NÁVRH ÚVODNÉHO KURZU KVANTOVEJ MECHANIKY PRE INFORMATIKOV

SITKEY Matúš, SR

Resumé

Článok je úvodom do problematiky kvantovej informatiky. Jeho cieľom je jednoduchou formou ozrejiť problematiku kvantového bitu – qubit. Vychádzame z opisu kvantového systému. Následne pomocou Machovho–Zenderovho interferometra vysvetľujeme princíp superpozície, ako elementárny pojem kvantovej fyziky. Nadväzujúc na uvedenú teóriu kvantovej informatiky je spracovaná problematika kvantových registrov prinášajúca vysokú operačnú rýchlosť kvantových počítačov. Uvedená teória bola spracovaná ako úvod kurzu kvantovej fyziky pre študijné zameranie orientované na informatiku, perspektívne na špecializáciu kvantová informatika.

Kľúčová slova: superpozícia, qubit, kvantový register, kvantové počítanie.

PROPOSAL FOR THE INITIAL COURSE OF THE QUANTUM MECHANICS FOR INFORMATICS

Abstract

Quantum mechanics has been traditionally taught copying its historical development. This process for the quantum informatics purposes is not effective. Quantum informatics deals mainly with two state systems, therefore, from the aspect of its needs, it is better to begin with the description of the simplest quantum systems. Such a system, for example, is a particle with the spin of $\frac{1}{2}$, if we are considering just its spin property, while these are described in two dimensional state space which is the basis also for the description in informatics. The key position of the paper is a simple quantum-theoretical description of the systems keeping the information and physical processes of the information processing as well as comparison of the classic and quantum description of such systems. The aim of this contribution is, on one hand, the choice of thematic units, on the other hand, methodological approaches and didactic methods suitable to processing of the introductory course of the quantum theory for the field of study oriented to informatics, prospectively to the specialisation of the quantum informatics. Here we used the methods of quantum mechanics description of simple systems derived from classic and current literature sources as well as new processes of the manipulation with quantum states pushed from the current magazine publication sources. The outcome has been a view of the introduction into quantum mechanics, the introduction of the quantum system and quantum state conception, the introduction of the state superposition principle and the introduction of the quantum co - relation states specifications in such a superposition. The key point is the two state system description used in informatics - the approach leading to the application of the quantum bit - qubit - as well as the application of the quantum data registers and their quantum measurement. We analyse on simple examples the background of the quantum calculations with the emphasis on the role of the entangled states and the quantum parallelism. The main gain of this contribution is to point out on another than the classic approach to the quantum mechanics through a two state system and the description of the basic terms leading to quantum informatics with the emphasis on qubit.

Key words: superposition, qubit, quantum register, quantum computing.

Úvod

Dnešný život bez počítačov a informačných technológií si už ani nevieme predstaviť. Sprevádzajú nás na každom kroku či už v práci, na verejnosti alebo súkromí. S narastajúcim rozšírením počítačových technológií stúpa i potreba na ich výkon a pamäťové schopnosti. Hoci technológie sa rozvíjajú rýchlym tempom, sú prípady, keď potreby ich praktického nasadenia sú limitované možnosťami binárnych technológií. Ide najmä o simulácie dejov v reálnom čase alebo o náročné matematické výpočty v kryptológii a kryptoanalýze. Riešenie tohto problému prichádza vo forme kvantových počítačov. Čo je kvantový počítač? Je to vlastne počítač, ktorý na rozdiel od klasických binárnych počítačov na vykonávanie výpočtov algoritmov a ukladanie dát priamo využíva pri svojej činnosti kvantovo mechanické fenomény, akými sú napríklad superpozícia alebo kvantové previazanie. V klasickom alebo konvenčnom počítači je množstvo dát určené bitmi, v kvantovom počítači sa používajú qubity - kvantové bity. Základným princípom kvantových výpočtov je i to, že kvantové vlastnosti častíc sa môžu použiť na reprezentáciu a štruktúru dát a kvantové mechanizmy sa môžu použiť na vykonávanie operácií s týmito dátami. Takýto kvantový počítač dokáže vykonať matematickú operáciu hoci aj nad miliardou čísel naraz, tento výpočet sa volá kvantový paralelizmus. Ale ako to všetko vlastne funguje? Odpoveď prináša kvantová mechanika, ktorej základy je potrebné poznať, aby sme s princípmi fungovania kvantových počítačov vedeli zmysluplne narábať. V tejto súvislosti prirodzene vystupuje otázka ako voliť základný kurz kvantovej mechaniky pre potreby informatikov.

