Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék
Mobil Kommunikáció és Kvantumtechnológiák Laboratórium

Kvantum alapú hálózatok - bevezetés

Mérési útmutató

A mérést kidolgozta:

Dr. Bacsárdi László
Galambos Máté
Dr. Imre Sándor

Budapest, 2014

Jelen mérési útmutató a BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium által tartott „Kvantum alapú hálózatok – bevezetés" című mérésre készült. Az útmutatóval és a mérési feladatokkal kapcsolatos észrevételeket, megjegyzéseket a szerzők szívesen fogadják a bacsardi@hit.bme.hu címen.

1. Bevezetés

A kvantumjelenségek, amelyek még Einsteint is megdöbbentették, lehetővé teszik, hogy olyan kvantum alapú algoritmusokat alkossunk, amelyek a hagyományos társaikhoz képest hatékonyabban (gyorsabban, kevesebb művelettel) oldanak meg számításelméleti feladatokat, és biztonságosabbá teszik a kommunikációt. A kvantuminformatika születését a 80-as évek közepére tehetjük, ekkor publikálta először David Deutsch a kvantumszámítógép elméleti leírását, és ekkor jelent meg Bennett és Brassard cikke, amelyhez a kvantumkriptográfia születését köthetjük. Mára számtalan cég kínál kvantum alapú kulcsszétosztó rendszereket, mint például az 1999-ben alapított amerikai MagiQ Technologies, a 2001-ben egyetemi spin-off cégként alakult svájci id Quantique és az ausztrál QuintessenceLabs. A kanadai D-Wave System cég 2011 májusában mutatta be a D-Wave One nevű számítógépet, amely állításuk szerint egy 128 kvantumbites processzort használ.

Jelen mérésnek az a célja, hogy egy rövid áttekintést adjon a kvantum alapú hálózatok világáról, bemutatva néhány érdekes területet.

2. Kvantuminformatikai alapok – olvasmányosan

Jelen fejezet a Természet Világa folyóiratban 2013 januárjában megjelent, Bacsárdi László és Imre Sándor által írt tudománynépszerűsítő cikk felhasználásával készült.

Kvantummechanikai alapokon

Sok ember számára a kvantummechanika szó régi, homályos emlékeket jelent, bonyolult egyenletekkel és matematikai műveletekkel. Mi mérnökként az alkalmazás és alkalmazhatóság oldaláról közelítjük meg ezt a területet, és a Schrödinger-egyenletek által leírt világot négy kvantummechanikai posztulátumra helyezzük. (Innentől kezdve a mindennapi világra klasszikus világként és klasszikus informatikaként fogunk hivatkozni). Az első a rendszer állapotát írja le, a második az időbeli fejlődésre vonatkozik, és abban segít, hogy a teljes rendszer viselkedését zárt transzformációkkal tudjuk leírni. A harmadik a mérésre vonatkozik, és definiálja a kapcsolatot a kvantumvilág és a klasszikus világ között, a negyedik pedig az összetett rendszerekre vonatkozik.

Az első posztulátum lehetővé teszi, hogy bevezessük a kvantumbit fogalmát (angolul quantum bit vagy qubit), amely a kvantuminformatika alapvető információs egysége. Míg a klasszikus bit esetében két jól meghatározott értékről beszélünk (0 és 1), addig a kvantumbit az előző két alapállapot tetszőleges kombinációjában (ún. szuperpozíciójában) létezhet, azaz végtelen sok állapotban lehet. Amikor azonban végrehajtjuk a mérést, akkor egy klasszikus 0 vagy 1 értéket kapunk vissza. A kvantumbitet a bázisállapotai és komplex valószínűségi amplitúdóival adjuk meg, az alábbi módon:

$$|\varphi\rangle = a|0\rangle + b|1\rangle \qquad (1)$$

ahol az *a* és *b* komplex számok. Az a és b valószínűségi amplitúdó abszolútértékének négyzete azt mutatja meg, mekkora valószínűséggel mérünk 0-t illetve 1-et (innen származik a valószínűségi amplitúdó elnevezés), a két valószínűség összege pedig 1-et ad. A fenti zárójelezést a Dirac-jelölést követve használjuk, és a fenti kvantumbitet „ket fi”-nek ejtjük (és ehhez hasonlóan, „ket nulláról” és „ket egyről” beszélünk). Ha például a=0,6 és b=0,8·i, akkor 0,36 valószínűséggel 0-át kapunk a mérés végén, 0,64 valószínűséggel pedig 1-et. Mivel egységnyi hosszú vektorokról beszélünk, a legegyszerűbb egy Descartes-féle koordinátarendszerben körként elképzelni a kvantumbitet, a körvonal tetszőleges pontja lehet a bitünk értéke. (Ez a kétdimenziós kvantumbit, de tudjuk definiálni magasabb dimenziókra is.) A két tengely pedig a két bázisállapot, a „ket nulla” és a „ket egy”. Természetesen a körvonal csak egy geometriai megfeleltetés, ha szeretnénk, akkor Felix Bloch nyomán akár a Bloch-gömbön is ábrázolhatjuk a kvantumbitet (ekkor a gömb felületén vehet fel tetszőleges értéket).

