko vykonalo výpočet za nás. Samozrejme nejde o ideálny spôsob, pretože zanedbávame trenie a nepresnosti merania času, dĺžky a rýchlosti. Avšak podobným, aj keď oveľa komplikovanejším spôsobom, za nás „fyzika“ vykonáva výpočty aj v kalkulačkách, alebo počítačoch.

Ak chceme postaviť prístroj, ktorý by vyriešil danú úlohu za nás, tak musíme poznať postup, ako sa k výsledku dostať. Takýto postup výpočtu, resp. návod na riešenie nejakého problému sa odborne nazýva *algoritmom*. Algoritmus napísaný v reči, ktorej rozumie napr. počítač, sa nazýva *programom*. Ani si to neuvedomujeme, ale algoritmy vykonávame celkom bežne. Všetci to poznáme: *pri prechode cez cestu pozri vľavo, pozri vpravo, pozri vľavo a ak nič nejde, tak prejdi cez cestu*. Ide o vžitú procedúru, ktorú si vôbec neuvedomujeme. Každý algoritmus je vlastne receptom, alebo návodom, ako vyriešiť nejaký problém, prípadne splniť nejakú úlohu. Tento návod je zložený z postupnosti inštrukcií, pokynov, ktoré je potrebné uskutočniť. Tieto inštrukcie sú akýmisi základnými operáciami prístroja, ktorý ich má splniť, resp. ide o operácie, ktoré je tento prístroj schopný vykonávať.

**Turingov stroj**

Prvé mechanické prístroje, ktoré nás odbremenili od základnej aritmetiky, zostrojili ešte v 19. storočí. Tieto „primitívne“ kalkulačky sa postupne zdokonaľovali a nakoniec predbehli svojich stvoriteľov nielen v rýchlosti výpočtu. Mechanické zariadenia sa začali používať aj v takých oblastiach ako je napríklad kryptografia. Nemecká armáda (ešte pred druhou svetovou vojnou) používala na zakódovanie a dekódovanie tajných rozkazov prístroj zvaný *ENIGMA*. Žiadny človek nie je schopný dostatočne rýchlo rozlúštiť takto zakódované posolstvo. Počas vojny anglická tajná služba zamestnávala okrem iných aj matematika *Alana Turinga*, ktorý prišiel s myšlienkou postaviť stroj proti stroju. Alan Turing zovšeobecnil pojem výpočtu a vymyslel všeobecný model stroja, ktorý je schopný vykonať ľubovoľný algoritmus. Inými slovami, riešenie akejkoľvek úlohy (aj dekódovania) sa dá uskutočniť pomocou opakovania zopár základných operácií tohto prístroja. Napríklad vieme, že pri sčítaní, násobení, delení, nám stačí používať jednoduché sčitovanie čísel menších ako desať, t.j. „počítanie na prstoch“.




**Obr. 1. Turingov stroj a Shorov algoritmus.** *Anglický prístroj Bombe počas II. svetovej vojny pomáhal odhaľovať nemecké rozkazy zašifrované zariadením Enigma. Mechanický šifrovací prístroj Enigma bol vyrobený Arthurom Scherbiusom a mal plnú dôveru nemeckého hlavného štábu. Na anglickej strane však tajná služba zamestnávala matematika Alana Turinga, ktorý položil základy modernej informatiky a vymyslel koncepciu univerzálneho počítacieho zariadenia, tzv. Turingov stroj. Turing sa nemalou mierou podielal aj na zotrojení zariadenia Bombe. V dnešnej dobe je situácia podobná. Metóda RSA šifrovania sa považuje za bezpečnú, avšak zotrojenie kvantového počítača (QuIntelu) by túto situáciu zmenilo podobným spôsobom ako kedysi Bombe.*

Idea *Turingovho stroja* bola významným krokom pre rozvoj *informatiky*, ktorá skúma vlastnosti algoritmov, t.j. postupy ako nejaké základné a jednoduché operácie využiť na vykonanie tých najkomplikovanejších úloh. Jedným z hlavných poznatkov informatiky je, že Turingov stroj je ten najvšeobecnejší možný typ počítacieho stroja, pretože dokáže vykonať akýkoľvek výpočet. Moderný počítač nedokáže viac ako Turingov stroj. Vývoj v posledných rokoch však toto tvrdenie informatiky trochu poopravil, resp. upresnil. Záver je dnes taký, že Turingov stroj je najvšeobecnejší možný stroj pracujúci na princípoch *klasickej fyziky*.

**Cesta ku kvantovým počítačom**

V súvislosti s univerzalitou Turingovho stroja je prirodzenou otázka, ktoré operácie sa skutočne realizujú vo fyzikálnych systémoch, resp. procesoch? Na túto otázku teória okolo Turingových strojov v princípe zodpovedať nemôže. Turingov stroj pracuje s logickými operáciami na abstraktných bitoch informácie. Tieto operácie sú odvodené z našej každodennej skúsenosti, ktorá žiaľ nezahŕňa skúsenosť s kvantovým svetom. Základné funkcie Turingovho stroja sú odpozorované z tzv. *klasickej fyziky*. Kvantové zákony sú však úplne iné a základnou otázkou je, či v oblasti počítania umožňujú niečo nové a lepšie, alebo nie. Druhou (praktickejšou) otázkou je potom cena, ktorú nás využitie týchto nových operácií bude stáť, resp. či skutočne tieto nové možnosti potrebujeme, alebo nie. Tieto „nové“ prístroje pracujúce na princípoch kvantovej fyziky nazývame *kvantovými počítačmi*.

Jedna z dôležitých úloh, ktorú riešia počítače, je *simulácia* fyzikálnych systémov. Hlavnou motiváciou na postavenie prvého počítača *ENIAC* bola práve simulácia atómovej bomby. Asi ani nenájdeme „lepší“ príklad na užitočnosť simulácií. Ich úlohou je nepriamo zistiť vlastnosti a správanie sa fyzikálnych systémov. Nepriamo v tomto prípade znamená, že na to, aby sme niektoré dôsledky otestovali, nemusíme nechať atómovú bombu skutočne vybuchnúť. Podobne pri konštrukciách lietadiel, áut, alebo aj pri výrobe liekov sú simulácie veľmi užitočným nástrojom, ktorý v neposlednom rade šetrí aj peniaze. Simulácie však nie sú vôbec jednoduchým problémom. Ani pre počítač. V osemdesiatich rokoch známy americký fyzik *Richard Feynman* postrehol fakt, že kvantové systémy nebudeme nikdy schopní efektívne simulovať na našich počítačoch. Príčinou je princíp superpozície, vďaka ktorému počet parametrov narastá s veľkosťou systému príliš rýchlo. Ak chceme modelovať kvantové systémy, tak potrebujeme kvantový počítač, t.j. zariadenie, ktoré má vlastnosti kvantového sveta zabudované priamo vo svojich funkciách.

**Čo je zložité?**

Vráťme sa teraz späť k algoritmom. Začnime úlohou, v ktorej treba spočítať čísla od 1 do 100. Ako prvý spôsob každému zíde na um jednoducho postupne sčítať všetkých 100 čísiel, t.j. 1+2+3+4+5+... . Existuje však aj jednoduchší postup. Stačí si uvedomiť, že platí 100+1=99+2=98+3=...=51+50=101. Vďaka tomuto faktu celkový súčet dostaneme, ak vynásobíme 50x101. Podobným trikom spočítame čísla od 1 po hocijaké číslo N. Štandardným postupom násobenia, ktorý sme sa naučili v škole, prídeme k výsledku oveľa skôr ako postupným sčítavaním N čísiel. Tento príklad nám ukazuje, že na riešenie aj jedného problému existuje viacero algoritmov, z ktorých jeden môže byť jednoduchší ako ten druhý.

*Zložitosť* samotného problému potom určujeme podľa času, ktorý je potrebný na vykonanie toho najrýchlejšieho známeho algoritmu. Inými slovami čím je problém zložitejší, tým na jeho vyriešenie potrebujeme uskutočniť viac krokov. Táto definícia zložitosti plne zodpovedá našej intuitívnej predstave. Typickým príkladom zložitého problému je rozklad na prvočísla. Momentálne síce nevieme povedať nakoľko je tento problém zložitý, pretože stále ešte nepoznáme ten najrýchlejší algoritmus na jeho riešenie. Veríme však tomu, že ide o úlohu veľmi ťažkú. Dokonca sme na tomto fakte založili aj bezpečnosť našich informácií na internete (RSA šifra). Skúste si samy zistiť násobkom ktorých dvoch prvočísiel je 403. Opačná úloha, t.j. zistiť výsledok 19x23, je oproti tomu hračkou.

**Rozklad na prvočísla**

Prvočísla majú vcelku výsadné postavenie medzi číslami. Ide o čísla, ktoré nie sú deliteľné ničím iným ako sebou samým a jednotkou, napr. 1,2,3,5,7,11,13,17,19,...

Každé iné číslo sa dá jednoznačne napísať ako súčin prvočísiel, napr. 182=2x7x13. Úlohou rozkladu na prvočísla je nájsť pre ľubovoľné číslo príslušné prvočísla. Ako na to?

Najjednoduchšou metódou je skúšať dané číslo *N* postupne deliť všetkými prvočíslami menšími ako odmocnina z *N*. Takýto postup je však pre veľké čísla veľmi náročný a čas potrebný na jeho realizáciu by trval veky. Poznáme síce niektoré rýchlejšie algoritmy, ale zrýchlenie nie je príliš citeľné, resp. je ďaleko od toho, aby sme problém považovali za jednoduchý. Ak za sekundu počítač vykoná miliardu operácií, tak čas potrebný na rozloženie 50-ciferného čísla je zhruba 23 miliónov rokov. Bola vypísaná odmena 200 000 dolárov pre toho, kto nájde rozklad istého 617-ciferného čísla. Zatiaľ sú však tieto peniaze v bezpečí, pretože kvantový počítač je ešte v nedohľadne a dnešným počítačom by to trvalo dobu, ktorá ďaleko presahuje odhadovanú existenciu vesmíru.

Jeden z trikov na riešenie rozkladu na prvočísla využíva výsledky z teórie čísiel týkajúce sa tzv. *modulárnej aritmetiky*, ktorej prototypom sú napríklad hodiny, ktoré ukazujú čísla iba od 1 po 12. Ak chceme na hodinách vyrátať 7+8, tak výsledok dostaneme tým že ručičku zo 7 posunieme o 8 hodín doprava. Po tomto sčítaní bude ručička ukazovať 3 hodiny. Učene takýto výpočet zapíšeme nasledovne 7+8=3 (mod 12) a čítame 7 plus 8 rovná sa 3 modulo 12. Nájdenie prvočísiel pre *N* je ekvivalentné problému nájsť periódu postupnosti čísiel $f(k) = y^k \pmod N$ pre nejaké $y<N$ a pre $k$=0,1,2,3,... . Napríklad postupnosť 1,4,3,6,1,4,3,6,1,4,3,6,.... má periódu rovnú 4. Ak nájdeme periódu *r*, tak hľadané prvočísla získame nájdením najväčších spoločných deliteľov (NSD) pre dvojice $\left[y^{r/2}+1, N\right]$ a $\left[y^{r/2}-1, N\right]$. Táto úloha je jednoduchá na vypočítanie a získaní delitelia sú hľadanými prvočíslami v rozklade *N*. Dôvod, prečo tento postup funguje, žiaľ nie je úplne jednoduchý a využíva výsledky *teórie čísiel*. Uveďme si iba ako príklad rozklad čísla N=15 a zvoľme y=7. Funkcia $f(k) = y^k \pmod N$ v tomto prípade predstavuje číselnú postupnosť 1,7,4,13,1,7,4,13,1, ..., ktorá má periódu 4, t.j. $7^4 \pmod{15} = 1$ . Teraz určíme $y^{r/2}=7^2=49$ a NSD(48,15)= 3, NSD(50,15)=5. Tým dostávame rozklad 15=5x3.

Namiesto hľadania prvočísiel je našou úlohou nájsť periódu. Na analýzu periodických funkcií sa v matematike využívajú metódy tzv. *Fouriérovej analýzy*. Napríklad pri analýzach zvuku pomocou tejto metódy vieme určiť tóny (frekvencie) z akých sa daný zvuk skladá. V našom prípade ide o diskrétnu periodickú funkciu a úlohou je uskutočniť tzv. *diskrétnu Fouriérovu transformáciu*, ktorá robí niečo veľmi podobné. Vďaka tejto transformácií získame hľadanú informáciu o perióde. Realizácia diskrétnej Fouriérovej transformácie je práve tým zložitým krokom, ktorý na klasických počítačoch nevieme uskutočniť efektívne.

**Kvantové bity**

Základnou jednotkou, s ktorou pracujú dnešné počítače je jeden *bit*, ktorý predstavuje najmenšie možné množstvo informácie. Jeden bit môže mať jednu z dvoch hodnôt: *nula*, alebo *jedna*. Akúkoľvek inú informáciu vieme vyjadriť pomocou týchto základných jednotiek informácie. Iba 8 bitov nám stačí na vyjadrenie ľubovoľného čísla od 0 po 255. Zo školy tento prepis čísla do bitov poznáme ako prepis z desiatkovej sústavy do dvojkovej. Napríklad číslo 25 zapisujeme ako **11001**, čo znamená **1**.16+**1**.8+**0**.4+**0**.2+**1**.1=25. Akýkoľvek výpočet vieme zapísať ako postupnosť operácii, ktoré menia hodnoty jednotlivých bitov, čím vstupnú informáciu menia na výstupnú, t.j. na výsledok. Napríklad pri výpočte **101**x**101=11001** (5x5) postupujeme presne tak isto ako pri obyčajnom násobení, iba používame vzťahy pre súčin 0x0=1x0=0x1=0, 1x1=1 a pre súčet 0+0=0, 0+1=1+0=1,

1+1=10. Ľubovoľný výpočet vieme napísať ako súčet, prípadne súčin núl a jednotiek. Ak k tomu prirátame operáciu negácie, ktorá zmení hodnotu bitu na opačnú a kopírovanie, tak máme v podstate všetky operácie, ktoré počítač vykonáva.