1 Opis kvantového systému

Fyzikálna realizácia pamäťových prvkov počítačov je založená na dvojstavových fyzikálnych systémoch, ktoré reprezentujú jednotku informácie 1 bit. Dvojhladinový kvantový systém predstavuje ten najjednoduchší kvantovomechanický systém. Tento fakt priamo núka koncipovať základný kurz pre informatikov vyšetrovaním vlastností opisu najjednoduchšieho kvantového systému – dvojhladinového systému. Prototypom takéhoto systému je napr. častica so spinom $\frac{1}{2}$, keď abstrahujeme od ostatných premenných a zaujíma nás len opis spinu. Vhodné je preto začať napr. analýzou Sternovho – Gerlachovho experimentu merania priemetu spinu (ďalej len „S-G“) do zvoleného smeru. Nech prístroj je nastavený tak, že meria priemet spinu do zvislého smeru. Potom vo všeobecnosti zväzok častíc so spinom $\frac{1}{2}$ nalietaťavajúci do prístroja sa za prístrojom rozdelí na dva zväzky, jeden nasmerovaný nahor a zodpovedajúci priemetu spinu orientovanému nahor a druhý podobne smerujúci nadol. Ak by sme do cesty horného zväzku postavili rovnako natočený Sternov – Gerlachov aparát, tak v takomto prípade by z neho vychádzal už len horný zväzok. Teda častica, ktorú sme po prechode cez S-G identifikovali, že má priemet spinu nahor, pri ďalšom meraní na S-G rovnako natočenom bude mať priemet spinu vždy smerujúci nahor. Podobnú skúsenosť získame s dolným zväzkom. Tento fakt nás, v súlade so zaužívanou klasickou predstavou o stave systému, oprávňuje hovoriť o časticiach v hornom zväzku za S-G, že sú v spinovom stave priemetu spinu nahor (a podobne v dolnom zväzku v stave priemetu spinu nadol). Ak by však druhý S-G nebol natočený vo zvislom smere, potom by už z neho vychádzali znova dva zväzky a nasledujúcim tretím S-G natočeným zvisle by sme už nemohli zreprodukovať hodnotu priemetu spinu vo zvislom smere, ktorú mala častica pred druhým S-G. Teda akoby v stave reprezentujúcom priemet spinu nahor boli zakomponované aj dva stavy priemetu spinu do smeru natočenia druhého S-G. To navodzuje myšlienku superpozície stavov, ktorej sa budeme venovať v ďalšej časti. Navyše meranie na druhom S-G zmazalo informáciu o stave priemetu spinu pred týmto meraním. Vidíme, že nie je možné súčasne zmerať priemet spinu do smeru zvislého a smeru zvierajúceho s ním nenulový uhol. Hovoríme, že tieto dve veličiny (dva priemety) sú nekompatibilné, nedajú sa súčasne merať.

Výsledok ich merania závisí od poradia, v ktorom ich budeme merať. Tieto dve základné odlišnosti vlastností kvantového stavu a kvantovej veličiny od ich protipólov v klasickej fyzike sú zdrojom zvláštností správania sa kvantových systémov. Výborným úvodom do problematiky je kniha o kvantovom meraní na jednotlivom systéme (Alter - Yamamoto, 2001).

