Pokroky matematiky, fyziky a astronomie

Daniel Reitzner

Kvantové previazanie a Nobelova cena za fyziku 2022

Pokroky matematiky, fyziky a astronomie, Vol. 68 (2023), No. 1, 29–45

Persistent URL: http://dml.cz/dmlcz/151601

Kvantové previazanie a Nobelova cena za fyziku 2022

Daniel Reitzner

Abstrakt. Nobelova cena za fyziku bola v roku 2022 udelená za *experimenty s previazanými fotónmi, overenie narušenia Bellových nerovností a priekopnícky prínos v oblasti kvantovej informácie.* Výsledky ocenených vedcov Alaina Aspecta, Johna F. Clausera a Antona Zeilingera viedli nielen k lepšiemu pochopeniu neklasického správania sa kvantovej teórie, ale aj k opätovnému záujmu o štúdium základov kvantovej teórie a k rozvoju teórie kvantovej informácie a následne k súčasnému rozmachu v kvantovom počítaní, či kvantovo-asistovanej komunikácii.

V nasledujúcich riadkoch sa pokúsim podať stručný historický kontext pre udelenú Nobelovu cenu. Veľkú časť voľne čerpám z knihy *How the Hippies Saved Physics* [22], ktorá čitateľa prevedie často vtipnými príhodami z obdobia, kedy došlo k výraznému posunu v pochopení kvantového previazania. Nie je však cieľom tohto článku podať vyčerpávajúci historický výklad, ale vyberiem len časti podstatné pre pochopenie historického pozadia, na ktorom sa výskum odohrával.

Štúdium kvantovej teórie po druhej svetovej vojne sa celosvetovo silne orientovalo na praktické účely. Zložitá geopolitická situácia medzi svetovými mocnosťami nepriala základnému výskumu, ktorý by sa zaoberal otázkami *ako* a *prečo* kvantová teória funguje. Praktický prístup vystihnutý Merminovým pomenovaním Kodaňskej interpretácie kvantovej teórie *shut up and calculate* viedol síce k mnohým pokrokom vo fyzike, ale pochopenie kvantového previazania k nim nepatrí.

Po mnohých diskusiách Einsteina s Bohrom a po publikovaní slávneho *EPR článku* [14] bolo kvantové previazanie považované iba za exotický prejav našej neznalosti celkového kvantového stavu. Aj keď to nebolo explicitné, kvantové previazanie bolo poväčšinou chápané v zmysle skrytých parametrov a nebol záujem vedeckej obce o hlbšie pochopenie previazania. Tento postoj mal vplyv aj na tých, ktorých téma zaujímala, vrátane ocenených vedcov, ktorí boli často odhováraní od štúdia danej problematiky. Táto oblasť bola považovaná za neperspektívnu, čo malo mať neblahý vplyv na ich vedeckú budúcnosť.

Našťastie tvrdohlavosť u všetkých troch laureátov zvíťazila a ich výsledky viedli k hlbšiemu pochopeniu kvantového previazania. Spomenutie si zaslúži aj John Stewart Bell, ktorého teoretické výsledky boli kľúčové pri pochopení kvantového previazania a nebyť jeho skorého úmrtia (1990), aj on by bol vážnym adeptom na Nobelovu cenu.

V nasledujúcich pasážach si tento historický vývoj priblížime aj s trochou teórie.

RNDr. Daniel Reitzner, PhD., VTT Technical Research Centre of Finland, P.O. Box 1000, FI-02044 VTT, Fínsko, e-mail: daniel.reitzner@vtt.fi

Obr. 1. Laureáti Nobelovej ceny za fyziku 2022: Alain Aspect, John F. Clauser a Anton Zeilinger (autori fotografií: Clément Morin a Nanaka Adachi, © Nobel Prize Outreach)

1. Kvantové previazanie na okraji záujmu

Ak výskum, za ktorý bola tento rok udelená Nobelova cena, považujeme za následok, je vhodné sa pozrieť aj na príčinu. Tá je zhmotnená v článku [14], v ktorom v roku 1935 autori Einstein, Podolsky a Rosen predstavili myšlienkový experiment, ktorý vedie k paradoxu. Tento dnes nazývame podľa iniciál ich mien ako EPR paradox.

V tomto článku autori používajú vlnový formalizmus, ale vzhľadom na celistvosť tohto článku, ich argument budem prezentovať za pomoci Diracovho bra-ket formalizmu, približujúc sa skôr k alternatívnemu popisu Bohma a Aharonova [9]. Autori študujú dvojčasticový previazaný singletový stav[1] dvoch dvojhladinových častíc (qubitov)

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{1}$$

Dôležitá vlastnosť tohto stavu pre nás je, že vyzerá rovnako v každej báze. Ak budeme mať napríklad bázu $\{|b_0\rangle, |b_1\rangle\}$, tak stav bude opäť

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|b_0 b_1\rangle - |b_1 b_0\rangle).$$

Špeciálne, ak si definujeme jednoqubitové stavy

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle),$$

tak zapisujeme

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle).$$

[1] Z praktických dôvodov budeme štvoricu maximálne previazaných stavov, $|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ a $|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, nazývať *Bellove stavy* a dvojčasticové meranie v tejto báze ako *Bellovo meranie*. Špeciálne sa tiež môžeme stretnúť s pomenovaním singletového stavu $|\Psi_-\rangle$ ako EPR pár.

Teraz predpokladajme, že tieto dve častice tohto stavu vzdialime od seba dostatočne ďaleko, jednu časticu bude mať Alica a druhú Bob[2]. Alica si zvolí bázu na meranie, a to buď pôvodnú bázu $\{|0\rangle, |1\rangle\}$, alebo bázu $\{|\pm\rangle\}$, ktorú nazveme rotovaná báza. Ak si zvolila pôvodnú bázu, tak s pravdepodobnosťou 1/2 nameria 0 a s pravdepodobnosťou 1/2 nameria 1. Vzhľadom na antikoreláciu medzi časticami Alice a Boba bude v tom okamihu jasné, že Bob nameria buď 1, alebo 0 v jednotlivých prípadoch, ak aj on zvolí pôvodnú bázu. V prípade, že Alica aj Bob zvolia rotovanú bázu, tak Alica a Bob budú opäť dostávať antikorelované výsledky, buď $(+, -)$, alebo $(-, +)$.

Einstein, Podolsky a Rosen predpokladali, že ak informácia o voľbe smeru merania Alice nemá čas dôjsť k Bobovi (Alica a Bob sú dostatočne vzdialení), a zároveň vieme s určitosťou tvrdiť, aké výsledky nameria Bob pri jednotlivých meraniach, tieto musia byť tzv. elementami reality, t. j. musia byť vopred určené, napríklad v momente vytvorenia EPR páru. Avšak zároveň jedným zo základných princípov kvantovej teórie sú vzťahy neurčitosti, ktoré hovoria, že existujú páry meraní, u ktorých ak máme presne určený výsledok u jedného merania, je výsledok u komplementárneho nutne neurčitý.