Fyzikálne jeden bit zodpovedá dvom (perfektne rozlíšiteľným) stavom fyzikálneho systému, napr. svieti/nesvieti, prúd tečie/netečie, atď. Každý z týchto stavov zodpovedá inej informácii (alternatíve). Môžeme povedať, že informácia je zakódovaná do stavu fyzikálneho systému. Ako sme si ale povedali v tretej časti tohoto seriálu, v kvantovej teórii okrem týchto dvoch stavov existuje aj stav, ktorý je ich superpozíciou, t.j. niečo medzi nulou a jednotkou. Takéto niečo v klasickom prípade neexistuje. Hovoríme o *kvantovom bite*, ktorý je základným stavebným kameňom kvantového počítača. Stavy, ktoré sú niečo medzi nulou a jednotkou, sú charakteristické tým, že pri zisťovaní, o ktorú hodnotu vlastne ide, s istou pravdepodobnosťou dostávame obidva výsledky, t.j. aj nula, aj jedna. Pomocou viacerých kvantových bitov vieme zapísať ľubovoľné číslo presne tým istým spôsobom ako pomocou „obyčajných“ klasických bitov. Opäť však platí, že okrem toho, že máme ľubovoľné čísla, tak máme aj ich superpozície. Inými slovami existujú stavy, ktoré čiastočne obsahujú všetky čísla. Napríklad pre osem kvantových bitov všetky čísla od 0 po 255.

Pri riešení úlohy nás niekedy zaujíma hodnota nejakej funkcie pre dané číslo. Napríklad pri rozklade $N$ na prvočísla nás zaujíma, či nejaké číslo delí $N$, alebo nie. Inými slovami zaujíma nás podiel. Problémom je, že výpočet tej istej funkcie (podielu) potrebujeme urobiť veľmi veľa krát. Vlastne pre každé číslo zvlášť až pokým nenarazíme na ten správny výsledok. S kvantovými bitmi však akoby túto funkciu počítame naraz pre všetky hodnoty, pretože máme stavy, ktoré sú superpozíciou všetkých hodnôt. Táto vlastnosť kvantových výpočtov sa nazýva *kvantovým paralelizmom*, pretože kvantový počítač súčasne (paralelne) vykonáva všetky úlohy.

Proces výpočtu si môžeme predstaviť tak, že v algoritmoch na výpočet funkcie používame akúsi čiernu skrinku. Napríklad pri hľadaní rozkladu táto čierna skrinka počíta podiel čísla, ktoré rozkladáme a nášho tipu na výsledok. Ak dostaneme celočíselný výsledok, tak vieme, že sme hľadaný rozklad našli. Ak nie, tak pokračujeme ďalším tipom. Kvantová mechanika nám umožňuje iba pri jednom použití „kvantovej“ čiernej skrinky zistiť hodnoty funkcie pre všetky potenciálne tipy. Jediným problémom zostáva, že tento výsledok má tiež formu superpozície a je stále skrytý v kvantovom svete. Musíme vykonať meranie, ktoré náhodne vyberie iba jedinú hodnotu, čím sme zdanlivo tam, kde sme boli aj predtým. Nie je to však úplne tak. Nás totižto zaujíma tento výpočet iba pre hodnotu, pre ktorú je výsledkom delenia celé číslo bezo zvyšku. O tejto hodnote vieme, že je jediná. Vhodnou manipuláciou (ďalším kvantovým výpočtom) sa pokúsime nastaviť pravdepodobnosti tak, aby sme zvýhodnili práve tento prípad. Vďaka tomu s vysokou pravdepodobnosťou nameriame hodnotu, ktorú hľadáme. Kvantová mechanika za nás skúsi paralelne všetky možnosti a vyberie tie, ktoré hľadáme.

**Deutch-Jozsov algoritmus**

Teraz si ukážeme jednoduchý príklad ako kvantový paralelizmus funguje v praxi. Ide o nasledovnú úlohu. Majme čiernu skrinku, ktorá počíta funkciu $f$ a nás zaujíma, či je táto funkcia konštantná, alebo nie. Pre jeden bit existujú 4 rôzne čierne skrinky, z ktorých dve počítajú konštantné funkcie, a dve nie: (1) *identita* $f(0)=0$, $f(1)=1$, (2) *negácia* $f(0)=1$, $f(1)=0$, (3) *nula* $f(0)=f(1)=0$ a (4) *jednotka* $f(0)=f(1)=1$. Klasicky nemáme inú možnosť ako vyskúšať čiernu skrinku pre každý možný vstup, t.j. pre obidve hodnoty bitu. Použitím kvantového bitu nám však stačí čiernu skrinku použiť jediný raz a zmeraním jednoznačne zistiť, či je funkcia konštantná, alebo nie. Nevieme, síce povedať, o ktorú čiernu skrinku konkrétne ide, ale to ani nie je našou úlohou. Kľúčovým momentom je použitie kvantového bitu v superpozičnom stave nuly a jednotky. Tento stav obsahuje v rovnakej miere informáciu o obidvoch hodnotách, t.j. pri zisťovaní hodnoty získavame obidva výsledky s rovnakou pravdepodobnosťou. Naviac ešte použijeme jeden ďalší kvantový bit, ktorý je v stave s hodnotou nula aj na začiatku a aj na konci výpočtu. Dá sa povedať, že má funkciu akéhosi „katalyzátora“ výpočtu. Nebudeme popisovať detaily tohoto algoritmu. V skutočnosti nejde o veľmi užitočný algoritmus, ale slúži ako veľmi jednoduchá ukážka toho, že kvantový počítač vďaka superpozícii, resp. paralelizmu, umožňuje efektívnejšie riešenie problému.

**Obr. 2. Mooreov zákon pre procesory Intel.**
*Krivka znázorňuje exponenciálny trend vývoja moderných počítačov.*

**Shorov algoritmus**

V roku 1994 *Peter Shor* našiel spôsob ako efektívne uskutočniť diskrétnu Fouriérovu transformáciu za pomoci kvantového počítača. Ako sme si povedali, táto transformácia je tým komplikovaným krokom v probléme rozkladu na prvočísla. Vďaka tomuto výsledku sa kvantový počítač stal jedným z hlavných potenciálnych nepriateľov niektorých kryptografických protokolov

a 200 000 dolárov si začalo hľadať svojho majiteľa. Shorov algoritmus je doposiaľ jedným z najväčších výsledkov dosiahnutých v oblasti kvantových počítačov. V princípe vieme, ako Shorov algoritmus vykonať. Chýba nám už len samotný kvantový počítač. Hlavným problémom pri jeho zostrojení je prílišná citlivosť kvantových systémov na vplyvy okolia. Tieto interakcie v podstate ničia kvantovú superpozíciu medzi kvantovými bitmi, ktorá, ako sme si povedali, je podstatná. V laboratóriách po celom svete sa testujú tie najrôznejšie fyzikálne systémy, ktoré by nám mali slúžiť ako kvantové bity. Neustále sme svedkami drobných pokrokov, ale na skutočný prielom v technológii ešte len čakáme. V roku 2001 bol Shorov algoritmus zrealizovaný v laboratóriách IBM, kde sa podarilo experimentálne nájsť prvočíselný rozklad čísla 15.

Vývoj súčasných počítačov je extrémne rýchly. V roku 1965 americký elektronik *George Moore* odpozoroval, že počet tranzistorov (základných operačných jednotiek) na jednom elektronickom čipe sa zdvojnásobuje zhruba každého polroka. V tom čase bol tento počet rovný zhruba 50 tranzistorom. Vyslovil domnienku, že tento trend bude pokračovať aj naďalej. Dnes sme svedkami toho, že jeho predpoveď stále platí a hovoríme o tzv. *Mooreovom zákone*. Ak sa však pozrieme obdobia okolo roku 2015, tak zistíme, že miniaturizácia dosiahne úroveň atómov. Na týchto rozmeroch však kraľuje kvantová mechanika a platia iné zákony než na aké sme zvyknutí. Vďaka tejto perspektíve je skúmanie potenciálu kvantových počítačov vlastne nevyhnutnosťou. Skôr či neskôr v praxi narazíme na podivuhodný svet kvantovej teórie. V tejto časti sme sa snažili načrtnúť základné idey kvantového počítania. Pre detailnejšie vysvetlenie odporúčame populárnu knižku od *Georga Johnsona* s názvom „Zkratka napříč časem“. V ďalšej časti sa vrátime späť k fyzike a povieme si niečo o systémoch, z ktorých by sa mohol budúci kvantový počítač skladať.

## VI. Skladáme kvantový počítač

*Základným stavebným kameňom dnešných počítačov sú tzv. čipy, resp. integrované obvody. Ide o elektronické zariadenia obsahujúce množstvo tranzistorov, ktorých činnosti rozumieme vďaka kvantovej teórii. Napriek tomu však tranzistory svoj kvantový pôvod nevyužívajú a z pohľadu informatiky je ich fungovanie úplne klasické. V tejto časti si predstavíme základné súčiastky kvantových počítačov a naznačíme si základné experimentálne techniky, ktoré sa pri kvantovom počítaní používajú.*

V dnešnej dobe sa o jeden bit informácie stará niekoľko desaťtisíc častíc, avšak tento počet sa z roka na rok závratne znižuje. Prirodzenou hranicou tejto miniaturizácie bude informácia reprezentovaná jednotlivými časticami. Ešte skôr ako narazíme na túto principiálnu hranicu, prídeme do oblastí, v ktorých je už chod sveta určený kvantovou fyzikou. Táto teória je plná zvláštností a podivností, ktorým síce nerozumieme tak ako by sme chceli, ale vieme ich využívať. Princípy kvantovej fyziky prinášajú do oblasti spracovania informácie úplne nové prvky. V minulej časti (*Quark 2005/06*) sme načrtli, že hlavná sila kvantových počítačov je v tzv. *kvantovom paralelizme*, ktorý nám v istom zmysle umožňuje vykonať naraz obrovské množstvo výpočtov, t.j. operácií.

### *HĽADÁ SA KVANTOVÝ BIT*

Kvantový počítač by mal namiesto s bitmi informácie pracovať s tzv. *kvantovými bitmi*, t.j. dvojhladinovými kvantovými systémami. Každá z hladín reprezentuje jednu z logických hodnôt (nula, alebo jedna). Aby sme vedeli plnohodnotne vykonávať kvantové výpočty, tak potrebujeme kvantové objekty, s ktorými vieme veľmi dobre manipulovať, ktorých správanie a vývoj vieme ustrážiť a kontrolovať. Ktoré častice si vybrať? Použiť priamo elektróny, alebo protóny by bolo perfektné. Avšak obidve tieto častice až priveľmi radi interagujú a dobrá „izolácia“ elektrónov a protónov nie je práve jednoduchá vec. Iná je situácia s atómmi, prípadne iónmi. Častíc tohoto typu je okolo nás pomerne dosť. Ako je to však s ich kvantovými vlastnosťami?

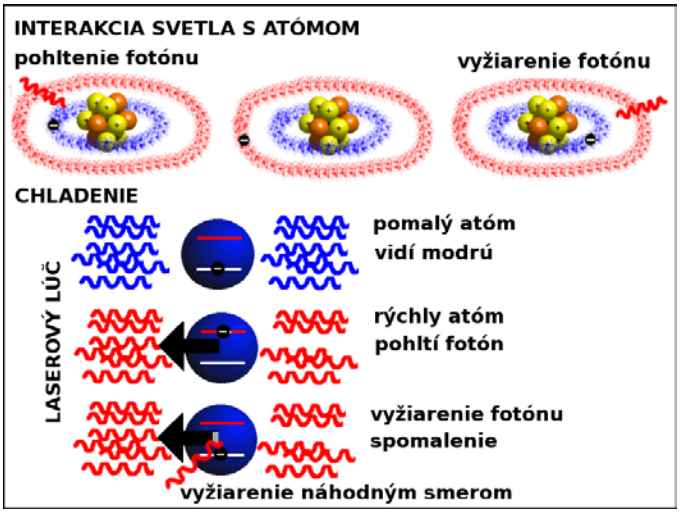
Jedným z prvých úspechov kvantovej fyziky bolo vysvetlenie spektrálnych čiar atómu vodíka. Vďaka kvantovej mechanike sa nám podarilo pochopiť nielen periodicitu Mendelejevovej tabuľky prvkov (atómov), ale aj princíp chemickej väzby, chemických reakcií a v neposlednom rade aj stabilitu hmoty. Tieto výsledky samy osebe ešte neznamenajú, že atómy okolo nás prejavujú všetky črty kvantových systémov. Skôr opak je pravdou a bežne nemusíme brať do úvahy ich kvantovú podstatu. Ak chceme pripraviť atóm v nejakom superpozičnom stave a overiť *princíp superpozície*, prípadne *interferenciu* (písali sme o tom v *Quarku 2005/03*), tak si potrebujeme tieto častice pripraviť v laboratóriu za veľmi špecifických podmienok.

### *CHLADENIE*

Jedným z hlavných nepriateľov kvantových nádejí je *teplota*, ktorá svojim spôsobom pracuje proti prejavom kvantového sveta a s jej zvyšovaním sa vo všeobecnosti veľmi rýchlo strácajú kvantové vlastnosti. Podľa učebníc fyziky teplota vyjadruje mieru chaotického pohybu častíc a je úmerná priemernej energii častíc. Ak teda chceme použiť atómy na realizáciu kvantových bitov, tak ich potrebujeme najprv schladiť, resp. spomaliť. *Nulová teplota* teoreticky znamená stav bez pohybu, ale kvôli *princípu neurčitosti* kvantové systémy takýto stav „absolútneho pokoja“ nikdy nemôžu dosiahnuť. Predstavujeme si to tak, že kvantová častica neustále vykonáva akýsi vibračný pohyb, napr. elektróny stále akosi obiehajú okolo jadra. V kvantovej fyzike stav s nulovou teplotou definujeme ako stav s najmenšou energiou, tzv. *základný stav*.