V nasledujúcich častiach objasníme základné vlastnosti kvantovej superpozície stavov a niektoré termíny z oblasti kvantových počítačov, ktoré vyplývajú zo špecifik ich kvantového charakteru.

2 Kvantová superpozícia

Kvantová teória patrí medzi úspešné a najtestovanejšie fyzikálne teórie, avšak niektoré jej závery sú začiatočníkmi štúdia fyziky vnímané ako zvláštne, či ťažko pochopiteľné. Príčinu možno hľadať v tom, že náš pojmový systém bol formovaný zmyslovou interakciou s makrosvetom a kvantová teória opisuje vlastnosti mikrosвета. Najzákladnejšou a najrozporuplnejšou črtou kvantovej teórie z hľadiska klasického chápania stavu je superpozícia kvantových stavov. Dôležité je vedieť, že princíp superpozície stojí v pozadí všetkých odlišností kvantového opisu sveta od klasického (Petrovič, 2015). Princíp superpozície odráža vlastnosť kvantového sveta existovať v superpozícií viac stavov. Je to dôležitá vlastnosť, ktorá sa stala axiómou kvantovej mechaniky. Vo všeobecnosti princíp superpozície hovorí to, že ak je rovnica popisujúca skúmaný fyzikálny systém lineárna a vezmeme jej nejaké dve riešenia, tak aj lineárna kombinácia týchto riešení je tiež jej riešením.

Objasníme si, čo je to superpozícia na príkladoch. Nasledovný model, na ktorom si ukážeme princípy superpozície, je vysvetlenie superpozície pomocou Machovho - Zenderovho interferometra. Machov - Zenderov interferometer je zariadenie, ktoré sa skladá z emitora fotónov a sústavy dvoch polopriepustných zrkadiel PZ1 a PZ2, dvoch klasických zrkadiel Z1 a Z2, pričom na vyhodnotenie výsledných dopadajúcich lúčov fotónov sú dva detektory D1 a D2. Pri polopriepustných zrkadlách môžeme uvažovať, že fáza vlny sa po prechode nemení, avšak po odraze svetelného zväzku na nich a na zrkadlách dochádza k fázovému posunu o 90° . Koncové detektory lúčov vyhodnocujú fázový súčet lúčov do neho prenikajúcich. Po emisii lúča zo zdroja časť prejde polopriepustným zrkadlom PZ1 (modrý lúč), a časť zmení smer, odrazí sa (čiarkovaný červený lúč – obr. 1) Čo zaznamenajú detektory? Detektor D2 vzhľadom na skutočnosť, že do neho súčasne vchádzajú dve vlnenia s opačnou fázou, nezaznamená nič, nakoľko nastane deštruktívna interferencia, teda amplitúdy oboch prichádzajúcich lúčov sa interferenciou navzájom eliminujú. Naopak, detektorom D1 zaznamenáme všetky častice, pretože zväzky sú vo fáze, čím nastane konštruktívna interferencia. Ale čo sa stane v prípade, ak touto aparátúrou necháme prechádzať iba jediný fotón? Výsledok bude zaujímavý. Jeden fotón rovnako vždy zaregistrujeme iba v detektore D1. Osamotený fotón teda musel byť v superpozícií, prejsť oboma ramenami a interferovať sám so sebou!