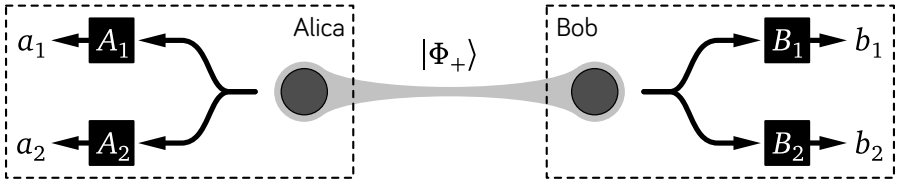
Tieto dva závery si navzájom protirečia a tvoria základ EPR paradoxu – keďže máme zároveň presne určené výsledky meraní v normálnej aj rotovanej báze a tieto z princípu nemôžu byť zároveň presne definované. Z tohoto autori usúdili, že kvantová teória je neúplná. Aj keď debata naďalej prebiehala, asi 30 rokov sa, aj na základe tohto výsledku, usudzovalo, že existuje, pre nás zatiaľ skrytá, informácia, ktorá bližšie určuje, čo sa v experimente deje. Diskutovalo sa skôr o tom, ako korelácie výsledkov meraní vznikajú, aby tak neboli v rozpore s princípom neurčitosti, a ich popis sa skôr držal analógie s klasickými koreláciami [9]. Hlavne toto pochopenie korelácií v EPR paradoxe sa ukázalo ako nesprávne a prelomový článok Johna Bella poukázal na ďalší zaujímavý aspekt kvantovej teórie.

2. Bellove nerovnosti a ich overovanie

V roku 1964 vydal John Stewart Bell článok [6], v ktorom matematicky rigorózne ukázal, že ak existujú nejaké pre nás skryté parametre, ktoré určujú výsledky meraní, tak existujú štatistické veličiny, ktoré môžu v kvantovej teórii nadobúdať iné hodnoty, než v klasickej fyzike. Konkrétne Bell ukázal, že ak platí model skrytých parametrov (zahŕňajúci akékoľvek situácie popísané cez klasické korelácie), tak istá funkcia korelácií získaných výsledkov je ohraničená konkrétnou hodnotou. Táto nerovnosť môže byť v kvantovej teórii narušená.

Bellov článok bol prelomový – po jeho publikovaní sa základy kvantovej teórie opäť dostali do pozornosti a ako uvidíme, ich výskum viedol k dnešnému rozmachu kvantových technológií. Vráťme sa však k podstate. Článok je síce dôležitým míľnikom, ale dôkaz v ňom prezentovaný je z fyzikálneho pohľadu nevhodný na priame experimentálne overenie a z didaktického hľadiska je dosť komplikovaný. Bol však inšpiráciou pre množstvo ďalších článkov, v ktorých sú prezentované podobné nerovnosti skúmané pri rôznych ďalších parametroch (rôzne počty častíc, dimenzií, meraní, či výsledkov meraní). Často sa tieto nerovnosti spoločne nazývajú *Bellove nerovnosti*.

[2] Alica a Bob sú štandardnými účastníkmi v komunikačných úlohách, kam môžeme zaradiť aj túto. Ďalšími častými stranami sú Charlie alebo Eva (ako *eavesdropper*, odpočúvajúca strana, narušiteľka).



Obr. 2. Narušenie CHSH nerovnosti sa experimentálne overí za použitia maximálneho previazaného stavu, ktorý je poslaný dvom stranám, Alici a Bobovi. Tí si náhodne volia jedno z dvoch meraní. Koincidencie týchto meraní sa použijú na výpočet funkcie B (2). Ak táto hodnota naruší nerovnosť (4), tak kvantová teória nie je popísateľná za pomoci skrytých parametrov

Na prvé overenie Bellových záverov bola použitá tzv. CHSH nerovnosť [12], ktorá je pomenovaná podľa iniciál mien autorov, ktorými sú Clauser, Horne, Shimony a Holt. Clauser je práve jeden z minuloročných laureátov Nobelovej ceny. Tú získal za experimentálne overenie CHSH nerovnosti v spolupráci so Stuartom Freedmanom [16]. V článku je skúmaný systém veľmi podobný nastaveniu z článku EPR. Situácia je znázornená na obrázku 2. Jedna častica Bellovho stavu $|\Phi_+\rangle$ je poslaná Alici a druhá Bobovi. Každý z nich si náhodne vyberá jedno z meraní, ktoré majú k dispozícii – Alica merania A_1 a A_2, a Bob merania B_1 a B_2 – a vykonajú meranie na svojej častici. Tu predpokladáme, že Alica aj Bob sú od seba dostatočne vzdialení, a prevádzajú merania súčasne tak, aby informácia o voľbe jedného merania nestihla ovplyvniť meranie na druhej strane (predpokladáme konečnú rýchlosť šírenia informácie). Výsledky týchto meraní nech sú ± 1. Alica aj Bob si zaznamenávajú výsledky mnohých behov takéhoto experimentu a potom porovnávajú štatistiku a pozerajú sa na špeciálnu funkciu korelácií medzi výsledkami. Tá je

$$\mathsf{B} = C(A_1, B_1) + C(A_1, B_2) + C(A_2, B_1) - C(A_2, B_2), \tag{2}$$

kde

$$C(A, B) = \sum_{a,b} ab\, p(a, b|A, B) \tag{3}$$

a kde suma ide cez všetky výsledky a a b (u nás ± 1) pri voľbe meraní A a B a $p(a, b|A, B)$ určuje pravdepodobnosť namerania týchto výsledkov pre dané merania. V rámci tohto označenia napríklad podmienku, že Alicina voľba merania neovplyvňuje Bobove výsledky, vieme zapísať

$$\sum_a p(a, b|A_1, B) = \sum_a p(a, b|A_2, B) \equiv P(b|B)$$

pre ľubovoľné meranie B Boba a vybrané dve merania A_1 a A_2 Alice. Samozrejme vzťah platí pre ľubovoľné Alicino meranie. Túto podmienku nazývame *no-signalling*.

Vypočítajme si teraz hodnotu B jednak za predpokladu existencie modelu skrytých parametrov a potom jeho hodnotu, ktorú vieme získať v kvantovej teórii.

2.1. Model so skrytými parametrami

V článku EPR je niekoľko predpokladov, ktoré je potrebné splniť. Záver o neúplnosti kvantovej teórie implikuje existenciu nejakých skrytých parametrov, ktoré určujú konkrétnu, aj keď nám neprístupnú, informáciu o výsledkoch všetkých meraní, aj takých, ktoré sú navzájom komplementárne, čiže napr. poloha a hybnosť, alebo spinové komponenty. Zároveň sa predpokladá, že informácia o tom, ktoré meranie zvolila Alica, sa šíri konečnou rýchlosťou a teda ak Alica a Bob prevádzajú merania súčasne, ich jednotlivé častice musia mať výsledky už vopred dané a tie musia byť lokálne ako pre Alicu, tak aj pre Boba.

Predchádzajúce obmedzenia pre nás efektívne znamenajú, že pravdepodobnosť $p(a, b|A, B)$ sa dá zapísať v tvare

$$p(a, b|A, B) = \int \mathrm{d}\lambda \; p(a|A, \lambda)p(b|B, \lambda)p(\lambda),$$

kde λ je skrytý, potenciálne mnohorozmerný a spojitý parameter určujúci výsledky meraní, ktorý môže byť náhodný s distribúciou pravdepodobnosti $p(\lambda)$. Zároveň je pravdepodobnosť výsledku na strane Alice nezávislá od parametrov Boba a naopak, pravdepodobnosť výsledku na strane Boba je nezávislá od parametrov Alice. Všetko, čo vie jeden o druhom, je z času, kedy bol systém vytvorený a táto informácia je premietnutá do parametra λ. Zároveň môžeme sumu v (3) rozšíriť o výsledky meraní v ostatných meraniach, využijúc identitu $\sum_x p(x|X, \lambda) = 1$, ktorá platí pre ľubovoľné meranie X a hovorí, že pravdepodobnosť namerania nejakého výsledku je jedna. Potom napríklad korelátor $C(A_1, B_1)$ vieme zapísať v tvare

$$C(A_1, B_1) = \int \mathrm{d}\lambda \sum_{a_1,a_2,b_1,b_2} a_1 b_1 \; p(a_1|A_1, \lambda)p(a_2|A_2, \lambda)p(b_1|B_1, \lambda)p(b_2|B_2, \lambda)p(\lambda).$$