Podľa kvantovej mechaniky sa atóm zbavuje prebytočnej energie tým, že vyžiari fotón. Atómy aj molekuly okolo nás však neustále bombardujú fotóny najrôznejších energií, ktoré vracajú vyžiarenú energiu atómu späť. Aj preto sa atómy prakticky nenachádzajú vo svojom základnom stave a majú nenulovú teplotu. Aby sme pochopili akým spôsobom chladenie funguje, tak potrebujeme získať predstavu o vzájomnej interakcii svetla (fotóny) a látky (atómy, ióny, molekuly). Ide o pomerne komplikovaný fyzikálny proces, ktorá sa dá predstaviť nasledovne. V prvom rade treba povedať, že konkrétny atóm neinteraguje s hocakým fotónom, ale iba s fotónmi určitej energie, t.j. určitej farby, resp. frekvencie. Pri tejto interakcii prichádza k zmene stavu atómu, v ktorom zasiahnutý elektrón „preskočí“ na vzdialenejšiu obežnú dráhu (získa energiu fotónu), alebo úplne vyletí z atómu preč, t.j. vznikne záporný ión. Atómy majú tendenciu minimalizovať svoju energiu, t.j. elektróny časom popreskakujú na

bližšie a menej energetické obežné dráhy. Pri takomto preskoku stratia časť svojej energie, ktorá je vyžiarená do okolia vo forme fotónov. Rozdiel energií medzi dvoma obežnými dráhami (hladinami) je úmerný energii (frekvencii) absorbovaného, alebo vyžiareného fotónu.




**Obr.1** *Interakcia svetla s atómom pozostáva z troch fáz: pohltenie fotónu, excitácia atómu a vyžiarenie fotónu. Pri chladení atómov sa využíva Doplerov jav, podľa ktorého pre pohybujúci sa a pre stojaci atóm má ten istý fotón rozdielnu energiu (frekvenciu).*

Jedna z metód chladenia využíva tzv. *Dopplerov jav*. Atómy pohybujúce sa veľkou rýchlosťou vidia fotóny inej frekvencie, ako atómy pomalšie. Vyberieme teda laser, ktorý bude pohlcovaný rýchlymi atómmi, zatiaľ čo pomalšie si tento laser ani nevšimnú, t.j. fotóny pre ne nemajú tú správnu frekvenciu. Pri vzájomnom kontakte atómu a fotónu sa okrem energie zachováva aj hybnosť, čo sa prejavuje ako isté kopnutie fotónu do atómu. Ide o proces podobný zrážke dvoch guličiek. V tomto prípade však jedna z nich (fotón) po zrážke zanikne. Keďže spätné vyžiarenie fotónu je v úplne náhodnom smere, tak pri opakovaným interakciách sa príspevky k hybnosti pochádzajúce z vyžarovania fotónov navzájom vyrušia. Zostáva iba hybnosť pochádzajúca od absorbovaných fotónov, ktorá má však iba jeden smer a efektívne spomaľuje rýchlosť atómov, t.j. atómy ochladzuje (viď Obr.1).

***ČASTICE V PASCI***

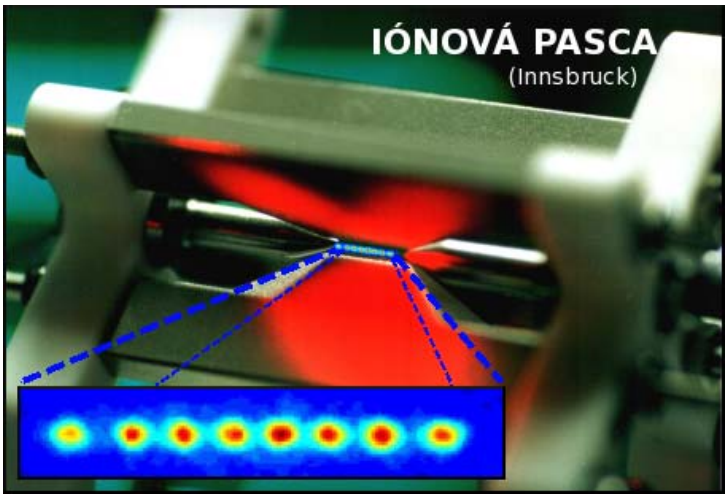
Aby sa nám spomalené atómy, alebo ióny zase nerozutekali, tak ich lapíme do pasce a pokiaľ možno, čo najviac odizolujeme od nežiadúcich vplyvov okolitého sveta. Samozrejme ide o špeciálnu pascu, ktorá sa tvorí pomocou laserov a elektród vytvárajúcich špeciálne silové pôsobenie. Pomocou elektrických a magnetických síl sa vytvorí akoby jama, do ktorej sa atóm alebo ión zachytí. Do takejto pasce vložíme niekoľko atómov, na ktorých sa budeme pokúšať vykonávať výpočty. Okrem priestorových stupňov voľnosti majú atómy a ióny aj vnútorné stupne voľnosti, ktoré zodpovedajú vzájomnému usporiadaniu elektrónov a protónov, z ktorých je atóm alebo ión zložený. Pre jednoduchosť si to predstavíme tak, že elektróny obiehajú okolo jadra po istých dráhach, ktoré zodpovedajú možným vnútorným stavom, resp. energetickým hladinám. Elektróny medzi niektorými hladinami preskakujú, pričom alebo vyžarujú fotón, alebo absorbujú energiu nejakého fotónu. Kvantový bit je realizovaný nejakými dvoma vnútornými hladinami týchto častíc. Vyberáme si také, s ktorými vieme čo najlepšie narábať. V laboratóriách po celom svete sa robia experimenty s atómmi, prípadne iónmi vápnika, berýlia, sodíka, lítia, atď.

Pri konštruovaní kvantových hradiel a pri kvantovom počítaní na časticiach v pasci opäť používame laser. Dve vybraté hladiny si označíme ako $|g\rangle$ *(„ground state“)* a $|e\rangle$ *(„excited state“)*. Je výhodné vybrať si také hladiny, medzi ktorými sú samovoľné preskoky elektrónov zakázané, t.j. hodnoty informácie sa nám náhodne nemenia. Ak však chceme hodnotu kvantového bitu zmeniť, tak práve pomocou lasera zmeníme podmienky atómu alebo iónu takým spôsobom, že tento prechod je umožnený. V závislosti od doby svietenia laserom na atóm zmeníme aj jeho vnútorný stav zodpovedajúci kvantovému bitu. Týmito *laserovými pulzmi* vykonávame výpočet na jednotlivých atómoch. Zložitejším spôsobom vieme pomocou laserov sprostredkovať aj vzájomné interakcie medzi kvantovými bitmi, t.j. realizovať zložitejšie kvantové hradlá a teda uskutočniť plnohodnotný kvantový výpočet.

Ak chceme zistiť v akom stave sa náš kvantový bit nachádza, tak použijeme laser pracujúci na inej frekvencii. Laserom, ktorým vykonávame výpočty na jednotlivých kvantových bitoch by sme totižto tento stav menili. K tomu aby sme zistili hodnotu kvantového bitu, používame ešte jednu pomocnú hladinu $|m\rangle$. Merací laser je nastavený tak, aby donútil elektrón z hladiny $|g\rangle$ preskočiť na hladinu $|m\rangle$. Samovoľný preskok medzi týmito hladinami je povolený a preto sa tento elektrón vráti na svoju pôvodnú hladinu, pričom sa vyžiari fotón. Ak svietime takýmto laserom na kvantový bit v hodnotou $|g\rangle$, tak pozorujeme, že atóm vyžaruje. Ak má kvantový bit hodnotu $|e\rangle$, tak žiadne vyžarovanie nepozorujeme. Ak sú obe hodnoty v superpozícii, tak pozorujeme striedanie sa vyžarovania a nevyžarovania.

*Ignacio Cirac* a *Peter Zoller* v roku 1995 ako prví navrhli využitie iónov v pasci na kvantové počítanie. Ešte v tom istom roku tento návrh experimentálne zrealizovali v laboratóriách NIST (*National Institute of Standards and Technology*) v USA. *Chris Monroe* a *Dave Wineland* použili kvantové bity zakódované v iónoch berýlia $^{9}Be^{+}$ a ako prví zrealizovali kvantové hradlo

s názvom *kontrolované NOT*. Na interakciu dvoch kvantových bitov pri tomto hradle sa využívajú pohybové stupne voľnosti iónov v pasci. Kontrolované NOT tvorí jednu zo základných súčiastiek kvantového počítača a pomocou neho dokážeme v podstate zrealizovať akýkoľvek kvantový výpočet. Zdanlivo nič nestojí v ceste ku kvantovému počítaču založenom na iónoch, prípadne atómoch v pasci. Ako to však býva, svet nie je taký jednoduchý a príroda nám stavia do cesty ďalšie prekážky. Nami popísané princípy kvantového počítania s atómmi a iónmi pomocou laserov sú v skutočnosti o niečo komplikovanejšie. V súčasnosti nie je problém uložiť do pasce niekoľko iónov, prípadne atómov. S ich množstvom však narastá aj ich vzájomné ovplyvňovanie a opäť narážame na známy problém. Čím je systém zložitejší, tým je ťažšie udržať a pozorovať všetky jeho kvantové prejavy.




**Obr.2** *Ióny vápnika zachytené v pasci. Fotka je urobená CCD kamerou.*

Isté vylepšenie by mohla priniesť myšlienka tzv. *mikropasci*, t.j. každý z kvantových bitov (atómov) bude vo svojej vlastnej maličkej pasci. V tomto prípade treba vytvoriť silové pole, ktoré si môžeme predstaviť ako periodicky usporiadané jamy, do ktorých sa atómy zachytia (niečo ako obal na vajíčka). Tento model je momentálne oblasťou veľmi intenzívneho výskumu, ktorý v sebe spája rôzne experimentálne techniky.

***POLOVODIČOVÉ A SUPRAVODIVÉ KVANTOVÉ BITY***

Okrem atómov a iónov exitujú aj iné návrhy na realizáciu kvantových bitov. Veľmi sľubnou oblasťou je oblasť polovodičov, ktorá dominuje dnešným klasickým počítačom, ako aj oblasť supravodičov. V roku 1997 *David Loss* and *David di Vincenzo* navrhli spôsob ako využiť spiny jednotlivých elektrónov uväznených v tzv. *kvantových bodkách*. Kvantové bodky sú akési nanoostrovčeky elektrónov v inak vyprázdnenom priestore v tuhých látkach. Takýto priestor je vytvorený medzi dvoma vrstvami kovov, ako napríklad GaAs (t.j. gálium a arzén) a AlGaAs (t.j. hliník, gálium a arzén). Tieto nanoštruktúry nám slúžia na zachytenie elektrónov, ktoré by nám inak poľahky unikli a akékoľvek výpočty by neboli možné. Následne bolo navrhnutých niekoľko ďalších typov kvantových bitov založených na technológiách spojených s polovodičovými štruktúrami a javom supravodivosti. Podrobnejšie si však o nich povieme až v niektorej z ďalších častí.

***BUDÚCNOSŤ***

Nikto dnes nevie povedať, aké riešenie prinesie budúcnosť. Nevieme povedať, či zdoláme všetky prekážky, ktoré nám konštruovanie kvantového počítača ešte postaví do cesty. Nie je síce známy žiadny principiálny dôvod, prečo by kvantový počítač nemal fungovať. Nie je však ani jasné, či vôbec bude fungovať. Hlavným problémom je fenomén tzv. *dekoherencie*, ktorá je pomenovaním procesu straty kvantových vlastností potrebných pre kvantový paralelizmus, t.j. kvantovej superpozície. Nevieme, či budeme niekedy schopní tento proces eliminovať pre ľubovoľne veľký počet kvantových bitov. Vypracovala sa technika tzv. *kvantovej korekcie chýb*, ktorá dokáže za istých predpokladov úspešne bojovať proti dekoherencii. Nakoľko ale možno tieto predpoklady splniť v praxi, je dnes ešte otázne. V súvislosti s týmto si pripomeňme počiatky vzniku počítačov. Aj v tej dobe bolo mnoho kritických ohlasov a málokto predpokladal, že sa počítače vyvinú do tej formy, v akej ich poznáme dnes. Prvý počítač ENIAC zaberal celú halu a odhady na veľkosť počítačov budúcnosti neboli veľmi nádejné. Zlom priniesol až objav polovodičových súčiastok, v ktorom má kvantová fyzika tiež svoje pevné miesto, pretože princíp fungovania polovodičov a tranzistorov chápeme iba vďaka nej. Čakáme na podobný prelom v technológii, ktorý konštrukciu kvantových počítačov posunie ďalej.

Potrebujeme vôbec kvantové počítače? Spomeňme si na motiváciu, ktorá ľudí priviedla k myšlienke kvantových počítačov. Argumenty týkajúce sa efektívnejšieho riešenia zložitých úloh, ktoré sú kľúčové pri súčasnej kryptografii, zatiaľ úplne neobstoja, pretože stále ešte nie je známe, či sú tieto problémy skutočne natoľko zložité. Môže sa stať, že už zajtra niekto vymyslí spôsob ako efektívne rozložiť číslo na prvočísla. Jedinou otázkou potom bude, či je Shorov kvantový algoritmus stále ešte rýchlejší, alebo nie. Odhliadnuc od tejto otvorenej otázky z teórie zložitosti, predsa len existuje akýsi dôvod, prečo by kvantové počítače mohli byť užitočné. Postreh *Richarda Feynmana* a iných o tom, že kvantové systémy nedokážeme efektívne simulovať na klasických počítačoch je stále pravdivý. Kvantový počítač by nám umožnil prekonať istú výpočtovú bariéru a pomohol nám riešiť úlohy z kvantovej fyziky používajúc priamo jej metódy. Simulácie a modelovanie majú aj praktický dosah, t.j. uplatňujú sa aj mimo samotnej fyziky. Napríklad pri výpočtoch vlastností a charakteristík zložitých molekúl, ktoré potenciálne môžu slúžiť ako lieky, alebo urýchľovať chemické reakcie pri výrobe nejakých materiálov, atď.