Ďalším variantom experimentu s Machovým - Zenderovým interferometrom je prípad, keď odstránime polopriepustné zrkadlo PZ2. V takomto prípade fotón nemá na čom interferovať a my ho nameriame buď na detektore D1, alebo D2 s rovnakou pravdepodobnosťou. Nepozorujeme, že by oba detektory zaregistrovali dopad fotónu súčasne, v koincidencii. Tento fakt sme nútení interpretovať tak, že fotón sa na polopriepustnom zrkadle PZ1 nerozdelí na dve časti, ale vždy putuje ako celok len jedným ramenom. Tým, že sme odstránili polopriepustné zrkadlo PZ2, získali sme informáciu o ceste fotónu do detektora D1 resp. D2, a tým superpozícia zanikne. Ak by sme sa pokúsili fotón nachytať tak, že polopriepustné zrkadlo vložíme do aparátúry až po tom, čo sa za polopriepustným zrkadlom PZ1 dal na cestu jedným alebo druhým ramenom, očakávajúc registráciu fotónu v detektore D1 a D2 s rovnakou pravdepodobnosťou, nepodari sa nám to a fotón budeme

registrovať len v detektore D1. Vidíme, že ak máme principiálnu možnosť zistiť ktorým ramenom fotón prešiel, správa sa ako klasická častica. V prípade, že tú možnosť principiálne nemáme, aby sme vysvetlili správanie sa fotónu (jeho dopad zaregistruje len detektor D1), musíme uvažovať, že fotón je v superpozícii stavov prechodu oboma ramenami interferometra.

Obrázok 1 – Machov-Zenderov interferometer (zdroj: Autor)

3 Qubit

V klasickej informatike môže byť logická úroveň len 1 alebo 0, teda nič medzi tým. Reprezentantom takéhoto systému môže byť spínač, ktorý je buď zapnutý 1 alebo vypnutý 0. To, že máme k dispozícii takéto zariadenie, to nám umožňuje zakódovať informáciu vopred dohodnutým kódom do radu využitím dvojkovej sústavy, teda jednotiek a núl. Možno teda povedať, že klasické bity sú základným stavebným kameňom klasickej teórie informácie rozpracovanej C. Shannonom. Klasický bit je založený na dvoch rôznych stavoch, a to buď 0 alebo 1. Obdobne kvantová teória informácie je založená na kvantovom bite, qubite (quantum bit), reprezentovanom dvojhladinovým kvantovým systémom. Týmto hladinám zodpovedajú dva stavy systému, avšak ako už bolo spomenuté, kvantová mechanika pripúšťa aj stavy tohto systému, ktoré sú ich ľubovoľnou superpozíciou. Matematické vyjadrenie ideu qubitu si ukážme na príklade izolovaného qubitu. Qubit môžeme definovať ako (jednotkový) vektor vo dvojrozmernom vektorovom priestore nad komplexnými číslami, ktorého bázové vektory sú $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ a $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ (Nakahara, 2008). Fyzikálna realizácia vektorov závisí od fyzikálneho systému, môže byť reprezentovaná spinom elektrónu alebo atómu, polarizáciou fotónu, stavom energie kvantovej jamy a podobne. Qubit sa od klasického bitu rozlišuje v tom, že okrem stavov $|0\rangle$ a $|1\rangle$ môže byť aj v stave všetkých možných superpozícií $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle = \omega_0\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \omega_1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \omega_0 \\ \omega_1 \end{pmatrix}$, kde ω_0, ω_1 sú komplexné čísla splňujúce vzťah $|\omega_0|^2 + |\omega_1|^2 = 1$. Koeficienty ω_0 a ω_1 nazývame amplitúdami pravdepodobnosti. Druhá mocnina absolútnej hodnoty koeficienta ω_0 (ω_1), nám hovorí s akou pravdepodobnosťou prejde $|\psi\rangle$ do stavu $|0\rangle$ ($|1\rangle$). Výsledkom zisťovania stavu qubitu kvantovým meraním je registrácia vždy len jedného z dvoch základných stavov a nie ich superpozícií. Aj keď je počet všetkých možných superpozícií stavov qubitu neohraničený, v praxi často stačí uvažovať iba dva základné stavy $|0\rangle$ a $|1\rangle$ a ich dve základné superpozície $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ a $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, resp. $\frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$, lebo s nimi pracuje väčšina navrhovaných kvantových informačných systémov. Pre lepšiu vizualizáciu qubitu slúži grafická pomôcka nazývaná Blochova sféra. Každý jeden bod na sfére zodpovedá jednému stavu qubitu.