Dosadením do vzťahu (2) dostávame

$$\begin{aligned}\mathsf{B} = \int \mathrm{d}\lambda \sum_{a_1,a_2,b_1,b_2} (a_1 b_1 + a_1 b_2 + a_2 b_1 - a_2 b_2) \times \\ \times p(a_1|A_1, \lambda)p(a_2|A_2, \lambda)p(b_1|B_1, \lambda)p(b_2|B_2, \lambda)p(\lambda).\end{aligned}$$

Zátvorku s výsledkami vieme zároveň prepísať a ohraničiť nasledovne:

$$a_1 b_1 + a_1 b_2 + a_2 b_1 - a_2 b_2 = a_1(b_1 + b_2) + a_2(b_1 - b_2) \leqq 2.$$

Pri nerovnosti sme využili, že výsledky sú ± 1, a že buď $b_1 + b_2 = 0$ alebo $b_1 - b_2 = 0$ a opačný člen je potom ± 2. Záverom teda platí nerovnosť

$$\mathsf{B} \leqq \int \mathrm{d}\lambda \sum_{a_1,a_2,b_1,b_2} 2p(a_1|A_1, \lambda)p(a_2|A_2, \lambda)p(b_1|B_1, \lambda)p(b_2|B_2, \lambda)p(\lambda) = 2.$$

A teda v každej teórii so skrytými parametrami nutne platí

$$\mathsf{B} \leqq 2. \tag{4}$$

Táto nerovnosť sa nazýva CHSH nerovnosť. Môžeme si všimnúť, že v článkoch [12], [16] má táto hranica inú hodnotu, aj tvar vyzerá byť odlišný. Je to jednak tým, že nerovnosť využíva špecifiká pre daný experiment, čím eliminuje niektoré korelátory, a jednak je inak normovaná a používa inú formu korelátora medzi meraniami – mieru koincidencie detekcie. Podobná situácia je aj v mnohých ďalších článkoch a pri ich čítaní je dobré dávať na to pozor.

2.2. Narušenie v kvantovej teórii

Teraz si ukážeme, ako môže dôjsť k narušeniu nerovnosti (4) v kvantovej teórii. V práci [16] bol ako počiatočný stav použitý stav

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

Autori ho získali ako fotónový pár vyžiarený pri kaskáde vápnika $6^1\mathrm{S}_0 \to 4^1\mathrm{P}_1 \to 4^1\mathrm{S}_0$. Použitím tohoto stavu sa dá ukázať, že pre jednoqubitové merania A a B v smeroch[3] $\vec{a}$ a $\vec{b}$ má korelátor tvar

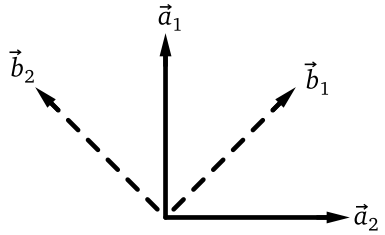
$$C(A, B) = \langle\Phi_+|A \otimes B|\Phi_+\rangle = a_x b_x - a_y b_y + a_z b_z,$$

kde a_x, a_y, a_z a b_x, b_y, b_z sú zložky vektorov $\vec{a}$ a $\vec{b}$. Naviac sa môžeme obmedziť len do roviny x-z a v takom prípade píšeme $C(A, B) = \vec{a} \cdot \vec{b}$ a funkcia B sa dá zapísať ako súčet skalárnych súčinov vektorov definujúcich jednotlivé merania (v rovine x-z),

$$\mathsf{B} = \vec{a}_1 \cdot \vec{b}_1 + \vec{a}_1 \cdot \vec{b}_2 + \vec{a}_2 \cdot \vec{b}_1 - \vec{a}_2 \cdot \vec{b}_2.$$

Táto forma ponúka veľké množstvo možností pre narušenie Bellovej nerovnosti s maximom, ktoré sa dá dosiahnuť napríklad pre voľbu smerov ako na obrázku 3. V tomto prípade dostávame

$$\vec{a}_1 \cdot \vec{b}_1 = \vec{a}_1 \cdot \vec{b}_2 = \vec{a}_2 \cdot \vec{b}_1 = -\vec{a}_2 \cdot \vec{b}_2 = \frac{1}{\sqrt{2}},$$



Obr. 3. Jedna z možností voľby Blochovych vektorov pre merania A_1, A_2, B_1, a B_2, ktoré vedú k maximálnemu narušeniu CHSH nerovnosti (4). Konkrétne si môžeme vziať horizontálny smer ako smer x a vertikálny ako smer z

[3]Používame Blochovú sféru, kde ortogonálne stavy sú reprezentované navzájom opačnými stavmi. Zhruba povedané, používame dvojnásobné uhly ako za použitia polarizátorov pri fotónoch.

a teda

$$\mathsf{B} = 4\frac{1}{\sqrt{2}} = 2\sqrt{2} > 2.$$

Ešte pred tým ako si predstavíme ďalšie experimenty, je vhodné sa pristaviť pri význame Bellovho výsledku. Pred jeho publikovaním boli rôzne názory na to, ako EPR paradox interpretovať, ale nebolo jasné, či ktorákoľvek interpretácia môže byť experimentálne overená. Bellov článok v tomto ohľade poskytol jednoznačnú odpoveď v tvare numerickej hranice, ktorá oddeľuje jednotlivé interpretácie. Zároveň otvoril priestor pre ďalší výskum v oblasti základov kvantovej teórie. Minimálne tento výsledok znamená, že predpoklad *lokálneho realizmu* v článku EPR je nesprávny a aj napriek tomu, že to znie neintuitívne, meranie na jednej strane akoby ihneď „určuje“ výsledok merania na druhom systéme. Neintuitívnosť tohoto pôsobenia spočíva v tom, že na rozdiel od klasickej korelácie, kedy sú výsledky vopred dané, v prípade EPR častíc tieto výsledky nie sú vopred určené. Bellov výsledok tak má hneď dva odkazy, jeden je, že aj keď EPR pôsobí na prvý pohľad paradoxne, paradox vyplýva z predpokladov, ktoré pre nás vyzerajú rozumne, ale v rámci kvantovej teórie musíme akceptovať, že neplatia – ide o predpoklad lokálneho realizmu. Druhým odkazom je, že kvantové korelácie sú (resp. vedia byť) iné ako klasické korelácie. Dá sa povedať, že môžu byť silnejšie ako tie klasické.

2.3. Ocenené experimenty

V predchádzajúcej časti sme videli, že existuje teoretická hodnota, ktorú nejaká funkcia korelácií v modeli so skrytými parametrami nemôže presiahnuť, zatiaľ čo kvantová teória umožňuje jej narušenie. Od teoretického výsledku k jej jednoznačnému preukázaniu bolo nutné prekonať veľké množstvo problémov a trvalo to približne 50 rokov.

Prvé overenie prišlo síce už v roku 1972 v už spomínanom článku [16] s presnosťou šiestich štandardných odchýlok, avšak experiment nemal splnené všetky predpoklady, ktoré boli vyžadované z teórie. Medzi tieto „diery“ (v angličtine je zaužívaný pojem *loopholes*) patria tzv. *detection loophole* a *locality / causality loophole*.[4] Prvá diera vzniká, keďže naše detektory nie sú dokonalé a teoreticky môže nastať situácia, kedy bude príroda hrať s nami takú hru, že síce kvantová teória bude fungovať na základe skrytých parametrov (kedy nemôže byť CHSH nerovnosť narušená), avšak v úspešných detekciách budú prítomné práve tie korelácie, ktoré prispievajú k pozitívnym hodnotám v B. V experimente s parametrami, ktoré sme používali (dve voľby merania, singletový stav), je pre narušenie CHSH nerovnosti v inak ideálnom experimente požadovaná presnosť detektorov nad 83 % [17]. Zaujímavé je, že z pohľadu dnešných kvantových počítačov ide o také výrazné zlepšenie v efektivite meraní, že táto diera je už rutinne zaplátaná.