V neposlednom rade myšlienka kvantových počítačov podnietila základný výskum jednej zo základných teórií nášho sveta – kvantovej fyziky, ktorú dnes vidíme v úplne inej rovine ako ju videli jej tvorcovia. Takisto podnietila experimentálnu snahu o presnejšiu manipuláciu s jednotlivými kvantovými objektmi, ktorá sa v budúcnosti môže hodiť napríklad pri výrobe presnejších meracích zariadení. Pri zmenšovaní nakoniec určite narazíme na atómy, resp. jednotlivé častice. Vôbec pritom nemusíme využiť celý potenciál ponúkaný kvantovou teóriou, ale iba niektoré jej črty (podobne ako aj pri tranzistore). Na bežné počítanie nepotrebujeme vytvárať superpozície. Kvantové počítače dokážu všetko, čo dokážu aj klasické a keď sa vzdáme snahy využívať kvantový paralelizmus, tak vyvinuté techniky pri manipuláciách s atómmi, iónmi, alebo supravodičmi si nájdu svoje využitie. Veľmi pravdepodobne raz postavíme aspoň klasický počítač používajúci jednotlivé častice na uchovávanie a spracovanie informácie. Ktorá z techník, resp. ktorá častica alebo aký polovodič v tomto súboji nakoniec zvíťazí je dnes neznáme. Budúcnosť bude určite plná prekvapení.

## VII. Problém merania, princípy a informácia

*Skôr ako pochopíme kvantovej fyzike, budeme musieť spojiť jej abstraktnosť s našim bežným vnímaním reality, t.j. s niečím čo cítime a čomu si myslíme, že rozumieme. Dnes nám chýbajú jasné a pochopiteľné princípy (tzv. Uhrprinzip). Aká je úloha informácie v tomto snažení?*

Istým znakom nášho pocitu, že nejakej fyzikálnej teórii rozumieme, je schopnosť túto teóriu zhrnúť do zopár základných tvrdení, ktoré učene (a možno aj trochu nadnesene) nazývame *princípmi*. Napríklad termodynamiku, t.j. náuku o teple a tepelných strojoch, charakterizujú dva princípy: 1) *energia* uzavretého systému *sa zachováva* a 2) *entropia* uzavretého systému *neklesá*. Prvý z týchto princípov obmedzuje vývoj systému kvantitatívne a zabraňuje nám skonštruovať *perpetum mobile*. Druhý princíp určuje kvalitatívne smerovanie vývoja a hovorí nám, ktoré procesy v prírode nepozorujeme. Ak nafilmujeme rozbitie pohára a pustíme tento film naopak, tak proces, ktorý vidíme (t.j. sformovanie pohára z črepov) v prírode nikdy nespozorujeme. Princíp narastania entropie tento proces zakazuje a hovoríme o nevratných dejoch.

Asi každý sa už stretol so základnými princípmi špeciálnej teórie relativity, t.j. *princípom relativity* a *princípom konštantnosti šírenia sa svetla*. Princíp relativity nám hovorí, že pozorovatelia popisujú udalosti rovnako bez ohľadu na to, či sa pohybujú, alebo nie, t.j. pre obidvoch platia tie isté fyzikálne zákony, tie isté rovnice. Iba konkrétne hodnoty polohy, času, rýchlosti, hmotnosti, energie a iných fyzikálnych veličín pre pozorované objekty sú pre rôznych pozorovateľov rôzne. Inými slovami: pre pozorovateľa stojaceho na stanici a pozorovateľa v idúcom vlaku má okolo letiaca vrana rôzne rýchlosti. Druhý princíp nám hovorí, že jedine svetlo, resp. nehmotné častice (napr. fotóny), sú výnimkou z tohoto pravidla a majú pre oboch pozorovateľov stále tú istú rýchlosť rovnú rýchlosti svetla vo vákuu, čo je približne $c$ = 300 000 km/s.

*NIKTO JEJ ÚPLNE NEROZUMIE*

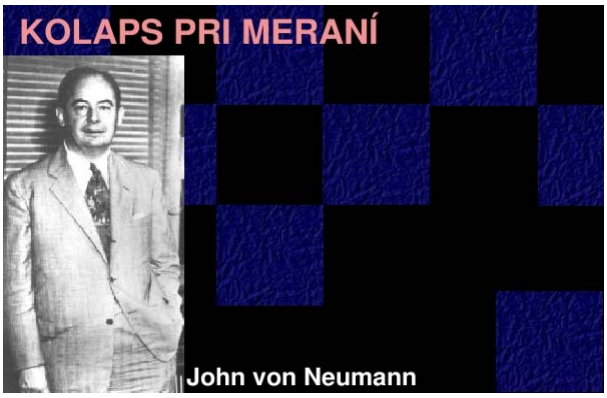
Jeden z dôvodov, prečo je kvantová fyzika menej známa a populárna ako napríklad teória relativity, je aj neprítomnosť takýchto jednoduchých princípov. Priamo to súvisí so známym tvrdením *Richarda Feynmana*, že nikto kvantovej fyzike úplne nerozumie. Vieme ako ju používať, ale nerozumieme jej. Sme v podobnej situácii ako pri varení. Máme kuchársku knihu (kvantovú fyziku), ktorá nám hovorí, čo máme robiť, ale prečo a ako vznikne z vajíčok omeleta nemusíme vedieť, a ani nevieme. Je otázne, či vôbec niečo ako princípy kvantovej fyziky niekedy budeme mať.

*PRESNÉ PREDPOVEDE*

Kvantová fyzika predpovedá deje s veľkou presnosťou. Jej hlavnou črtou, ktorú priamo pozorujeme, je kvantovanie hodnôt fyzikálnych veličín. Napríklad elektróny v atómoch môžu mať iba isté (diskrétne) hodnoty energie. Oveľa dôležitejšou črtou je však jej štatistický charakter. Kvantová fyzika nám neumožňuje predpovedať jednotlivý výsledok merania inak ako pravdepodobnostne. Táto vlastnosť úzko súvisí s tzv. *princípom superpozície* a *princípom neurčitosti*. Princíp superpozície je princípom, ktorý vyjadruje vlastnosti matematického popisu kvantových systémov. Nejde o princíp „fyzikálny", t.j. taký princíp, ktorý hľadáme, aby sme mohli povedať, že rozumieme. Princíp neurčitosti má zdanlivo oveľa bližšie k fyzikálnemu princípu, ale koniec koncov ide tiež iba o matematický princíp týkajúci sa obmedzení na presnosť súčasnej špecifikácie dvoch fyzikálnych veličín. Ak vieme určiť hodnotu jednej fyzikálnej veličiny úplne presne, tak hodnotu druhej veličiny poznáme iba nepresne a táto nepresnosť je daná práve formulkou, ktorá je obsahom princípu neurčitosti. Najznámejším príkladom tohoto princípu je trochu protiintuitívne poznanie, že pre kvantové častice nevieme presne naraz určiť ich polohu a rýchlosť.

*VEĽMI DISKUTOVANÁ TÉMA*

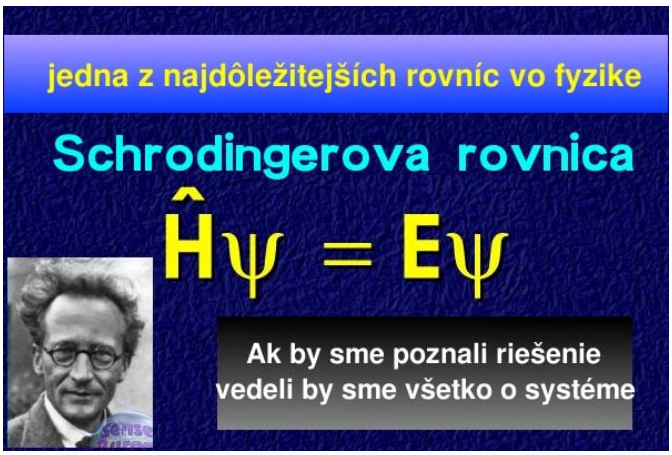
Na rozdiel od klasickej fyziky, v ktorej sa procesu merania nevenuje nejaká významná pozornosť a považuje sa viacmenej za triviálny akt, tak v prípade kvantového merania ide o veľmi diskutovanú tému. Prakticky od počiatku fyzikov trápila náhodnosť celého procesu, avšak až o niečo neskôr sa začalo diskutovať aj o probléme, čo sa vlastne s objektom pri meraní deje. Pri našej diskusii o dvojštrbinovom experimente sme si popísali tzv. vlnovo-časticový dualizmus (*Quark 2005/02*), ktorý v podstate ukazuje citlivosť interferencie na meranie. Pozorovaný interferenčný obrazec zmizol akonáhle sme mali možnosť povedať, ktorú cestu (štrbinu) si častica zvolila. Inými slovami, pri uskutočnení merania polohy častice, ktoré nám jednoznačne povie, ktorú cestu si častica vybrala, sa výsledok celého experimentu dramaticky zmení. To znamená, že pri kvantovom meraní sa s časticou udeje niečo dramatické. Všeobecné ponaučenie je, že vplyv merania kvantového objektu nemôžeme v žiadnom prípade zanedbať. Čo sa počas merania so systémom vlastne deje?




**Obr.1. John von Neumann.** *Pôvodom maďarský fyzik a matematik, ktorý sa veľkou mierou pričinil o modernú formuláciu kvantovej teórie.*

*DVA TYPY VÝVOJA*

Pôvodom maďarský fyzik *John von Neumann,* ktorý ako prvý matematicky jasne sformuloval kvantovú teóriu, rozlišoval dva rôzne typy (procesy) ako sa kvantový systém môže meniť. Prvý typ popisuje postupnú a hlavne úplne deterministickú zmenu kvantového stavu popísanú známou *Schrodingerovou rovnicou.* Druhým typom je práve zmena stavu pri meraní, ktorá sa z pohľadu času deje skokovo a naviac je úplne náhodná. Hovoríme, že systém pri meraní *skolabuje* do určitého stavu, ktorý závisí od nameranej hodnoty. Jediné, čo vieme povedať, je pravdepodobnosť, s akou tento proces nastane pre konrétny konečný stav, resp. konkrétnu nameranú hodnotu. Práve tento kolaps a táto dualita vývoja je pre niektorých fyzikov živnou pôdou na diskusie o úplnosti a univerzálnosti kvantovej fyziky. Stále je snaha vysvetliť celý proces merania pomocou Schrodingerovského vývoja, avšak doposiaľ každý takýto pokus stroskotal, pretože Schrodingerova rovnica vedie k deterministickému vývoju a pri meraní je zmena úplne náhodná. Tento vnútorný rozpor medzi oboma typmi vývoja sa zatiaľ nikomu nepodarilo prekonať.




**SCHRODINGEROVA ROVNICA**

Fyzika je bežne chápané ako veda, ktorá je plná vzorcov a človek zo školy neraz získa pocit, že celé jej umenie spočíva v úlohe nájsť a použiť ten správny vzorec. V skutočnosti vzorcov, resp. rovníc, ktoré sú dôležité, nie je až tak veľa a všetky vzťahy, ktoré sa naučíme sú odvodené zo zopár základných rovníc a platia pre špecifické situácie. Newtonova fyzika popisuje akýkoľvek pohyb všetkých telies a jej základ tvorí prakticky jediná rovnica, ktorá nám hovorí, že $F = m.a$ (sila=hmotnosť x zrýchlenie). Nič viac nepotrebujeme, aby sme popísali či už pád telesa na zem, alebo pohyb planét okolo Slnka. Táto rovnica nám popisuje akýkoľvek pohyb telies okolo nás. Albert Einstein nás naučil, že ide o rovnicu približnú a pre veľmi vysoké rýchlosti a energie platia úplne iné pohybové rovnice, tzv. *Einsteinove rovnice*. Svet elektriny a magnetizmu (vrátane celej optiky) úplne popisujú iba štyri *Maxwellove rovnice.* Pohybové vlastnosti kvantových systémov plne charakterizuje tzv. *Schrodingerova rovnica*, ktorá popisuje ako sa stav systému vyvíja v čase. Všetky tieto rovnice sú tzv. *diferenciálne rovnice*, ktoré popisujú ako sa vlastnosti skúmaných objektov menia vo veľmi krátkych časových škálach. Ak chceme uskutočniť nejaké užitočné predpovede, tak potrebujeme tieto rovnice vyriešiť. A práve táto úloha je nesmierne zložitou vo všetkých teóriach, kvantovú fyziku nevynímajúc. Vyriešiť Schrodingerocu rovnicu je jedným z kľúčov k pochopeniu vlastností kvantového sveta. Napriek tomu, že dnes ju vieme vyriešiť iba vo veľmi špecifických podmienkach a aj to poväčšine iba približne, tak využitím týchto riešení sa stretávame skutočne všade okolo nás. Napríklad pochopenie stability hmoty je toho príkladom, pretože podľa pohybových rovníc Newtonových a Maxwellových by elektróny prakticky v zlomku sekundy mali spadnúť do jadra, t.j. atómy by mali prakticky skolabovať. Schrodingerova rovnica ponúka síce ťažko stráviteľné, ale napriek tomu elegantné riešenie tohoto problému. Proces kvantového merania je zdá sa výnimkou z takéhoto modelu, pretože ide o proces, ktorý nie je riešením tejto rovnice.