Napríklad severný a južný pól na Blochovej sfére predstavujú stavy $|0\rangle$ a $|1\rangle$, všeobecný stav $|\psi\rangle$ sa dá popísať zadaním uhlov φ a θ , situáciu znázorňuje obrázok číslo 2.

Obrázok 2 – Klasický bit a qubit (zdroj: Autor)

Koeficienty superpozície $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$ súvisia s danými uhlami vo vyjadrení na Blochovej sfére nasledovne:

$$\omega_0 = \cos\theta$$

$$\omega_1 = e^{i\varphi} \sin\theta,$$

kde koeficient ω_0 sa volí ako reálne číslo (Preskill, 1998).

4 Kvantové počítanie

Keď už vieme zakódovať informáciu pomocou jednotiek a núl do istého stavu mali by sme s týmto stavom istým spôsobom narábať, meniť ho. Ak zmeníme tento stav na iný stav podľa istých logických krokov, hovoríme, že počítame. S myšlienkou kvantového počítania prišiel R. P. Feynman. Pre kvantové počítanie sú modelom kvantové počítačové obvody. Kvantový počítačový obvod je systém skladajúci sa z dvoch kvantových výpočtových prostriedkov, qubitov a kvantových brán. Okrem toho sú dôležité i pomocné obvody zabezpečujúce ich činnosť. Patria medzi ne napríklad i obvody pre uvedenie qubitov do určitého štandardného východiskového stavu, obvody pre zisťovanie stavu qubitov, inicializáciu logických operácií vodivé prepojenia prenášajúce údaje a povely atď. Matematicky je kvantové hradlo reprezentované unitárnym operátorom $\hat{U}$, ktorý zmení kvantový stav $|\psi\rangle$ na stav $\hat{U}|\psi\rangle$. Kvantový výpočet realizovaný viacerými kvantovými bránami potom môže byť uskutočnený jediným operátorom určeným maticovým súčinom operátorov jednotlivých hradiel. Rozdiel medzi klasickým a kvantovým počítaním je práve v unitárnosti kvantových operátorov, čo je dôsledkom princípu superpozície, z čoho vyplýva, že kvantový výpočet je z definície reverzibilný. Nevratnosť kvantového výpočtu je do výpočtu vnesená až neskôr, kedy chceme získať výsledok prostredníctvom merania. Spracovanie informácie o stave jedného alebo niekoľko qubitov kvantovou bránou je ekvivalentné násobeniu vektora stavu maticou prislúchajúcou hradlu $\hat{U}|\psi\rangle \rightarrow \mathbb{U}|\psi\rangle$. Elementárne jedno qubitové operácie sú matematicky vyjadrené Pauliho maticami X, Y a Z, ktoré reprezentujú unitárne operácie. Pauliho matice sú množina 2x2 komplexných hermitovských,

unitárných matic, a to $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ a $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Uvažujme najjednoduchší prípad, keď qubit, na ktorý sú aplikované príslušné operátory sa nachádza v jednom zo svojich dvoch báзовých stavoch. Potom funkcia X realizovaná Pauliho bránou X , mení jeho stav z $|0\rangle$ na $|1\rangle$ a opačne. Táto matica predstavuje ekvivalent funkcie NOT klasickej logiky. Funkcia Y mení stav qubit z $|0\rangle$ na $i|1\rangle$ a stav $|1\rangle$ na $-i|0\rangle$. Pauliho matica Z , zachováva stav qubit z $|0\rangle$ a mení stav $|1\rangle$ na $-|1\rangle$. Medzi základné funkcie kvantových obvodov patrí aj funkcia H matematicky opísaná maticou $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ a realizovaná Hadamardovým hradlom H . Výsledkom pôsobenia tejto matice na kvantový objekt je uvedenie daného objektu do vyváženého superpozičného stavu.