Druhou hlavnou dierou je problém s kauzalitou. Je extrémne zložité mať detektory dostatočne ďaleko od seba a dokázať ich náhodne prepínať tak rýchlo, aby informácia o nastavení na jednej strane nemala možnosť doraziť na druhú stranu pred tým, než

[4] Viac exotickou je *free-will loophole*, ktorá hovorí, že my samotní, ako aj meracie zariadenia, sme súčasťou experimentu a niekde pri zrode vesmíru sa skryté parametre nastavili tak, že naša „náhodná voľba“ nie je náhodná, ale je korelovaná s vnútornými hodnotami výsledkov presne tak, že to vyzerá, že dochádza k narušeniu CHSH nerovnosti. Táto diera sa tiež nazýva *superdeterminism*.

sa na druhej strane vykoná meranie. V desaťročí po Clauserovom experimente v sérii článkov Alain Aspect postupne odstraňoval práve túto dieru [4], [5], [3]. Sám však priznáva [2], že sa mu nepodarilo bez pochybností túto dieru zaplátať. To dokázal až Anton Zeilinger v roku 1998 [30]. Aj keď Aspect dokázal voliť dostatočne rýchlo nastavenia jednotlivých meraní, tie samotné neboli dokonale náhodné. Aj napriek tomu sa mu podarilo v jeho experimentoch dosiahnuť narušenie nerovností o desiatky štandardných odchýlok.

Čo sa týka nedokonalosti detektorov, aj tam sa podarilo problém s dierou vyriešiť, avšak až do roku 2015 bola zaplátaná výlučne jedna z hore uvedených dier. Obe diery naraz sa v danom roku podarilo zaplátať v troch článkoch [20], [19], [27], pričom v jednom z nich je autorom opäť Anton Zeilinger.

3. Previazanie ako zdroj

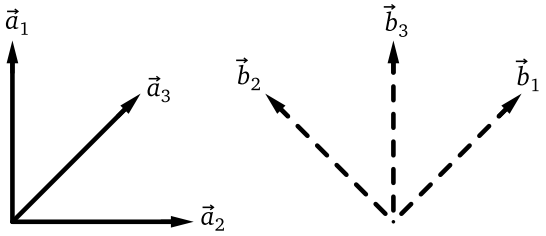
Kvantová teória informácie, ako jedno z odvetví, ktoré nazerá na kvantovú teóriu z pohľadu informácie, sa po predchádzajúcich výsledkoch dostala do centra pozornosti mnohých vedeckých kapacít. Predchádzajúce výsledky ukázali, že za kvantovou teóriou sa skrýva omnoho viac, ako sa myslelo. Rozvoj teórie, obzvlášť jej základov, sa zrýchlil, a postupoval rýchlejším tempom ako experimenty. Teória začala nazerať (nielen) na previazanie ako na „zdroj“ (resource), z ktorého môžeme čerpať pri riešení rôznych problémov.

Previazanie hrá dôležitú úlohu vo všetkých smeroch skúmania využitia kvantových javov od senzorov až po výpočty. Avšak ako zdroj figuruje takmer vo všetkých kvantovo-asistovaných kryptografických protokoloch, obzvlášť tých, ktoré sú z praktického hľadiska relevantné. Zároveň mnohé experimenty Antona Zeilingera spadajú pod túto oblasť, a preto sa jej ešte chvíľu povenujeme.

3.1. Praktická kvantovo-asistovaná kryptografia

V roku 1994 ukázal Peter Shor ako možno kvantový výpočet použiť na efektívnejší rozklad čísla na prvočísla než poznáme v klasickom počítaní [28]. To má za následok, že mnohé z moderných šifier už viac nemôžu byť považované za bezpečné. Aj keď z praktického hľadiska bude nutné mať desiatky tisíc až milióny qubitov a naša každodenná komunikácia je stále v bezpečí, existuje veľké množstvo šifrovaných dát, ktoré budú citlivé aj v blízkej budúcnosti, keď (pre pesimistov *ak*) dané kvantové výpočtové prostriedky budú k dispozícii. Práve preto sa tejto oblasti venuje obzvlášť veľká pozornosť.

Z pohľadu previazania ale zisťujeme, že kvantová teória vie poskytnúť aj prostriedky, ktoré bezpečnosť posilňujú. Aj keď prvé výsledky z oblasti kvantovo-asistovanej kryptografie boli už v roku 1984 [7], z pohľadu tohto článku je zaujímavý výsledok Artura Ekerta z roku 1991 [15], ktorý spája kvantový protokol pre tvorbu zdieľaného kľúča s možnosťou overenia, že nedochádza k snahe o odpočúvanie. Situácia je opäť podobná tej z obrázku 2, kde máme dve strany, ktoré chcú vytvoriť náhodný kľúč, ktorý medzi sebou zdieľajú tak, aby nikto iný nemal k nemu prístup. Alica a Bob použijú zdieľaný stav $|\Phi_+\rangle$ a smery meraní, ktoré sme použili pri narušení CHSH nerovnosti. Tieto smery sú však medzi Alicu a Boba rozdelené inak, konkrétne ako na obrázku 4, a teda obaja vyberajú náhodne z troch možností. Možnosti s indexami 1 a 2 sú v tých istých smeroch ako pri CHSH nerovnosti, ale pribudli smery $\vec{a}_3$ a $\vec{b}_3$.



Obr. 4. Smery meraní v protokole Ekert91. Merania v smeroch a_1, a_2, b_1, a b_2 vedú k overeniu narušenia CHSH nerovnosti za použitia stavu $|\Phi_+\rangle$, zatiaľ čo voľby smerov $(\vec{a}_1, \vec{b}_3)$ a $(\vec{a}_3, \vec{b}_1)$ ponúkajú možnosť vytvorenia náhodného zdieľaného kľúča

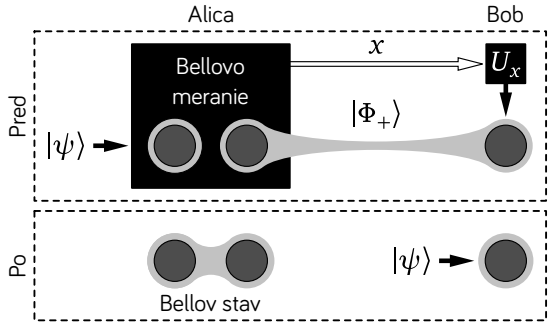
Pri protokole si teda Alica a Bob vyberajú merania náhodne a po ukončení meraní si Alica a Bob (cez autentifikovaný kanál) porovnajú bázy meraní. Nastávajú pre nás dve zaujímavé možnosti (ostatné Alica a Bob ignorujú). Jedna je, ak sa Alica a Bob zhodli na smere, t. j. buď zvolili $(\vec{a}_1, \vec{b}_3)$, alebo $(\vec{a}_3, \vec{b}_1)$. Druhá je voľba z CHSH báz (ako na obr. 3). Keď výsledky meraní v druhom prípade porovnajú, môžu vypočítať hodnotu B z rovnice (2) a otestovať CHSH nerovnosť (4). Ak je vyššia ako 2, tak nielen že neexistuje model skrytých parametrov, ale dá sa aj ukázať, že nedošlo k žiadnemu odpočúvaniu, čo zaručuje bezpečnosť protokolu. Tvorba kľúča potom pozostáva z ponechania výsledkov meraní z prvej sady, keďže tieto výsledky musia byť korelované.[5] Zároveň je zabezpečené, že sú náhodné a zdieľané len medzi Alicou a Bobom. Pri tom verejne zdieľaná informácia o smeroch daných meraní nemá pre prípadného odpočúvateľa žiadnu hodnotu, keďže je nekorelovaná s nameranými výsledkami, ktoré Alica a Bob nezdieľajú.