**Model merania**

Štandardne si dnes meranie predstavujeme ako dôsledok interakcie meraného objektu a meracieho prístroja. Počas interakcie, ktorá predchádza samotnému odčítaniu výsledku, popísanej Schrodingerovským vývojom sa systém kvantovo previaže s meracím prístrojom. Vďaka tomu sa vytvoria veľmi silné korelácie medzi oboma systémami, t.j. previazanie vytvorené v procese interakcie nám zabezpečuje, že vlastnosti meracieho prístroja sú v priamom vzťahu s fyzikálnymi veličinami popisujúcimi

meraný systém. Merací prístroj je makroskopický objekt, z ktorého vlastností nakoniec odčítame nameranú hodnotu, pričom oba systémy skolabujú do určitého známeho stavu. Inými slovami namiesto samotného systému nakoniec premeriavame merací prístroj. Ako však vykonávame toto meranie?

Problém merania sme týmto modelom nevyriešili, iba sme ho posunuli o poschodie vyššie. Problémom zostáva úloha, ako odčítať hodnotu z meracieho prístroja. Takto postupujeme ďalej na vyššie a vyššie poschodia, až nakoniec skončíme niekde pri našej schopnosti uvedomiť si výsledok, resp. zmerať stav nášho vedomia. Tu však dnešná fyzika končí. Neostáva nám zatiaľ nič iné ako prijať kvantové meranie sprevádzané kolapsom ako fakt.

**DVOJŠTRBINOVÝ EXPERIMENT**

Ako príklad si spomeňme už diskutovaný dvojštrbinový experiment. Pri zisťovaní, ktorú štrbinu si častica zvolila, zisťujeme v podstate polohu tejto častice. Inými slovami snažíme sa „pohľadom" zistiť, kde sa častica nachádza. Aby sme „videli", tak si štrbiny osvetlíme a pozorujeme či sa svetlo rozptyľuje alebo nie. Pri objektoch, s ktorými sa bežne stretávame, takéto osvetlenie prakticky nezmení ich polohu. Avšak pre malú časticu je pohltenie fotónov svetla veľkou udalosťou, ktorá mení jej vlastnosti. My nakoniec nepozorujeme priamo časticu, ale iba odrazené fotóny. V prípade, že spozorujeme rozptýlenie, tak vieme, ktorú cestu si častica vybrala. Toto meranie je úplne v súlade s popísaným modelom merania, v ktorom namiesto priameho merania systému (častice) uskutočňujeme meranie iného systému (fotónov), ktoré vlastne tvoria súčasť meracieho zariadenia.

*METÓDA HMATANIA*

Pri zaznamenávaní samotného výsledku tohoto experimentu, t.j. interferenčného obrazca, tiež meriame polohu častice, ale úplne iným spôsobom. Namiesto „pozerania" tentokrát používame skôr metódu akéhosi „hmatania", resp. častice zachytávame v detektoroch. Po dopade častice do detektora sa v detektore spustí celá lavína procesov, ktoré tento veľmi slabý jav pretransformujú do makroskopicky pozorovanej zmeny, akou je napríklad zapípanie detektora, prípadne očernenia časti fotografickej platne. Častica môže vyvolať v detektore prúd v nejakej časti elektronického obvodu, prípadne chemickú reakciu, alebo nejaký iný jav, ktorý vieme priamo odpozorovať našimi zmyslami. Pri takýchto typoch merania sa kvantová častica stáva súčasťou meracieho zariadenia a niekedy sa úplne zničí. V podstate ju strácame a hovoríme, že takýto typ merania polohy je *deštruktívnym meraním*. Každé meranie obsahuje tento element deštrukcie, ale v istých prípadoch, keď v skutočnosti robíme meranie na úplne inom systéme, prichádza k deštrukcii iného fyzikálneho systému, než ktorého vlastnosti meriame. Napríklad pri meraní polohy častice pozeraním prichádza k deštrukcii rozptyľovaných fotónov. Stále však v procese merania máme kolaps, ktorého filozofické dôsledky sú v nemalej miere príčinou existencie rôznych interpretácií kvantovej fyziky.

Fyzikálna teória je v podstate súhrnom pravidiel, ktoré nám hovoria akú informáciu o systéme máme k dispozícii a ako s touto informáciou máme pracovať. Jej úlohou je jednak informáciu predpovedať a jednak ju spracovávať. Je zrejmé, že informácia je fyzikálna, t.j. akékoľvek narábanie s informáciou (prenos informácie, uchovanie informácie, spracovanie informácie, alebo zmena informácie) je priamo spojené s reálnymi fyzikálnymi procesmi, a teda obmedzené platnými fyzikálnymi zákonmi a princípmi. Kvantová teória informácie sa pokúša tento pohľad obrátiť a chápať fyzikálny popis, resp. fyzikálne princípy ako princípy týkajúce sa spracovania informácie. Inými slovami pýtame sa, akým spôsobom obmedzenia na narábanie s informáciou určujú charakter fyzikálneho objektu, teórie. Niektorí fyzici si myslia, že práve tento pohľad nám umožní zrozumiteľne sformulovať základné princípy kvantovej fyziky.

*KOLAPS PRI MERANÍ*

Teória informácie nám ponúka zaujímavý pohľad aj na *proces merania* (pozri predchádzajúcu časť v *Quarku 2005/08*). Z abstraktenjšieho pohľadu je meranie spôsob akým kladieme prírode otázky a získavame o nej informácie. Namerané výsledky nám sprostredkúvajú informáciu (odpovede na otázky), s ktorou fyzikálna teória ďalej pracuje. V jednej z predošlých častí sme sa naučili, že kvantové stavy, resp. kvantovú informáciu, nevieme presne skopírovať. Teraz si ukážeme ako z tohoto faktu vyplýva, že pri meraní sa nevyhnutne musí stav kvantového systému zmeniť.

Predstavme si, že pri meraní získame informáciu o polohe častice, ale samotnú časticu pritom vôbec nezmeníme, t.j. stále je v tom istom stave. V ďalšom meraní určíme aj jej rýchlosť a opäť jej stav zostáva nezmenený. Takto postupne môžeme zistiť úplne celú informáciu o tejto častici, t.j. dokážeme povedať v akom stave sa častica nachádza, vieme všetky jej vlastnosti. Avšak zistenie stavu častice, ak máme iba jej jedinú kópiu, je v rozpore s nemožnosťou kvantového klonovania. Akonáhle totižto zistíme stav častice, tak nám nič nebráni pripraviť si takýchto častíc ľubovoľne veľa a teda uskutočniť kopírovanie. Celý tento postup však bezchybne funguje iba v prípade, ak pracujeme s objektami popísanými klasickou fyzikou. Pre kvantové systémy nielen takéto, ale akékoľvek kopírovanie nie je možné. Výsledkom tejo úvahy je, že ak sa pri meraní stav systému nemení, tak potom je možné kopírovať, čo je ale v rozpore s vlastnosťami kvantovej fyziky. Preto sme nútení prijať záver, že meranie kvantového systému nevyhnutne mení jeho stav. Inými slovami: akýkoľvek zisk informácie o kvantovom systéme je podmienený zmenou stavu tohoto systému a táto zmena je okamžitá. Trochu dramatickejšie hovoríme o *kolapse stavu* pri meraní.

Z pohľadu informácie je stav systému ideálne skompresovaná informácia o kvantovom systéme. Stav predstavuje maximum informácie, ktoré o systéme môžeme mať a ktoré v danej situácii aj máme. V prípade kvantových stavov sa preto niekedy používa trochu diskutabilný pojem *kvantová informácia* ako synonymum pojmu stavu fyzikálneho systému. Nejde pritom o nejaký nový typ informácie, ale iba o informáciu, ktorá je v kvantovom stave obsiahnutá, resp. ktorú používame pri jeho popise. Z takéhoto pohľadu je kolaps pri meraní iba náhlou zmenou našej vedomosti o systéme. So systémom samotným sa pritom nedeje nič dramatické, iba naša vedomosť o ňom (t.j. jeho stav) sa mení.

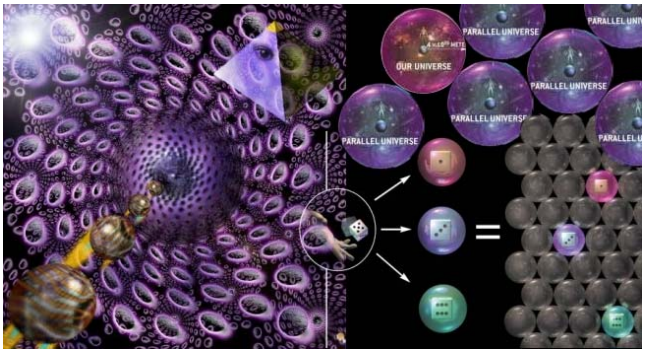
*CENTRÁLNE POSTAVENIE*

Už pred niekoľkými desaťročiami americký fyzik *John Archibald Wheeler* predpokladal, že pojem informácie by mal mať centrálne a zjednocujúce postavenie vo fyzikálnych teóriach. To, čo nazývame realitou sa skladá z otázok, ktoré sa pýtame, a z odpovedí, ktoré dostávame, t.j. z informácie. Skutočný význam informácie nielen vo fyzike, ale aj v iných oblastiach dnes postupne odhaľujeme. Jednoduché porovnanie potrebnej a dostupnej informácie mnohokrát vyrieši úlohu, ktorej priame riešenie je inak veľmi komplikované (*pozri rámček*). V predošlom odstavci sme si ukázali, ako sa jednoduchý princíp o neklonovaní kvantovej informácie môže použiť pri argumente, že kvantový stav nevyhnutne pri meraní skolabuje.

**Váženie guličiek a informácia.**
Všetci sme sa asi už stretli s úlohami typu: *Majme 16 úplne rovnakých guličiek, z ktorých jedna má inú hmotnosť. Na tri váženia určite, ktorá to je. Vieme povedať, či je ťažšia, alebo ľahšia?* Teória informácie nám pomôže zistiť, či sa nám vôbec oplatí nejaké riešenie hľadať, t.j. či riešenie vôbec existuje. Začnime prvou časťou úlohy, t.j. otázkou, ktorá z guličiek má inú hmotnosť? Očíslujme si guličky číslami od 1 po 16. Označme si situáciu, keď gulička číslo 1 má inú hmotnosť ako ostatné, ako stav $g_1$. Podobne označme stavy $g_1, ..., g_{16}$, t.j. spolu máme 16 rôznych stavov a našou úlohou je zistiť, o ktorý z týchto stavov konkrétne ide. Aby sme toho boli schopní, tak z meraní musíme získať aspoň $\log_2 16=4$ bity informácie (logaritmus transformuje počet možností na počet bitov informácie). Váženie má tri možné výsledky: *je to ťažšie (T)*, *je to ľahšie (L)*, *rovnaká hmotnosť (R)*. Pri jednom vážení teda dostávame jednu z troch možných odpovedí ($\log_2 3$ bitov informácie), čo samozrejme nepostačuje na určenie, ktorá zo 16 guličiek má inú hmotnosť. Pri dvoch váženiach sú možné výsledky *TT, TL, TR, LT, LL, LR, RT, RL, RR*, t.j. spolu 3x3=9 možností. Pri troch váženiach je už počet možných výsledkov 3x3x3=27, čo úplne postačuje na určenie, o ktorú zo 16 guličiek ide, pretože $\log_2 16 < \log_2 27$, čo znamená, že tri váženia poskytujú v princípe dostatok informácie na určenie guličky. Súčasne vidíme, že guličiek môže byť najviac 27. Ak sa však naviac spýtame aj na to, či je táto gulička ľahšia, alebo ťažšia ako ostatné, tak potom guličiek môže byť maximálne 27/2=13, pretože počet možností potencionálnych riešení je dvojnásobkom počtu guličiek. Takýto informačný pohľad na problém nám ešte nezaručuje, že riešenie určite existuje a stále musíme nájsť konkrétny spôsob váženia. Informácia nám iba pomáha vylúčiť situácie, kedy určite riešenie existovať nemôže. Podobná úvaha, t.j. jednoduché porovnanie potrebnej informácie s informáciou, ktorú máme k dispozícii, sa dá použiť aj pri iných úlohách podobného typu.

Práve táto vlastnosť, t.j. *nemožnosť kvantového klonovania,* je jedným z horúcich kandidátov na jeden zo základných princípov kvantovej fyziky. Ďalšou typickou vlastnosťou kvantovej fyziky je kvantové previazanie, ktoré v spojení s kolapsom pri procese merania tvorí základ tzv. Einstein-Podolski-Rosen paradoxu (*Quark 2005/01*) a otvára možnosť komunikácie nadsvetelnou rýchlosťou iba s pomocou vykonávania meraní. Kvantová teória nám nehovorí nič o tom, aký čas taký kolaps trvá a považujeme ho za okamžitý. Ako sme si povedali, tak zmeraním jednej častice z previazaného páru častíc, vieme okamžite povedať stav druhého systému, do ktorého táto častica skolabuje. Aj pri meraní na jedinej častice kolabujú obidve. Hlavne kvôli tejto vlastnosti hovoríme o "previazaní" medzi týmito časticami. Výberom merania na jednej častici dokážeme takto pripravovať rôzne stavy druhej častice, ktorá je ľubovoľne vzdialená. Práve okamžité ovplyvňovanie druhého systému pri meraní je zdrojom špekulácií o okamžitom prenose informácie na ľubovoľné vzdialenosti. Napriek tomu nevieme tento jav využiť na prenos informácie nadsvetelnou rýchlosťou.

Výsledky našich meraní sú náhodné a preto, ak zvolíme meranie *X,* tak druhá častia z previazaného páru je v jednom z náhodných stavov $x_1$, $x_2$ a nevieme dopredu, že v akom. Preto výberom merania *X* druhá častica skolabuje do akejsi zmesi stavov $x_1$ a $x_2$. Každý so stavov tvorí istú časť v tejto zmesi. Voľbou iného merania *Y* sme na tom podobne a častica sa premeria v zmesi stavov $y_1$ a $y_2$ v nejakom inom pomere. Kvantová fyzika však zaručuje, že tieto dve zmesi nevieme rozlíšiť a predstavujú pre nás ten istý kvantový stav. Vďaka tejto vlastnosti hovoríme o princípe *nemožnosti signalizácie pomocou meraní,* ktorý je jedným z ďalších kandidátov na základný princíp kvantovej fyziky motivovaných teóriou informácie.