5 Kvantové previazanie dvoch systémov

V kvantovej mechanike existujú stavy, ktoré porušujú „lokálnosť“, na akú sme zvyknutí z bežného života. Napríklad dve častice so spinom $1/2$, pokiaľ sú v tzv. singletnom stave, t. j. stave s celkovým spinom rovnajúcim sa nule, udržiavajú si medzi sebou akési „puto“. Nie je dopredu určený spin prvej častice, môže rovnako dobre (s pravdepodobnosťou 50 %) byť smerom hore aj dole. Ak ho raz však zmeriame, určíme aj výsledok prípadného neskoršieho merania spinu na druhej častici v tom istom smere. Nezávisle na tom, ako je ďaleko, priestorovo alebo časovo. Na jednej strane je ťažko predstaviteľné, ako sa informácia o našom meraní môže dostať k druhej častici. Z pohľadu kvantovej mechaniky nejde o dva systémy, ale o jeden jediný systém, ktorý sa zmenil ako celok po zmeraní spinu na prvej častici. A medzi dvoma časťami jedného systému vzniká väzba, previazanie. Hovoríme, že dve časti systému sú previazané (entangleované), resp. neseperovateľné (Plesch, 2004).

6 Kvantové registre

Zatiaľ sme uvažovali len izolovaný kvantový systém, ktorý predstavoval jeden qubit. Klasické počítače sú vybavené registrami skladajúcich sa z niekoľko bitových registrov. Analogicky v kvantových počítačoch sú kvantové registre. Pod pojmom kvantový register rozumieme sústavu istého počtu vzájomne komunikujúcich reprezentantov qubitov nachádzajúcich sa buď v čistých báзовých stavoch, alebo v ich superpozíciách. Kvantové registre predstavujú jadro každého kvantového počítača. Model, v ktorom treba popísať viacej qubitov sa v kvantovej mechanike zapisuje ako direktný tenzorový súčin viac stavov, ktoré zapisujeme pomocou operácie $\otimes$. Formálne tak vytvoríme nový priestor generovaný tenzorovým súčinom. Pre dva qubity možno písať $|\psi_a\rangle \in \mathcal{H}_1$ a $|\psi_b\rangle \in \mathcal{H}_2$, potom $|\psi_a\rangle \otimes |\psi_b\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$.

Ďalej platí $|\psi_a\rangle \otimes |\psi_b\rangle = \begin{pmatrix} \omega_{0a} \\ \omega_{1a} \end{pmatrix} \otimes \begin{pmatrix} \omega_{0b} \\ \omega_{1b} \end{pmatrix} = \begin{pmatrix} \omega_{00} \\ \omega_{01} \\ \omega_{10} \\ \omega_{11} \end{pmatrix} = |\psi_{ab}\rangle$. Odtiaľto dostaneme sadu nových

amplitúd pravdepodobnosti, ktoré zodpovedajú zloženým stavom $|00\rangle$, $|01\rangle$, $|10\rangle$ a $|11\rangle$. Nová báza

bude vyzeráť $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ a $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. Tento dvojqubitový pamäťový

register vyjadríme $|\psi_{ab}\rangle = \omega_{00}|00\rangle + \omega_{01}|01\rangle + \omega_{10}|10\rangle + \omega_{11}|11\rangle$ Takýmto spôsobom môžeme vytvoriť kvantové registre dĺžky n . Ak $B_1, B_2, \dots, B_n$ sú ortonormálnymi bázami priestorov $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$, potom $B = \bigotimes_{i=1}^n B_i$ je ortonormálna báza priestoru $\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i$. Pridaním ďalšieho qubit do registra sa zdvojnásobuje počet možných stavov registra. Všeobecne, systém n qubitov