Za prvou experimentálnou realizáciou Ekertovho protokolu stál opäť Anton Zeilinger, ktorý takto vytvoril bezpečný kľúč na vzdialenosť 144 km medzi dvomi Kanárskymi ostrovmi La Palma a Tenerife [29]. Experimenty sa neskôr podarilo zdokonaliť natoľko, že v roku 2016 Jian-Wei Pan zrealizoval distribúciu previazaných častíc na vzdialenosť 1 203 km [23], [26] použijúc spojenie za pomoci na to určeného čínskeho satelitu *Micius*. Za pomoci dvoch pripojení na tento satelit tak vedel dosiahnuť narušenie Bellovej nerovnosti na vzdialenosť až 2 400 km a neskôr takto distribuovať bezpečný kľúč medzi Pekingom a Viedňou (neprekvapivo opäť s Antonom Zeilingerom).

3.2. Teleportácia a prenos previazania

Jedným z najznámejších využití previazania je kvantová teleportácia [8], ktorá je znázornená na obrázku 5. V nej hrajú previazanie a experimenty Antona Zeilingera opäť centrálnu úlohu. Pri teleportácii Alica a Bob zdieľajú previazaný stav $|\Phi_+\rangle$ (zložky prislúchajúce Alici a Bobovi budeme označovať indexami A a B). Alica sa v istom momente rozhodne poslať (neznámy) stav $|\psi\rangle$ na tretej častici (s indexom 0) Bobovi. Prevedie špeciálne meranie v Bellovej bázi, t. j. projektuje na Bellove stavy $|\Phi_\pm\rangle_{0A}$

[5] Samozrejme v realite ide o komplikovanejšiu situáciu kvôli nepresnostiam v experimentoch a je nutné tieto nedostatky korigovať. To je zložité, ale možné. Kladie to však dodatočné podmienky na niektoré elementy experimentu, napr. minimálnu spoľahlivosť detektorov a pod.



Obr. 5. Teleportácia je prenesenie (neznámeho) kvantového stavu $|\psi\rangle$ od Alice k Bobovi, ktorí sú od seba dostatočne ďaleko. Podstatným zdrojom je predom vytvorené previazanie, stav $|\Phi_+\rangle$. Alica prevedie u seba Bellovo meranie na posielanom stave a svojej časti EPR páru a pošle Bobovi takto získanú informáciu x (2 bity). Bob má bez tejto informácie efektívne úplne zmiešaný stav, avšak za pomoci klasickej informácie x od Alice vie lokálnou unitárnou transformáciou zmeniť tento stav na žiadaný stav $|\psi\rangle$. Situácia na obrázku znázorňuje stav pred posielaním neznámeho stavu Bobovi (hore) a po vykonaní teleportačného protokolu (dole)

a $|\Psi_\pm\rangle_{0A}$. Veľmi ľahko sa dá ukázať, že stav pred Aliciným meraním je[6]

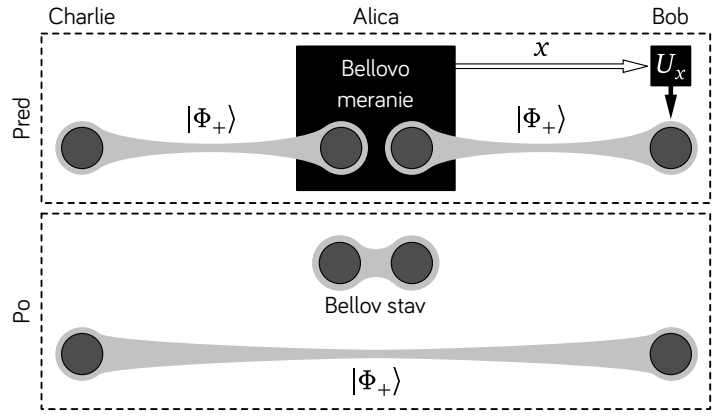
$$|\psi\rangle_0|\Phi_+\rangle_{AB} = \frac{1}{2}\big[|\Phi_+\rangle_{0A}(I|\psi\rangle_B) + |\Phi_-\rangle_{0A}(\sigma_z|\psi\rangle_B) + |\Psi_+\rangle_{0A}(\sigma_x|\psi\rangle_B) + |\Psi_-\rangle_{0A}(\sigma_x\sigma_z|\psi\rangle_B)\big], \tag{5}$$

kde I označuje identitu a σ_x, σ_y a σ_z sú Pauliho matice. Z predchádzajúceho vzťahu vidíme, že každý z výsledkov merania Alice je rovnako pravdepodobný. Naviac bez Alicinej informácie je pre Boba jeho stav úplne neznámy – je to úplne zmiešaný stav. Bob však môže klasickú informáciu, ktorú Alica má, použiť na úpravu tohoto stavu, aby dosiahol stav $|\psi\rangle$ – ak mu Alica povie, že namerala stav $|\Phi_+\rangle$, tak Bob vie, že má stav $|\psi\rangle$ a nemusí s týmto stavom nič viac robiť. Ak mu Alica ale povie, že namerala stav $|\Psi_-\rangle$, Bob vie, že má stav $\sigma_x\sigma_z|\psi\rangle$ a teda aby mal stav $|\psi\rangle$, musí stav zrotovať pomocou $\sigma_z\sigma_x$ operácie. Pri zvyšných dvoch možnostiach Bob použije buď samotnú σ_x rotáciu, alebo σ_z rotáciu. Prvé experimenty s teleportáciou boli urobené v roku 1997 skupinami Antona Zeilingera [11] a Francesca de Martiniho [10].

Dôležitou charakteristikou kvantovej teleportácie je opäť istá forma bezpečnosti. Alica a Bob totiž v čase teleportovania častice (previazaný pár si mohli vytvoriť dávno pred tým) môžu byť od seba veľmi ďaleko. Pre vykonanie teleportácie je potrebné mať pripravené previazanie (zdroj efektu) a zaslanie klasickej informácie o výsledku merania Alice. Tento výsledok, ako vidíme, je však náhodný a neobsahuje žiadnu informáciu o teleportovanom stave $|\psi\rangle$.

Z praktického hľadiska možno ešte dôležitejší je protokol, ktorý je analógiou ku kvantovej teleportácii, avšak v protokole neznámy stav nahradíme ďalším EPR pá-

[6]Využiť môžeme identity $|00\rangle = \frac{1}{\sqrt{2}}(|\Phi_+\rangle + |\Phi_-\rangle$, $|11\rangle = \frac{1}{\sqrt{2}}(|\Phi_+\rangle - |\Phi_-\rangle$, $|01\rangle = \frac{1}{\sqrt{2}}(|\Psi_+\rangle + |\Psi_-\rangle$ a $|10\rangle = \frac{1}{\sqrt{2}}(|\Psi_+\rangle - |\Psi_-\rangle$.



Obr. 6. Prenos previazania je podobný teleportácii, avšak v tomto prípade dochádza k využitiu previazania medzi Alicou a Bobom a Alicou a Charliem na vytvorenie previazania medzi Bobom a Charliem. Alica prevedie u seba Bellovo meranie na svojich častiach EPR párov a pošle napríklad Bobovi takto získanú informáciu x (2 bity). Bob vie lokálnou unitárnou transformáciou zmeniť stav, ktorý je medzi ním a Charliem, na žiadaný stav $|\Phi_+\rangle$, prípadne iný Bellov stav. Situácia na obrázku znázorňuje stav pred vytváraním previazania medzi Bobom a Charliem (hore) a po vykonaní protokolu (dole)

rom, ktorý Alica zdieľa s Charliem. Tak Alicino meranie v Bellovej bázi efektívne „teleportuje“ previazanie ktoré má s Charliem na Boba (viď obr. 6). Toto prenesenie previazania sa označuje pojmom *entanglement swapping* a pri experimentálnej realizácii opäť figuruje Anton Zeilinger [24].