**Obr.1. Jeden alebo mnoho svetov?** *Ak hodíme kvantovú kocku, tak podľa mnohosvetovej intepretácie nastanú všetky možné výsledky, ale každý v inom z paralelných vesmírov.*

*PRINCÍPY A INTERPRETÁCIE*

Princípy teórie relativity sa dajú tiež chápať ako obmedzenia na narábanie s informáciou: 1) i*nformácia je relatívna* a 2) *informácia sa šíri maximálne rýchlosťou svetla*. Prvý z týchto princípov treba v tomto informačnom balení ešte trochu upresniť, ale nebudeme sa tomu teraz venovať. V kvantovej fyzike sme sa zatiaľ stretli tiež s dvoma princípmi: *nemožnosť klonovania* a *nemožnosť signalizácie pomocou meraní*. Tieto princípy ešte nepostačujú na úplné charakterizovanie kvantovej fyziky a je otázkou, aké ďalšie princípy a koľko, je ešte treba pridať. Niektorí fyzici navrhujú princípy založené na kryptografii, t.j. na zabezpečení obsahu informácie. Otázka je však ešte stále otvorená. Chýbajúce princípy otvárajú množstvo filozofických otázok ohľadne interpretácie kvantovej fyziky, t.j. snáh o vysvetlenie, čo vlastne kvantová fyzika je, resp. čo popisuje. Najhorúcejšou témou pri diskusiách je práve problém merania, resp. kolapsu. Vo fyzike nie sme zvyknutí na takéto vskutku okamžité zmenu. Ako sme si už povedali, tento proces je v príkrom rozpore s postupným vývojom popísaným Schrodingerovou rovnicou. Preto nie

je divu, že rôzne interpretácie sa venujú práve vysvetleniu, resp. pochopeniu procesu kvantového merania. Spolu máme dnes asi osem rôznych interpretácii kvantovej teórie. My si však spomenieme iba dve.

Najznámejšia a najpoužívanejšia je tzv. *kodaňská interpretácia*, ktorá vyjadruje názor tvorcov kvantovej mechaniky z dvadsiatych rokov 20.storočia. Akýmsi mottom tejto interpretácie je, že *vieme odpovedať iba na experimentálne položiteľné otázky*. Vďaka tomu vyradíme množstvo filozofických otázok o zmysle a fungovaní kvantového sveta, o rozdieloch medzi klasickým a kvantovým svetom, atď. Z pohľadu kodaňskej interpretácie je proces merania výsledkom interakcie kvantového mikrosveta a klasického makrosveta. Podobne ako sme si to popísali v minulom čísle. Alternatívou je tzv. *mnohosvetová interpretácia*, ktorá hovorí, že pri meraní nastanú všetky možné výsledky, ale každý v inom vesmíre. My pozorujeme kolaps v závislosti od toho, v ktorom z týchto svetov sa nachádzame. Táto interpetácia môže znieť trochu bizardne, ale nemáme možnosť ju ani vyvrátiť, ani potvrdiť a je dnes veľmi populárna. Najmä pre ľudí, ktorý sa snažia aplikovať princípy kvantovej fyziky na vesmír ako celok. Takže možno niekde existuje akási vaša kópia, ktorá sa však pri čítaní nedostala až sem.

Situácia je taká, že kvantovú fyziku vieme používať a dostávame zaujímavé výsledky, aj bez prijatia nejakej konkrétnej interpretácie. Snaha o jej nájdenie je však veľmi dôležitá z pohľadu uspokojenia našej túžby rozumieť, prípadne dostať sa k širšej triede teórii, ktoré potencionálne môžu kvantovú teóriu rozšíriť. Práve informačno-teoretický pohľad na kvantovú fyziku a fyziku celkovo môže priniesť mnoho zaujímavých poznatkov a priblížiť kvantovú teóriu širšiemu publiku. Momentálne hrá informácia vo fyzike stále iba okrajovú úlohu, ale v budúcnosti sa jej postavenie môže zmeniť.

**VIII. Svetlo, fotóny, polarizácia.**

*Táto časť bude jednoduchá a menej abstraktná ako predchádzajúce. Zameriame sa na jav polarizácie, ktorý vieme popísať aj bez znalosti kvantovej fyziky, ale popritom ide o čisto kvantovú vlastnosť svetla, resp. fotónov. Polarizáciu používame pri fotografovaní, v 3D kine, v tenkých ("flat") LCD monitoroch, atď.*

Popisom a pochopením svetla sa zaoberali takmer všetci známy fyzici. *Isaac Newton* ho považoval za prúd častíc, neskôr však prevládol názor, že svetlo je vlnením. Zdalo sa, že konečnú bodku za týmto sporom dal *James Clark Maxwell*, ktorý sformuloval teóriu spájajúcu elektrinu a magnetizmus. Podľa tejto teórie je svetlo špeciálnym prípadom tzv. elektromagnetického vlnenia. Začiatok 20.storočia však naše chápanie svetla úplne zmenil. Jednoduchá otázka *čo je svetlo* je jednou z najkomplikovanejších otázok a ešte stále nemáme k dispozícii uspokojivú odpoveď. Neznamená to však, že by sme vôbec svetlu nerozumeli. Poznáme presne zákonitosti, ktorými sa riadi. Naše "nechápanie" je priamym dôsledkom našich problémov so základnými zákonitosťami kvantového sveta.

Koncom 19.storočia sa ľudia odpozorovali závislosť, ktorá popisovala aké svetlo vyžarujú zohriate telesá, resp. ako vyžarovanie závisí od teploty telesa (tzv. *zákon žiarenia čierneho telesa*). Akékoľvek pokusy o vysvetlenie tejto závislosti však stroskotali a tzv. klasická fyzika narazila na vážny problém (tzv. *ultrafialová katastrofa*), pretože jej predpovede boli v úplnom rozpore s tým, čo sa pozorovalo. Nastal čas na radikálne zmeny. *Max Planck* vyslovil na prelome storočí na tú dobu veľmi zvláštnu domnienku, že svetlo sa vyžaruje iba v malých, viac už nedeliteľných, kvantách energie. Použijúc tento predpoklad Max Planck uspokojivo a úplne presne odvodil zákon žiarenia čierneho telesa, čím položil základný kameň kvantovej fyziky. Tieto kvantá energie boli neskôr pomenované *fotónmi* a táto predstava nám umožnila pochopiť mnoho iných javov, s ktorými si klasická fyzika nevedela poradiť.

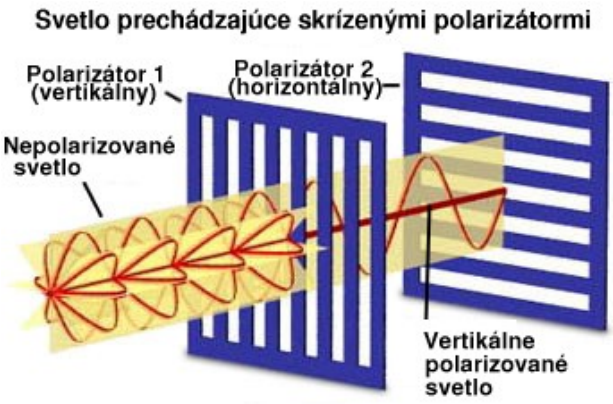
V učebniciach dnes nájdeme, že svetlo je prúdom fotónov, t.j. kvánt energie. Tieto častice však majú aj charakteristiky ako vlnová dĺžka a frekvencia, ktoré vyjadrujú energiu jednotlivých fotónov podľa známeho Planckovho vzťahu *energia=h* x *frekvencia,* kde sme použili označenie *h* pre tzv. Planckovu konštantu. Z nášho pohľadu rôzna frekvencia (energia) fotónov zodpovedá rôznym farbám, t.j. zelený receptor v našom oku je citlivý iba na dávku kvanta energie zeleného svetla. Bohužiaľ jediný fotón (ide skutočne o veľmi malú dávku energie) naše oko nedokáže zachytiť a vnem vzniká iba ak je počet fotónov dostatočne veľký.

**Polarizácia svetla v klasickej fyzike**

Vlnová dĺžka, resp. frekvencia fotónov priamo súvisí s chápaním svetla ako elektromagnetického vlnenia. Podľa tejto klasickej teórie je svetlo súčasným prejavom kmitania elektrického a magnetického poľa. Elektrické, aj magnetické pole je však vektorovou fyzikálnou veličinou, t.j. okrem svojej veľkosti majú tieto polia aj určitý smer a pri pohybe svetla kmitajú v nejakom smere (vždy kolmom na smer šírenia sa svetla). So smerom vektora elektrického poľa spájame pojem polarizácie. Polarizácia je teda vektorová fyzikálna veličina, ktorá udáva, v ktorom smere svetlo "kmitá". Naše oko na polarizáciu svetla nie je citlivé a aby sme javy spojené s polarizáciou mohli pozorovať, potrebujeme pomoc iných zariadení. Polarizátor je špeciálny materiál, ktorý prepúšťa iba svetlo istej polarizácie. Prejavuje sa to tým, že ak sa pozeráme na svetelný zdroj cez polarizátor, tak do nášho oka dopadne menej svetla (menej fotónov), ako keď polarizátor nepoužijeme. Čiže polarizátor "ztemňuje", t.j. *filtruje* svetlo. Preto ho niekedy nazývame aj polarizačným filtrom.

**Polarizátory, polaroidy**

Bežné svetlo je v skutočnosti zmesou svetiel rôznych polarizácií a nekmitá v žiadnom význačnom smere. Hovoríme, že takéto svetlo je nepolarizované. Avšak akonáhle položíme svetlu do cesty polarizátor, tak za ním už nájdeme svetlo dokonale spolarizované. Zdalo by sa, že polarizátor nám vyberie iba tú časť svetla, ktoré kmitá v tom správnom smere, a všetky ostatné pohltí. Ale nie je to také jednoduché. Ak by sme totižto postavili do cesty ďaľší (taký istý) polarizátor (iba inak natočený), tak stále by nejaké svetlo prechádzalo. Zistili by sme, že množstvo prejdeného svetla závisí na natočení druhého polarizátora, alebo trochu matematickejšie: od uhla pootočenia druhého polarizátora vzhľadom k prvému.




**Obr.1. Skrížené polarizátory.**

Predpokladajme, že svetlo, ktoré dopadá na druhý polarizátor má intenzitu $I_1$ . Intenzita svetla prechádzajúceho je daná vzťahom $I_2 = I_1 \cos^2\alpha$ , kde α je uhol medzi prvým a druhým polarizátorom. Vidieť (pozri obr.1), že intenzita je nulová iba pre uhly α=90 a 270 stupňov, t.j. keď sú polarizátory navzájom kolmé (skrížené). Naopak intenzita sa nemení ($I_2=I_1$), ak je druhý polarizátor nasmerovaný rovnako ako prvý alebo je otočený presne naopak, t.j. pre uhly α=0 a 180 stupňov. Ako doležitý výsledok dostávame, že dva skrížené polarizátory neprepúšťajú žiadne svetlo (pozri obrázok). Presne polovica svetla prejde druhým polarizátorom, ak uhol α = 45 stupňov ($I_2=I_1/2$).

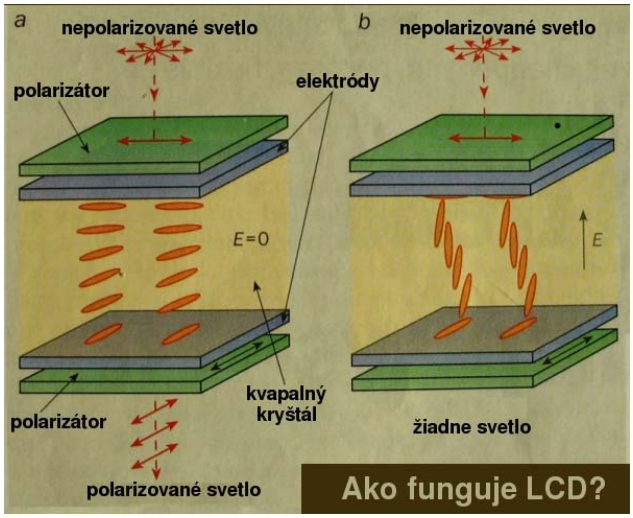
**Obr.2.** *Polarizovaný odraz svetla od vodnej hladiny, alebo vozovky.*

Tento jav napríklad využívajú slnečné okuliare, ktoré vďaka polarizačným sklám (filtrom) dokážu odfiltrovať svetlo odrážajúce sa od vodnej hladiny. Odrazené svetlo sa od povrchu vody je polarizované rovnobežne s vodnou hladinou (podobne aj od asfaltovej cesty, skla, alebo snehu). Stupeň polarizácie závisí od uhla pod akým svetlo na povrch dopadá. Úplná polarizácia nastáva, ak sa svetlo od povrchu iba odráža, t.j. keď dopadá pod tzv. *Brewsterovým uhlom*, ktorý je daný vzťahom $\theta = \arctan(n_{material}/n_{vzduch})$. Pripomeňme, že $n_{material}$ označuje index lomu materiálu, ktorý je pomerom rýchlosti svetla vo vákuu (cca 300 000 km/s) ku rýchlosti šírenia sa svetla v danom materiáli. Pre sklo je $n$=1.5 a θ=56.3 stupňa. Pre vodu $n$=1.33 a kritický uhol má hodnotu θ=53 stupňov. Prakticky to znamená, že najviac trblietania na hladine by sme mali vidieť, ak sa pozeráme pod 53 stupňovým uhlom.