vytvára kvantový register s kapacitou n , pričom tento register sa môže nachádzať v 2^n rôznych stavoch súčasne. Na kľúčovú rolu kvantového registra upozornili kvantoví fyzici, keď pri výpočtoch vlastností kvantových systémov a simuláciách ich správania pomocou klasických počítačov narazili na problém exponenciálneho rastu zložitosti tejto úlohy s rastom počtu elementárnych kvantových objektov systému (Petrovič, 2015). Práve schopnosti qubitov existovať v kvantovej superpozícii vďaka kvantové počítače mimoriadne vysokej rýchlosti výpočtu, lebo vďaka stavu superpozície kvantový register obsahuje vo svojich qubitoch súčasne všetky možné varianty výpočtu.

Záver

Príchod modernej kvantovej teórie znamená prelomovú zmenu vo formovaní predstáv o povahe fyzikálneho sveta prinášajúcu revolúciu v chápaní fyzikálnych procesov. Z uvedeného dôvodu znalosť kvantových ideí by sa mala stať súčasťou všeobecného vzdelania gymnaziálnych a odborných škôl technického smeru. Táto potreba vzrastá i s prichádzajúcou syntézou informatiky a kvantovej fyziky do jedného vedeckého odboru kvantovej informatiky. Uvedený príspevok predstavuje prvotné úvahy o tom, ako koncipovať úvodný kurz kvantovej mechaniky určený práve pre túto cieľovú skupinu študentov. Jeho hlavnou ideou bolo sústrediť sa na objasnenie pojmu kvantového systému, kvantového stavu, princípu superpozície stavov, problému nekompatibility veličín a z neho plynúcich vplyvov na výsledok kvantového merania. Snahu naplnenia tohto cieľa predstavujú jednotlivé kapitoly prezentovaného príspevku, v ktorých je stručne spracovaný opis dvojstavového systému použitého v informatike, ktorý vedie k zavedeniu kvantového bitu – qubit a následne kvantovým registrom dát a ich kvantového merania. Na jednoduchých príkladoch bola okrem iného spracovaná aj analýza pozadia kvantových výpočtov. Na záver môžeme vysloviť názor, že prichádzajúca éra kvantovej informatiky môže v tomto storočí spôsobiť porovnateľnú revolúciu vo všetkých oblastiach ľudského života tak, ako spôsobili klasické binárne informačné technológie v dvadsiatom storočí.

Literatúra

- Alter, O. & Yamamoto, Y. (2001). *Quantum Measurement of a Single System*. New York.: John Wiley and Sons, Inc. 136 s. ISBN 0-471-28308-8
- Nakahara, M. & Ohmi, T. (2008). *Quantum Computing. From Linear Algebra to Physical Realizations*. Boca Raton, USA: Taylor & Francis Group. 421 s. ISBN 978-0-7503-0983-7
- Peres, A. (2002). *Quantum Theory: Concepts and Methods*. New York, USA: Kluwer Academic Publishers. 446 s. ISBN 0-792-33632-1
- Petrovič, P. (2015). FYZIKA II. *Vybrané kapitoly zo základov modernej fyziky a kvantových počítačov*. Košice, Slovenská republika: EQUILIBRIA. 526 s. ISBN 978-80-8143-152-4
- Plesch, M. (2004). *Kvantové korelácie v mnohočasticových systémoch*. Bratislava: SAV. Dostupné dňa 30.7.2018 na : <http://www.quantum.physics.sk/rcqi/docs/thesis2005_plesch.pdf>
- Preskill, J. (1998). *Quantum Information and Computation*. California: Institute of Technology. Dostupné dňa 30.7.2018 na : <<http://www.theory.caltech.edu/~preskill/ph219/index.html#lecturev>>

Kontaktní adresa:

Matúš Sitkey, Mgr.

Katedra fyziky, Fakulta prírodných vied, Tr.Andreja Hlinku 1, 949 74

Nitra, SR, tel.:+421917 570 956, e-mail: matus.sitkey@ukf.sk