Ak označíme jednotlivé častice v poradí ako na obr. 6 postupne C, A', A a B, tak analogicky k rovnici (5) vieme odvodiť

$$\begin{aligned}|\Phi_+\rangle_{CA'}|\Phi_+\rangle_{AB} = \frac{1}{2}\big[&|\Phi_+\rangle_{CB}|\Phi_+\rangle_{A'A} + |\Phi_-\rangle_{CB}|\Phi_-\rangle_{A'A} + \\ &+|\Psi_+\rangle_{CB}|\Psi_+\rangle_{A'A} + |\Psi_-\rangle_{CB}|\Psi_-\rangle_{A'A}\big] = \\ = \frac{1}{2}\big[&(I\otimes I|\Phi_+\rangle_{CB})|\Phi_+\rangle_{A'A} + (I\otimes\sigma_z|\Phi_+\rangle_{CB})|\Phi_-\rangle_{A'A} + \\ &+(I\otimes\sigma_x|\Phi_+\rangle_{CB})|\Psi_+\rangle_{A'A} + (I\otimes\sigma_x\sigma_z|\Phi_+\rangle_{CB})|\Psi_-\rangle_{A'A}\big],\end{aligned}$$

kde znova I označuje identitu a σ_x, σ_y a σ_z sú Pauliho matice. Tu vidíme, že Bob vie na základe informácie od Alice opraviť stav zdieľaný s Charliem na $|\Phi_+\rangle$ (prípadne iný Bellov stav – tieto sú ekvivalentné v rámci lokálnych operácií či už na strane Boba, alebo Charlieho) a vytvoriť tak previazaný stav bez toho, aby Bob musel byť kedykoľvek v blízkosti Charlieho.

Prenos previazania je dôležitým fenoménom pri praktickej komunikácii. Tá je v praxi prevádzaná výlučne opticky. Dôvodom je dobre rozvinutá technológia, obzvlášť možnosť využitia klasickej optickej infraštruktúry. Tá je totiž dostatočne kvalitná pre prenos kvantových stavov za pomoci jednotlivých fotónov. Úpravu tak vyžadujú len koncové zariadenia. Hlavnou nevýhodou však stále zostáva zoslabovanie signálu, kedy k poklesu o 1 dB príde po niekoľkých desiatkach kilometrov. Kvôli nemožnosti kopíro-

vania kvantovej informácie [32], [13] je toto výrazný problém, na ktorého odstránení sa intenzívne pracuje. Jedna z možností je použitie práve vyššie spomenutého prenesenia previazania. To však vyžaduje „autoritu“, ktorá sprostredkuje dané prehodenie (tu je to Alica). Z dlhodobého hľadiska teda nejde o optimálnu stratégiu. Tu opäť môžeme spomenúť výsledky Jian-Wei Pana [23], [26], kde bola komunikácia dosiahnutá na veľké vzdialenosti tým, že pri prenose signálu na satelit (Micius) máme efektívne len približne 40 km atmosféry a mimo nej dochádza k zoslabovaniu signálu len minimálne.

4. Nerealizovateľné zariadenia kvantovej fyziky

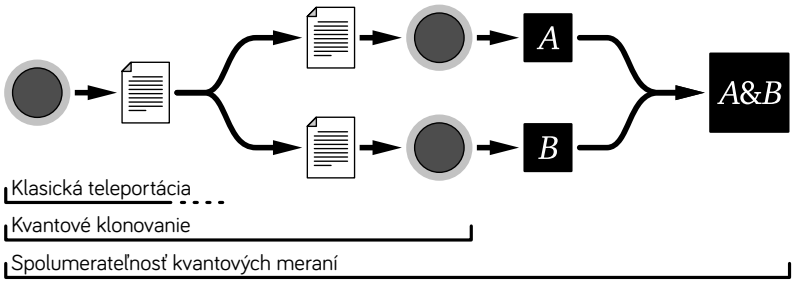
V predchádzajúcich častiach sme si predostreli previazanie nielen ako zaujímavý jav v kvantovej teórii, ale aj ako dôležitý zdroj pre praktické využitie. Previazanie je však neustále opradené tajomstvom, za ktorým veľa ľudí hľadá viac, než je v ňom skryté.[7] Jedným zo stálych dôsledkov nepochopenia previazania je snaha nájsť spôsob jeho využitia na komunikáciu nadsvetelnou rýchlosťou. Práve efekt akoby okamžitého pôsobenia na diaľku pri prevedení merania na previazanom stave priťahuje veľkú pozornosť. V tejto časti sa teda pozrieme na to, čo nám už kvantová teória nedovoľuje. Nebude prekvapením, že medzi tieto efekty patrí aj komunikácia nadsvetelnou rýchlosťou.

Práve v období, keď Bell publikoval svoj prelomový článok, dochádzalo v USA k znižovaniu podpory fyziky. Zároveň bol viditeľný nástup nových, často ezoterických, myšlienkových prúdov, do ktorých sa dostávali aj idey z kvantovej teórie (vlastne tak je tomu aj dnes). Na tej rozumnejšej (ak sa to tak dá povedať) strane ezoterického spektra v sedemdesiatych rokoch stála práve skupina vyštudovaných fyzikov, ktorí hľadali podporu aj u New Age hlásateľov. Títo sí hovorili *Fundamental Fysiks Group*. Jedným z týchto fyzikov je Nick Herbert, ktorého článok [21] z roku 1982 stojí za spomenutie. Viac si o tomto období môže zaujatý čitateľ prečítať v [22].

V článku [21] Nick Herbert popisuje práve zariadenie využívajúce previazanie na nadsvetelnú komunikáciu. Jeho zariadenie sa volá FLASH (First Laser-Amplified Superluminal Hook-up), ktoré je zostavené podľa obrázku 2, kde $A_1 = B_1 = \sigma_x$ a $A_2 = = B_2 = \sigma_z$, avšak, dajme tomu Bob, svoje fotóny znásobí, z nich polovicu pošle na meracie zariadenie B_1 a druhé na B_2. Idea je, že ak Alica previedla meranie $A_1 = \sigma_x$, tak polovica fotónov poslaná na B_1 bude nameraná v tom istom stave, zatiaľ čo druhá polovica poslaná do B_2 bude dávať náhodné výsledky. Alica by takto voľbou merania na svojej strane mohla posielať Bobovi informáciu nadsvetelnou rýchlosťou.