S polarizáciou sa možeme stretnúť napríklad aj pri návšteve 3D kina (pozri box). Takisto pri fotografovaní vďaka polarizačným filtrom dosiahneme obrázky, ktoré voľným okom nikdy neuvidíme. Správnym nastavením filtra dokážeme odstrániť čiastočnú polarizáciu modrej oblohy (oslňujúci lesk) a dostaneme krásne modrú oblohu. Fungovanie a princíp LCD monitorov takisto využíva polarizačné vlastnosti svetla. Polarizáciu vnímajú aj niektoré zvieratá. Napríklad mravce, alebo včely si polarizáciou pomáhajú pri navigácii. Kedysi vraj aj vikingovia na svojich ďalekých cestách po severných moriach využívali tzv. “slnečný kameň” (pravdepodobne polarizačný filter), ktorý im aj vo veľmi zlej viditeľnosti umožňoval lepšiu orientáciu. Nemenej zaujímavé možnosti nám polarizácia ponúka pri kvantovom popise svetla, kde namiesto o vlnení hovoríme o časticiach - fotónoch, z ktorých sa svetlo skladá.

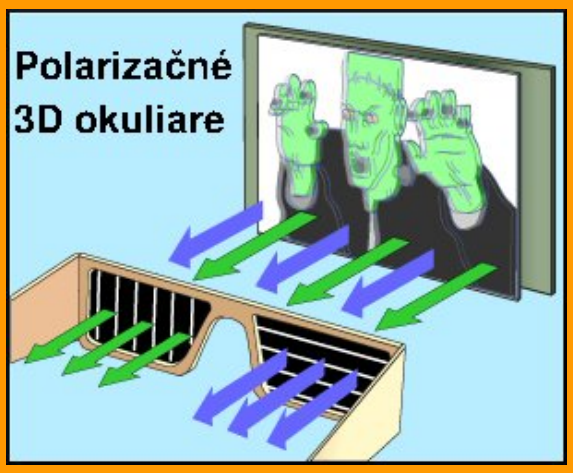
**Polarizácia kvantovo**

Klasický obraz svetla a polarizácie sa nám rýchlo rozplynie, keď prijmeme predstavu fotónov. Ak máme iba jediný fotón, tak elektromagnetické pole pre tento jediný fotón neexistuje. Napriek tomu má každý fotón okrem svojej frekvencie (energie) a hybnosti, aj istú polarizáciu. Ak by tomu tak nebolo, tak by sme mali problém s mnohými experimentmi, ktoré vieme vysvetliť pomocou klasickej predstavy o svetle a jeho polarizácii. V kvantovej teórii namiesto o smere polarizácie fotónu hovoríme o polarizačnom stave fotónu. Poďme sa pozrieť, čo sa vlastne deje s jediným fotónom v polarizátore.




**Obr.4. Ako funguje LCD?** *Nepolarizované svetlo prechodom cez polarizátor a priesvitnú elektródu vstupuje do kvapalného kryštálu, v ktorom sa jeho polarizácia postupne stočí do kolmého smeru. Po prechode druhej elektródy prechádza polarizované svetlo skríženým polarizátorom. Ak na elektródy pripojíme napätie, tak molekuly kvapalného kryštálu sa natočia do smeru poľa, čo spôsobí, že polarizácia sa počas prechodu nezmení. Takto natočené molekuly nijako polarizáciu fotónu neovplyňujú a teda pri zapnutí napätia svetlo druhým polarizátorom neprejde. Tento jav sa využíva jednak na displejoch kalkulačiek a jednak v moderných plochých obrazovkách*

**Ako funguje 3D kino IMAX?**
Človek vníma svet okolo seba trojrozmerne vďaka dvom veciam. Po prvé "priestor je trojrozmerný" a po druhé "máme dve oči". Pravé a ľavé oko vidia každé trochu iný obraz. Až skladaním týchto obrazov, ktoré vnímame oboma očami, náš mozog produkuje trojrozmerný obraz sveta. V klasickom kine máme problém s bodom číslo jeden, t.j. obraz ktorý vnímame je dvojrozmerný (premietacia plocha). IMAX technológia rieši problém ako vrátiť tretí rozmer nafilmovanej realite.




Princíp je vskutku jednoduchý a práve v tom je jeho genialita. Na filmové plátno sa vysielajú dva obrazy a našou úlohou je ich skladať. K tomu však potrebujeme špeciálne okuliare, ktoré zabezpečia, že každé naše oko vníma iba jeden z týchto obrazov. Svetlá oboch obrazov kmitajú (polarizácia) v navzájom kolmých smeroch. Sklíčka týchto okuliarov sú z takého materiálu, ktorý k Vášmu oku prepustí iba jeden obraz, t.j. jedno z kmitajúcich svetiel. Takto naše oči dostávajú presne také isté vnemy, ako keby sme boli v reálnom priestore, t.j. pravé a ľavé oko majú mierne odlišný obraz, z ktorého si hravo výsledný trojrozmerný obraz poskladáme. Ak by sme si v kine okuliare zložili, tak vidíme iba rozmazaný obraz, čo je dosledkom toho, že oboma očami vnímame obidba vysielané obrazy.

V kine IMAX je však všetko trocha iné ako v normálnom kine. Pri natáčaní 3D filmu sa nepoužíva obyčajná kamera. Kamera má "dve oči", t.j. dve blízke šošovky snímajú filmovaný predmet a film sa zaznamenáva na dve pásky. Pri premietaní vlastne premietame filmy dva, kaž pre jedno oko. Hmotnosť takejto kamery je zhruba 109 kg a pri natáčaní vraj robí hluk ako motorová píla. Ozvučenie filmu sa preto musí robiť až dodatočne. Ak by ste si zblízka pozreli premietaciu plochu IMAX kina, tak si určite všimnete množstvo dierok, do ktorých kľudne vopcháte svoj prst. Tieto dierky nemajú žiadny efekt na kvalitu obrazu, ale skrývajú zvukové reproduktory, ktoré potom umožnujú lepšiu priestorovosť zvuku, a teda lepší celkový 3D dojem.

Vezmime si dva rovnaké polarizátory (podobne ako na obr.1), postavme ich za sebou a skúsme či fotón prejde cez obidva polarizátory, alebo nie. V prípade, že sú polarizátory potočené navzájom o 90 stupňov, tak fotón nikdy neprenikne (polarizátory sú navzájom skrížené). Spôsobené je to tým, že fotón ktorý prejde cez prvý polarizátor sa automaticky nachádza v stave určenom týmto polarizátorom. Označme si tento stav ako vertikálny stav polarizácie fotónu. Fotón, ktorý prenikne a dopadá na druhý polarizátor má vertikálnu polarizáciu, a preto druhý, horizontálne nastavený polarizátor, tento fotón zastaví. Ak meníme pootočenie prvého polarizátora, tak pozorujeme, že niekedy fotón prejde, a niekedy nie. Pravdepodobnosť zachytenia fotónu je daná polarizačným stavom, ktorý je určený nastavením prvého polarizátora vzhľadom k horizontálnej rovine. Okrem vertikálne polarizovaných fotónov majú všetky ostatné istú pravdepdobnosť, že ich polarizátor prepustí. Táto náhodnosť je principiálna a

polarizátor si skutočne "svojvoľne" vyberá, či fotón prepustí, alebo nie. Jediné pravidlo, ktoré dodržuje sú pravdepobnosti presne určené kvantovou fyzikou.

Teraz si popíšeme kúzelnícky trik, ako vložením kúska priesvitnej hmoty (polarizátora) donútiť svetlo (fotóny) prejsť aj dvoma navzájom skríženými polarizátormi. Vložme medzi skrížené polarizátory ďalší polarizátor pootočený o 45 stupňov. Fotón má 50% šancu, že ním prenikne, avšak ak prenikne, tak je polarizovaný diagonálne a teda má istú šancu, že prenikne aj druhým, horizontálne nastaveným, polarizátorom. Jeho šanca je opäť 50%. Ak pošleme 100 fotónov, tak 50 prenikne cez novo vložený polarizátor a ďalšia polovica z nich, čo je približne 25 fotónov, prenikne aj posledným polarizátorom. Po vložení ďalšieho polarizátora skrížené polarizátory prepustia 25% z fotónov, ktoré sa dostali za prvý, vertikálne nastavený polarizátor. V istom zmysle teda vieme pomocou vloženia polarizátora urobiť svieti z nesvieti, čo je pre nezasvätených výsledným efektom nášho kúzla. V skutočnosti však nerobíme nič iné, iba využívame jeden zo základných princípov kvantovej teórie, *princíp superpozície.*

**Kvantová informatika**

Polarizácia fotónu je ideálnym prototypom elementárnej jednotky kvantovej informatiky, tzv. kvantového bitu (o kvantovej informatike sme písali v predchádzajúcich častiach). Logické hodnoty 0/1 sú reprezentované dvoma polarizačnými stavmi, napr. horizontálna/vertikálna polarizácia a všetky ostatné hodnoty kvantového bitu sú definované superpozíciou týchto polarizácií. Pomocou takejto identifikácie nie je žiadny principiálny problém overiť Bellove nerovnosti, rozdistribuovať šifrovací kľúč, teleportovať kvantový stav, alebo aj uskutočniť kvantový výpočet. Vďaka svojej rýchlosti je svetlo skutočne ideálnym kuriérom kvantových správ, avšak polarizácia sa pri šírení (či už vzduchom, alebo optickými káblami) mení v závislosti od podmienok prostredia, ktoré sú prakticky nekontrolovateľné a z nášho pohľadu viacmenej náhodné. Napriek tomu je polarizácia bezpochyby užitočnou vlastnosťou, ktorá si už našla využitie v mnohých zaujímavých aplikáciách. Svetlo, resp. fotóny samotné, dnes hrajú veľmi významnú úlohu takmer vo všetkých realizáciach kvantových bitov a hradiel.

## IX. Stavba hmoty a tunelovanie

*Podľa všetkého prvým, kto vyslovil hypotézu, že hmota okolo nás (zem, voda, vzduch atď.) sa skladá z viac už nedeliteľných častíc, tzv. atómov, bol grécky učenec Demokritos žijúci v piatom storočí pred našim letopočtom. Dokázať, prípadne vyvrátiť túto hypotézu však ľudia boli schopní až po vyše dvetisícich rokoch. Chemikom sa v tej dobe podarilo odhaliť, že hmota sa skladá z molekúl, ktoré sú zložené z ešte elementárnejších stavebných kociek – atómov, ktoré ruský chemik Dmitrij Mendelejev zoradil do tzv. periodickej tabuľky elementárnych prvkov.*

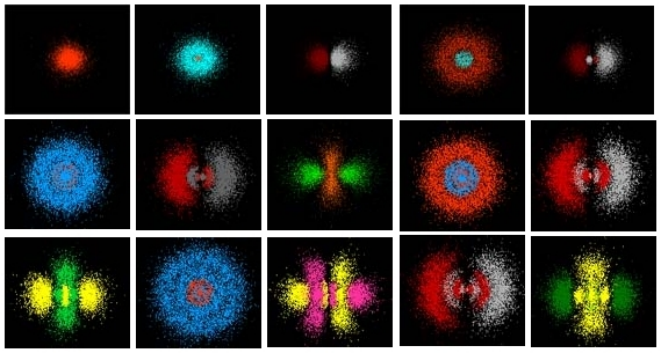
Koniec 19. storočia však priniesol nejedno prekvapenie. Objav elektrónu naznačil, že aj atómy predsa len majú akúsi vnútornú štruktúru. Začali sa pokusy o pochopenie stavby samotných atómov.

**Model atómu**

*Ernst Rutherford* pozoroval rozptyl kladne nabitého alfa žiarenia na atómoch striebra a prišiel k záveru, že atómy sa skladajú z veľmi malého kladne nabitého jadra a elektrónov. Svojimi experimentmi vyvrátil predstavu tzv. pudingového modelu atómov, podľa ktorého sa atóm skladá z akejsi kladne nabitej hmoty (pudingu) a elektróny si plávajú v takejto hmote podobne ako hrozienka v pudingu. E. Rutherford dokázal, že v atóme je kladný náboj sústredený do extrémne malého objemu v porovnaní s celkovým rozmerom atómu. Odtiaľto bol už len malý krôčik k tzv. planetárnemu modelu atómov. Podľa tohoto modelu elektróny v atóme obiehajú okolo jadra po eliptických dráhach podobne ako planéty okolo Slnka. Takmer okamžite však nastalo sklamanie, pretože takýto model nesúhlasí s predpoveďami teórie elektromagnetizmu. Podľa tejto teórie by mal krúžiaci elektrón vyžarovať a tým strácať svoju pohybovú energiu. Za približne $10^{-12}$ sekundy by sa mal elektrón v atóme zrútiť do jadra, čo je ale v rozpore s tým, čo pozorujeme. Záver je teda jednoznačný: atóm nemôže byť a nie je malá slnečná sústava. Klasická fyzika nielenže nebola schopná popísať svetlo ako prúd fotónov (písali sme o tom v minulej časti v *Quarku 2005/11*), ale nedokáže ani úplne popísať správanie a stavbu hmoty.

Začiatkom 20. storočia sa fyzici pokúšali vymyslieť model aspoň toho najjednoduchšieho atómu – vodíka, ktorý sa skladá z jediného elektrónu a jeho jadro má jednotkový kladný náboj, t.j. atóm ako celok je elektricky neutrálny. Trochu bizarné východisko z krízy ponúkol dánsky fyzik *Niels Bohr*, ktorý nedbal na známe fyzikálne zákony a jednoducho postuloval pravidlá, ktorými sa atóm vodíka riadi. Predpokladal, že elektrón sa pohybuje po kruhovej dráhe (orbite) okolo jadra, ale nevyžaruje. Naviac orbity, po ktorých sa elektrón pohybuje, nie sú ľubovoľné. Elektrón môže mať iba isté hodnoty energie (energia zodpovedá orbite), t.j. jeho energia v atóme je *kvantovaná*. Atóm má povolené vyžarovať iba v prípade, ak elektrón preskakuje zo vzdialenejšej orbity na orbitu bližšiu k jadru. Podobným mechanizmom atóm vodíka aj prijíma energiu od fotónov. Iba ak má fotón tú správnu energiu a elektrón je na tej správnej hladine, tak atóm dokáže tento fotón pohltiť. Popritom elektrón povyskočí na vzdialenejšiu orbitu, t.j. získa energiu.