Tento článok bol zaslaný do časopisu Foundations of Physics a dostal sa až na recenzné konanie. Asher Peres, ako jeden z recenzentov, spomína na tento článok slovami [25]: „Bolo mi jasné, že tento článok nemôže byť správny, pretože porušoval špeciálnu teóriu relativity. Avšak bol som si istý, že to bolo jasné aj autorovi článku. Jeho argument však nemal žiadny vzťah k relativite, takže chyba musela byť inde... Doporučil som editorovi žurnálu článok publikovať. Napísal som, že článok je zjavne chybný, ale že očakávam, že vzbudí dostatočný záujem a že nájdenie chyby bude viesť k významnému pokroku v našom chápaní fyziky.“

[7] Reinhard Werner v [1] ponúka „lakmusový papierik“, ktorým môžeme zistiť funkčnosť nejakého paradoxu súvisiaceho s previazaním: „Vezmite si vysvetlenie autora k Bellovým nerovnostiam a nahraďte každú časticu ping-pongovou loptičkou. Ak to, čo autor prezentuje ako paradox, zostáva platné, autor nerozumie tomu, čo sa snaží vysvetliť.“



Obr. 7. Reťaz nerealizovateľných zariadení. Existencia zariadenia, ktoré by vedelo klasicky teleportovať kvantový stav, by umožnila jeho kopírovanie. To by umožnilo aj spolumerateľnosť nekompatibilných meraní. Existencia takéhoto zariadenia – krabička $A\&B$ – by nakoniec umožnila komunikáciu nadsvetelnou rýchlosťou

Ako sa rýchlo ukázalo, Asher Peres mal pravdu[8] a aj tento článok prispel k živému záujmu o teóriu kvantovej informácie. Konkrétne druhý recenzent, Giancarlo Ghirardi, poskytol dôkaz *no-cloning* teorémy, ktorá hovorí, že kvantová informácia sa nedá kopírovať (viac v [18]). Tento dôkaz bol poskytnutý ešte pred jeho prvou publikáciou Wootersom a Zurekom [32] ako aj Dieksom [13], ale autorstvo bolo Ghirardimu priznané len nedávno.

No-cloning teoréma je len jedným z kúskov kvantovej teórie, ktorý tvorí mozaiku obmedzení, ktoré v nej nachádzame. Príkladom je reťaz nerealizovateľných zariadení, ktorú poskytol Werner v kapitole 3 v [1]. Znázornená je aj na obrázku 7. Začiatok tejto reťaze je zariadenie, ktoré dokáže klasicky teleportovať kvantový stav, tzn. len za použitia klasickej informácie (bez previazania a iných kvantových javov) zrekonštruovať nejaký pred tým zaznamenaný kvantový stav. Toto zariadenie bude v tejto reťazi „najsilnejšie“, jeho existencia implikuje existenciu ďalších zariadení. Na druhú stranu neexistencia ktoréhokoľvek nasledujúceho zariadenia vylučuje aj existenciu všetkých predchádzajúcich.

Predpokladajme teda, že zariadenie pre klasickú teleportáciu kvantového stavu by existovalo. Keďže klasickú informáciu vieme kopírovať, tak by sme na základe takto získanej klasickej informácie mohli zostrojiť ľubovoľný počet kópií pôvodného stavu. Z predchádzajúcej diskusie vieme, že to nie je možné, a tak zariadenie zaznamenavajúce kvantový stav do klasickej informácie tiež nemôže existovať. My však môžeme ísť v implikovaní zariadení ešte ďalej. Predpokladajme, že by sme teda kvantovú informáciu vedeli kopírovať. Nič by nám nebránilo v tom, aby sme dve merania, ktoré teraz považujeme za komplementárne (vo všeobecnosti môžeme povedať nekompatibilné) previedli jedno na jednom stave a druhé na jeho kópii. Vedeli by sme tak prevádzať zároveň aj nekompatibilné merania.

Existencia takejto spolumerateľnosti však vedie k existencii zariadenia, pomocou ktorého by sa dalo komunikovať nadsvetelnými rýchlosťami. Dá sa to ukázať opäť použitím experimentu z obrázku 2, kde budeme predpokladať, že Bob má k dispozícii meracie zariadenie $B_1\&B_2$, ktoré vie vykonať zároveň meranie B_1 a B_2. Ak označíme

[8] Je však otázne, nakoľko by takýto prístup mal byť pri publikovaní akceptovaný.

$p(a_i, b_1, b_2) = p(a_i, (b_1, b_2)|A_i, B_1\&B_2)$ pre $i = 1, 2$, tak spolumerateľnosť znamená

$$\sum_{b_1} p(a_i, b_1, b_2) = p(a_i, b_2|A_i, B_2), \tag{6a}$$

$$\sum_{b_2} p(a_i, b_1, b_2) = p(a_i, b_1|A_i, B_1). \tag{6b}$$

Ak má Bob k dispozícii toto zariadenie, tak mu Alica môže poslať informáciu voľbou svojho merania A_1 alebo A_2 (za predpokladu, že jednotlivé merania sú vyberané s rovnakou frekvenciou, čo nie je výrazné obmedzenie). Bob potom interpretuje rovnosť medzi výsledkami $b_1 = b_2$ ako „A_1“ a nerovnosť $b_1 \neq b_2$ ako „A_2“. Toto nastavenie sa potom dá použiť na komunikáciu nadsvetelnou rýchlosťou, ak Bobova pravdepodobnosť p_{ok} správnej interpretácie Alicinho merania je väčšia ako 1/2. Táto pravdepodobnosť sa dá vyjadriť vzťahom

$$p_{\text{ok}} = \frac{1}{2} \sum_{a_1,b_1,b_2} \left| \frac{b_1 + b_2}{2} \right| \ |a_1| \ p(a_1, b_1, b_2) + \frac{1}{2} \sum_{a_2,b_1,b_2} \left| \frac{b_1 - b_2}{2} \right| \ |a_2| \ p(a_2, b_1, b_2),$$

kde prvý člen vyjadruje pravdepodobnosť správneho identifikovania „A_1“ a druhý člen pravdepodobnosť správneho identifikovania „A_2“. Tento vzťah sa dá zdola ohraničiť odstránením absolútnych hodnôt,

$$\begin{aligned} p_{\text{ok}} &\geqq \frac{1}{4} \sum_{a_1,b_1,b_2} (b_1 + b_2) a_1 \ p(a_1, b_1, b_2) + \frac{1}{4} \sum_{a_2,b_1,b_2} (b_1 - b_2) a_2 \ p(a_2, b_1, b_2) = \\ &= \frac{1}{4} \big[C(A_1, B_1) + C(A_1, B_2) + C(A_2, B_1) - C(A_2, B_2) = \frac{1}{4} \mathsf{B}, \end{aligned}$$

kde na redukciu na jednotlivé korelácie použijeme rovnosti (6).

Vidíme, že ak zvolíme merania také, že príde k narušeniu CHSH nerovnosti (4), tak $p_{\text{ok}} > 1/2$. Záverom je, že ak by sme mali zariadenie, ktoré prevádza nekompatibilné merania, viedlo by to k možnosti komunikácie nadsvetelnými rýchlosťami. Keďže aj toto je nemožné, všetky predchádzajúce zariadenia sú takisto nerealizovateľné – nemôžeme mať spolumerateľnosť, kopírovať kvantový stav, ani ho (vo všeobecnosti) klasicky zaznamenať.

Pozrúc sa z iného pohľadu [31] na CHSH nerovnosť, platí dualita medzi narušením nerovnosti a použitím nekompatibilných meraní. Konkrétne platí, že pre dva páry dvojvýsledkových meraní vieme narušenie nejakej nerovnosti v kvantovej teórii dosiahnuť vtedy a len vtedy, ak použijeme nekompatibilné merania (ako u Alice, tak aj u Boba). Toto vo všeobecnejších nastaveniach nie je vždy pravda, ale vždy platí, že na narušenie nejakej nerovnosti je nutné použiť nekompatibilné merania. Nekompatibilita je tak tiež priamo spojená s nemožnosťou komunikovania nadsvetelnými rýchlosťami a je zdrojom v podobnom ponímaní ako aj previazanie.

5. Diskusia

Previazanie malo od začiatku v teórii významné postavenie ako výrazne neintuitívny kvantový jav, na ktorý existovalo veľké množstvo interpretácií. Až výsledok Johna

Bella viedol k presunu chápania previazania z oblasti filozofie do exaktnej vedy. Jeho výsledky poskytli nielen možnosť overiť záhadné chovanie sa previazania a zúžiť jeho fundamentálne interpretácie (a napr. vylúčiť predpoklad lokálneho realizmu), ale ukázal aj, že kvantové korelácie môžu byť v istom zmysle silnejšie než tie klasické. Týmto jedným výsledkom sa otvoril priestor pre rozvoj nových oblastí výskumu založených na kvantovej teórii. Zároveň sa časom podarilo pochopiť, že obmedzenia kvantovej teórie nie sú vnímané ako niečo čo nás zväzuje, ale ako zdroj nových efektov využiteľných v praxi.