Napriek tomu, že Bohrov model atómu vodíka bol vlastne prvým skutočným krokom ku kvantovej fyzike, nie je úplne správny. Ide síce o veľmi dobrú predstavu, ako chápať správanie vo vnútri atómu, ale stále používa predstavu orbít, t.j. predstavu, že elektrón sa v atóme pohybuje po akejsi dráhe. Dnes vieme, že v kvantovej fyzike elektróny nemajú presne určenú dráhu, po ktorej sa pohybujú. Vieme iba povedať, s akou pravdepodobnosťou sú na akom mieste, ak poznáme ich energiu, resp. orbitu. Podľa kvantovej fyziky sú elektróny v atóme akosi rozmazané. Hovoríme, že tvoria elektrónový obal, o ktorom má zmysel hovoriť, ale o konkrétnych dráhach elektrónov nevieme povedať nič. S tou istou situáciou sme sa už stretli v časti o kvantovej interferencii (*Quark 2005/02*).



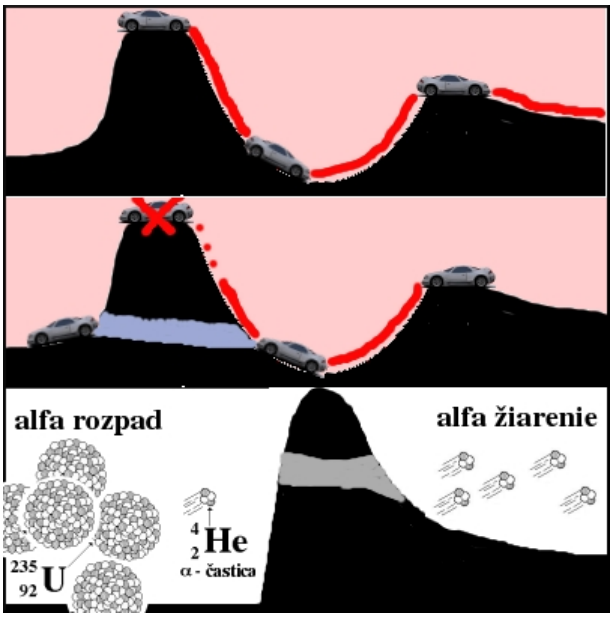
**Obr.1. Orbity atómu vodíka.** Ako *sa elektrón v atóme pohybuje? Nepoznáme jeho konkrétnu dráhu, pretože žiadnu nemá, ale poznáme pravdepodobnosti, kde sa asi v atóme nachádza. Na obrázku vidíme výskyt elektrónu v atóme vodíka. Každý obrázok zodpovedá rôznej energii, t.j. orbite. Na každej orbite sa môže nachádzať iba istý maximálny počet elektrónov. Rôzne farby zodpovedajú rôznym elektrónom s tou istou energiou.*

**Schroedingerova rovnica**

Bohrov model zožal svojho času obrovský úspech, pretože presne vysvetlil spektrum atómu vodíka, t.j. frekvencie elektromagnetického žiarenia, ktoré vodík dokáže pohltiť. Bohužiaľ sa však nepodarilo tento model rozšíriť na zložitejšie atómy obsahujúce viacero elektrónov. Presnú teóriu atómov sa podarilo naformulovať rakúskemu fyzikovi *Ervinovi Schroedingerovi*, ktorý napísal rovnicu opisujúcu akékoľvek dianie v kvantovom svete. Ide o rovnicu, ktorá je ekvivalentom Newtonovej rovnice pre mechaniku telies alebo Maxwellových rovníc pre elektromagnetizmus. Kľúč ku kvantovému svetu a stavbe atómov je skrytý v tejto rovnici. Schroedingerova rovnica nám okrem iného pomohla pochopiť periodickosť Mendelejevovej tabuľky elementárnych prvkov, chemické väzby a chemické reakcie. Akým spôsobom vlastne táto rovnica vysvetľuje, resp. zabezpečuje stabilitu atómov? Trochu zjednodušene môžeme povedať, že Schroedingerova rovnica zaväzuje kvantové systémy k istému správaniu. Presnejšie povedané, určuje, ako napríklad elektrón môže narábať s pridelenou energiou. V prípade elektrónov v atóme nám hovorí, že energia sa zachováva, t.j. atóm nevyžaruje! Naviac ešte Schroedingerova rovnica určuje, aké energie vlastne elektróny v atóme môžu mať, t.j. ktoré „orbity" sú povolené. Skôr ako o orbitách však zvykneme hovoriť o energetických hladinách, t.j. povolených hodnotách energie. Klasická fyzika používa pri predpovediach Newtonovu rovnicu a Maxwellove rovnice, ktoré keď aplikujeme na atómy, tak vedú k ich kolapsu, ale Schroedingerova rovnica je tým pravidlom, ktorý pozorovanú stabilitu atómov presne opisuje.

**Tunelovanie**

Okrem toho, že kvantová fyzika vysvetľuje stavbu atómov a hmoty, otvára dvere aj možnosti tzv. tunelovania, t.j. ako prekážajúcu hmotu „prekonávať". Pri tomto jave kvantová častica dokáže preniknúť aj cez bariéru, cez ktorú by podľa klasickej fyziky prejsť nemala, pretože nemá na to dostatočnú energiu. Predstavme si cestu spájajúcu dva vrcholy, ktoré nemajú rovnakú výšku. Ak auto spustíme z väčšieho kopca a vylúčime z hry trenie, tak hravo prejde za nižší kopec. Naopak to však v žiadnom prípade nepôjde, t.j. auto pustené z nižšieho kopca nemá šancu na ten vyšší kopec ani len vyjsť. Kvantové auto by sa však dokázalo dostať aj za tento vyšší kopec. Aby sme tento jav vysvetlili, tak si musíme predstaviť, že kvantové auto využíva akýsi tunel, ktorý ale v skutočnosti neexistuje, t.j. pretuneluje cez kopec. Ako je to možné? Odpoveď je opäť skrytá v Schroedingerovej rovnici, ktorá určuje ako kvantové auto so svojou energiou narába.




**Obr.2.Tunelovanie.** *Auto spustené z vyššieho kopca na nižší vyjde bez akýkoľvek problémov, ale naopak nikdy, pretože energia auta spusteného z menšieho kopca nie je dostatočná. Auto sa teda nikdy do priestoru za vyšší kopec nedostane. Toto však neplatí pre kvantové objekty (kvantové auto), ktoré sa za kopec niekedy môže dostať napriek tomu, že nemá dostatočnú energiu na prekonanie vyššieho kopca, t.j. využije akýsi tunel, ktorým kopec prekoná. Podobne sa „cíti" aj alfa častica v jadre napríklad*

*uránu. Pomocou pretunelovania dokáže prekonať jadrové sily a opustiť uránové jadro. Tento jav je prejavom rádioaktivity, pri ktorej vzniká tzv. alfa žiarenie.*

Ako sme už spomínali, kvantová fyzika predpovedá iba pravdepodobnosti, t.j. aj tunelovanie je javom pravdepodobnostným a častica (kvantové auto) má iba istú pravdepodobnosť, že bariéru pretuneluje. Bariéru môžeme charakterizovať energiou $U$, ktorá je potrebná na to, aby ju častica podľa klasickej fyziky prekonala. Ak je pohybová energia častice $E$ väčšia ako $U$, tak častica bariéru prekoná. Ak ale $E<U$, tak podľa klasickej fyziky (Newtonova rovnica) častica nikdy za bariéru neprenikne. Podľa kvantovej fyziky existuje istá pravdepodobnosť, že častica cez bariéru prenikne aj v takomto prípade. Táto pravdepodobnosť klesá exponenciálne z dĺžkou (hrúbkou) bariéry $L$, hmotnosťou častice $m$ a rozdielom energii $U$ a $E$, teda

$$\text{pravdepodobnosť} = \exp[-2L\,(2m(U-E))^{1/2} / h],$$

kde $h = 1.06 \times 10^{-34}$ J.s je Planckova konštanta. Tunelovanie je preto ťažšie ak je bariéra hrubá, hmotnosť veľká a energia oveľa menšia ako energia bariéry. Ak si do tohoto vzťahu dosadíme parametre typické pre náš každodenný život, tak zistíme, že pravdepodobnosť pretunelovania človeka cez múr je približne $10^{-30}$, čo je skutočne zanedbateľná hodnota, ktorá prakticky znamená, že človek nikdy cez múr neprejde bez toho, aby ho vôbec nepoškodil. Bolo preto potrebné vymyslieť dvere. Aby to nevyzeralo, že kvantová fyzika dokáže len „rúcať" bariéry, tak ich aj stavia. Častice, ktoré majú dostatočnú energiu na preniknutie bariéry ($E>U$) niekedy nepreniknú, t.j. máme aj situáciu akéhosi odrazenia sa od neexistujúcej prekážky. Inými slovami to, že kvantovému autu udelíme dostatočnú energiu ešte nezaručuje, že auto cez kopec prejde. Vidíme, že kvantová fyzika je v istom zmysle férová a nielen povoľuje zakázané (tunelovanie), ale aj zakazuje povolené.

Pravdepodobne prvou aplikáciou javu tunelovania bolo vysvetlenie rádioaktívneho alfa rozpadu americkým fyzikom *Georgom Gamowom*. Pri alfa rozpade sa jadro atómu rozpadá a produkuje héliové jadrá, t.j. alfa častice. Héliové jadro je stabilným systémom a je preto prirodzené predpokladať, že v nejakom zmysle existuje v jadre atómu ešte pred alfa rozpadom. Podobne ako predpokladáme, že elektrón sa nachádza v atómoch aj pred ich ionizáciou. Môžeme si predstaviť, že alfa častica je v jadre viazaná nejakou silou. Táto jadrová sila vytvára istú bariéru, cez ktorú sa alfa častica nevie dostať a vďaka tomu je držaná v jadre atómu. Podľa kvantovej fyziky však existuje istá pravdepodobnosť, že alfa častica pretuneluje, t.j. jadro a aj celý atóm opustí. A to je presne to, čo pozorujeme. Pravdepodobnosť tunelovania priamo súvisí s polčasom rádioaktívneho rozpadu daného atómu., t.j. vďaka tunelovaniu sme trochu viac pochopili proces rádioaktívneho rozpadu.

**Kvantová elektronika**

Javy spojené s tunelovaním pozorujeme napríklad aj v polovodičoch, resp. na rozhraniach polovodičov ako napríklad v tzv. „tunelovej dióde". Tunelovanie je jednou zo základných techník, ktoré sa uplatňujú v tzv. kvantovej elektronike. V roku 1985 ruskí fyzici *Dmitrij Averin* a *Konstantin Licharev* navrhli tzv. jednoelektrónový tunelový tranzistor (z ang. „*single electron tunneling (SET) transistor*"), ktorý o dva roky neskôr skonštruovali v Bellovych laboratóriách v USA. Tento tranzistor sa skladá z nevodiča vloženého medzi dve vodivé elektródy. Elektróny bežne cez nevodič neprejdú, ale v tomto prípade ide skutočne o veľmi úzky nevodivý pás (asi 1 nanometer, t.j. 10 atómov vedľa seba), ktorý je z pohľadu elektrónov bariérou.

Akonáhle majú kvantové častice pred sebou bariéru, tak sa snažia tunelovať. A presne na tomto princípe funguje aj SET tranzistor. Ak sme už spomínali, prechod závisí od hrúbky bariéry, ktorá je v tomto prípade veľmi úzka a prúd, ktorý vzniká závisí od množstva elektrónov, ktoré sa snažia bariéru prekonať. Toto zariadenie pracuje s individuálnymi elektrónmi a má veľmi blízko k tzv. kvantovým bodkám, ktoré sa fyzici snažia použiť ako kvantový bit, t.j. základný stavebný kameň kvantového počítača. Okrem toho SET tranzistor našiel svoje využitie aj pri presných meraniach veľkosti náboja a prúdu.

**Nadsvetelná rýchlosť**

Tunelovanie otvára zaujímavú otázku, akou rýchlosťou vlastne častica cez bariéru prechádza? Existujú experimenty, v ktorých fyzici tvrdia, že namerali nadsvetelné rýchlosti prenosu informácie pomocou tunelovania. Najznámejší je asi prípad, v ktorom bola vraj prenesená časť Mozartovej symfónie rýchlosťou 4,7-krát vyššou než je rýchlosť svetla vo vákuu. Napriek tomu, že akademická debata o príslušných experimentálnych výsledkoch stále trvá, všeobecne sa prijal konzensus, že v ani jednom experimente sa nenarušila kauzalita, t.j. neuskutočnil sa nadsvetelný prenos informácie. Celý problém je v definovaní, čo je rýchlosť prenosu cez bariéru, resp. ako sa vysporiadať s pravdepodobnostným charakterom celej teórie pri definovaní takejto rýchlosti. Diskusia o tejto téme však ešte nebola uzavretá.

**Záverom**

Dočítali ste poslednú časť seriálu článkov o svete kvantovej fyziky. Tento seriál nemal ambíciu a ani časopriestor podrobne krok za krokom vysvetľovať zákonitosti kvantového sveta. Skôr išlo o vyvolanie pocitu, že kvantová fyzika, aj keď je teóriou technicky komplikovanou, nie je až taká úplne odtrhnutá od života a jej prejavy môžeme nepriamo sledovať aj okolo nás. Tak je to koniec koncov s akoukoľvek fyzikou, stačí sa len pozorne a kriticky pozerať.

*MÁRIO ZIMAN*