K pozitívnemu nazeraniu na tieto obmedzenia významnou mierou prispeli experimenty, za ktoré boli Alain Aspect, John F. Clauser a Anton Zeilinger ocenení Nobelovou cenou. Prví dvaja laureáti dokázali svojimi experimentami s narušením Bellových nerovností aký význam má práve previazanie a stimulovali ďalší vývoj v tejto oblasti. Tretí laureát svojimi mnohými inovatívnymi experimentami pomohol k nástupu *druhej kvantovej revolúcie*. Táto revolúcia prebieha aj dnes a je charakteristická schopnosťou bezprecedentne presne narábať s jednotlivými kvantovými stavmi a využívať ich na špecifické účely, akými sú kvantovo-asistovaná kryptografia, či kvantové počítanie. Výsledky všetkých spomenutých vedcov tak dláždia cestu k dnešnému rozmachu kvantových technológií.

L i t e r a t ú r a

[1] Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, H., Werner, R., Zeilinger, A.: *Quantum information: An introduction to basic theoretical concepts and experiments*. Springer, 2001.

[2] Aspect, A.: *Bell's inequality test: more ideal than ever*. Nature 398 (1999), 189–190.

[3] Aspect, A., Dalibard, J., Roger, G.: *Experimental test of Bell's inequalities using time-varying analyzers*. Phys. Rev. Lett. 49 (1982), 1804–1807.

[4] Aspect, A., Grangier, P., Roger, G.: *Experimental tests of realistic local theories via Bell's theorem*. Phys. Rev. Lett. 47 (1981) 460–463.

[5] Aspect, A., Grangier, P., Roger, G.: *Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities*. Phys. Rev. Lett. 49 (1982), 91–94.

[6] Bell, J. S.: *On the Einstein Podolsky Rosen Paradox*. Physics 1 (1964), 195–200.

[7] Bennett, C. H., Brassard, G.: *Quantum cryptography: Public key distribution and coin tossing*. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, 1984, 175–179; open-access vydanie pri príležitosti 30. výročia publikovania článku je v Theor. Comput. Sci. 560 (2014), 7–11.

[8] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K.: *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Phys. Rev. Lett. 70 (1993), 1895–1899.

[9] Bohm, D., Aharonov, Y.: *Discussion of experimental proof for the Paradox of Einstein, Rosen, and Podolsky*. Phys. Rev. 108 (1957), 1070–1076.

[10] Boschi, D., Branca, S., De Martini, F., Hardy, L., Popescu, S.: *Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Phys. Rev. Lett. 80 (1998), 1121–1125.

[11] Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: *Experimental quantum teleportation*. Nature 390 (1997), 575–579.

[12] Clauser, J. F., Horne, M. A., Shimony, A., Holt, R. A.: *Proposed experiment to test local hidden-variable theories*. Phys. Rev. Lett. 23 (1969), 880–884.

[13] Dieks, D.: *Communication by EPR devices*. Phys. Lett. A 92 (1982), 271–272.

[14] Einstein, A., Podolsky, B., Rosen, N.: *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev. 47 (1935), 777–780.

[15] Ekert, A. K.: *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett. 67 (1991), 661–663.

[16] Freedman, S. J., Clauser, J. F.: *Experimental test of local hidden-variable theories*. Phys. Rev. Lett. 28 (1972), 938–941.

[17] Garg, A., Mermin, N. D.: *Detector inefficiencies in the Einstein-Podolsky-Rosen experiment*. Phys. Rev. D 35 (1987), 3831–3835.

[18] Ghirardi, G.: *Entanglement, Nonlocality, Superluminal Signaling and Cloning*. In: P. Bracken (Ed.), Advances in Quantum Mechanics, IntechOpen, 2013.

[19] Giustina, M., Versteegh, M. A. M., Wengerowsky, S., Handsteiner, J., Hochrainer, A., Phelan, K., Steinlechner, F., Kofler, J., Larsson, J.-A., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M. W., Beyer, J., Gerrits, T., Lita, A. E., Shalm, L. K., Nam, S. W., Scheidl, T., Ursin, R., Wittmann, B., Zeilinger, A.: *Significant-loophole-free test of Bell's theorem with entangled photons*. Phys. Rev. Lett. 115 (2015), 250401.

[20] Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S., Ruitenberg, J., Vermeulen, R. F. L., Schouten, R. N., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M. W., Markham, M., Twitchen, D. J., Elkouss, D., Wehner, S., Taminiau, T. H., Hanson, R.: *Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km*. Nature 526 (2015), 682–686.

[21] Herbert, N.: *FLASH – A superluminal communicator based upon a new kind of quantum measurement*. Found. Phys. 12 (1982), 1171–1179.

[22] Kaiser, D.: *How the hippies saved physics*. W. W. Norton & Company, 2011.

[23] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., Pan, J.-W.: *Satellite-to-ground quantum key distribution*. Nature 549 (2017), 43–47.

[24] Pan, J.-W., Bouwmeester, D., Weinfurter, H., Zeilinger, A.: *Experimental entanglement swapping: Entangling photons that never interacted*. Phys. Rev. Lett. 80 (1998), 3891–3894.

[25] Peres, A.: *How the no-cloning theorem got its name*. Fortschr. Phys. 51 (2003), 458–461.

[26] Ren, J.-G., Hu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., Yang, K.-X., Han, X., Yao, Y.-Q., Li, J., Wu, H.-Y., Wan, S., Liu, L., Liu, D.-Q., Kuang, Y.-W., He, Z.-P., Shang, P., Guo, C., Zheng, R.-H., Tian, K., Zhu, Z.-C., Liu, N.-L., Lu, C.-Y., Shu, R., Chen, Y.-A., Peng, C.-Z., Wang, J.-Y., Pan, J.-W.: *Ground-to-satellite quantum teleportation*. Nature 549 (2017), 70–73.

[27] Shalm, L. K., Meyer-Scott, E., Christensen, B. G., Bierhorst, P., Wayne, M. A., Stevens, M. J., Gerrits, T., Glancy, S., Hamel, D. R., Allman, M. S., Coakley, K. J., Dyer, S. D., Hodge, C., Lita, A. E., Verma, V. B., Lambrocco, C., Tortorici, E., Migdall, A. L., Xhang, Y., Kumor, D. R., Farr, W. H., Marsili, F., Shaw, M. D., Stern, J. A., Abellán, C., Amaya, W., Pruneri, V., Jennewein, T., Mitchell, M. W., Kwiat, P. G., Bienfang, J. C., Mirin, R. P., Knill, E., Nam, S. W.: *Strong loophole-free test of local realism*. Phys. Rev. Lett. 115 (2015), 250402.

[28] Shor, P. W.: *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, 124–134.

[29] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., Zeilinger, A.: *Entanglement-based quantum communication over 144 km*. Nat. Phys. 3 (2007), 481–486.

[30] Weihs, G., Jennewein, T., Simon, C., Weinfurter, H., Zeilinger, A.: *Violation of Bell's Inequality under strict Einstein locality conditions*. Phys. Rev. Lett. 81 (1998), 5039–5043.

[31] Wolf, M. M., Perez-Garcia, D., Fernandez, C.: *Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory*. Phys. Rev. Lett. 103 (1009), 230402.

[32] Wootters, W. K., Zurek, W. H.: *A single quantum cannot be cloned*. Nature 299 (1982), 802–803.