Fizikailag kvantumbit lehet bármilyen két jól megkülönböztethető állapottal rendelkező kvantumrendszer (pl. elektron jelenléte vagy hiánya, elektron spinállapotai, atomi hiperfinom állapotok, stb.), a kommunikáció területén a foton különböző polarizációs állapotait (vízszintes, függőleges) feleltetjük meg a bázisállapotoknak.

A mérési posztulátum rámutat arra, hogy a mérőműszerünk csak valamekkora valószínűséggel mutatja a mérés végeredményét. Ha a valós világban ráállunk egy mérlegre, biztosak lehetünk abban, hogy újra és újra megismételve a kísérletet ugyanazt az értéket mérjük (kivéve, ha közben elfogyasztottunk egy bőséges vacsorát), és a mérleg valóban a testsúlyunkat mutatja. A kvantummérlegre ráállva nem lehetünk biztosak abban, hogy a megjelenő hatalmas szám valóban a sok elfogyasztott süteményt tükrözi, vagy éppen nem a helyes értéket látjuk. De ez a posztulátum még egy érdekességet tartogat: a mérés hat a teljes rendszerre, és megváltoztatja annak állapotát. Vagyis azáltal, hogy ráállunk a mérlegre, megváltozunk mi magunk és a mérleg is. Mindezek alapján leszögezhetjük, hogy egy-egy mérési elrendezés megtervezése különösen fontos a kvantuminformatikában. Ha rosszul választjuk ki a mérési operátorokat (vagyis rosszul állítjuk be a mérőműszert), akkor könnyen előfordulhat, hogy nem értelmezhető eredményt kapunk. Szerencsére jól bevált receptek állnak rendelkezésünkre, mint például a projektív mérés (más néven Neumann-mérés) vagy a pozitív operátor értékű mérés (az angol positive-operator valued measure elnevezés rövidítéséből POVM).

A kvantumbitek állapotait egyetlen rendszerré egyesítve több bites kvantumregisztereket tudunk készíteni. Ahhoz, hogy kvantumáramkörökről beszéljünk, a mérést elvégző mérőműszerek mellett még kvantumkapukra van szükségünk. Ezek a kvantumkapuk a kvantumrendszert egyik állapotából egy kiválasztott másikba viszik át. Ennek megfelelően az állapot időfejlődését szabályozó második posztulátum segítségével írhatóak le. Ezek a speciális időfejlesztési lépések valamilyen geometriai transzformációt hajtanak végre a bemeneti kvantumbit állapotát jellemző vektoron. Tudjuk a kvantumbitet forgatni, tükrözni, negálni és még nagyon sok más műveletet is elvégezhetünk.

Összefonódás

A negyedik posztulátum az összetett rendszerek részrendszereinek állapotára vonatkozó leírást adja, amelynek következményei közül az összefonódás sokáig a fizikusok előtt is rejtélyes volt.

Összefonódásról akkor beszélünk, amikor különböző részecskék (fotonok, elektronok, de akár apró gyémántok is) kapcsolatba lépnek egymással, és miután szétválnak, a közöttük lévő kapcsolat eredményeként állapotuk egyetlen korrelált kvantummechanikai állapottal írható le. A legegyszerűbb összefont állapotban a pár kétállapotú tagjai mindig ugyanabban (vagy éppen az „ellentétes" kiegészítő) állapotban vannak, függetlenül a közöttük lévő távolságtól. Ha Marsra augusztusban leszállt Curiosity elvitte volna magával a Földről egy bizonyos összefonódott qubit-pár egy tagját, míg a pár másik fele a NASA Sugárhajtás Laboratóriumában (JPL) maradt volna, akkor azt követően, hogy a Curiosity megméri a Marson a pár nála lévő felét, bármikor később elvégzett mérés sorána JPL-nél ugyanazt a mérési értéket kapják a kutatók. Ha a Marson nullát mutat a mérőműszer, akkor függetlenül a két bolygó távolságától és a fénysebességgel kapcsolatos megkötésektől, itt a Földön minden statisztikus szórás nélkül ugyanazt az értéket mutatja a mérőműszer. Természetesen vihetett volna magával olyan összefonódott qubit-párt, amelynél az egyik oldalon nullát mérve a másik oldalon biztosan egyet kapunk, de a lényeg az összefonódáson van. Fénysebességnél gyorsabb kommunikációra azonban nem használhatjuk ezt a jelenséget, mert bármelyik qubit-en elvégzett mérés eredménye önmagában teljesen véletlenszerű. Vagyis nem tud a földi pár viselkedését egyértelműen irányító információt küldeni a marsi rover, mert nem tudja befolyásolni, hogy nullát vagy egyest mérjen a mérőműszere – de ettől még nagyon sok mindenre fel tudjuk használni ezt a jelenséget. Például használhatjuk véletlenszám-generátorként, amelyre bizony nagyon sok informatikai eljárásnál szükség van. 2004-ben a világ első olyan banki tranzakcióját valósították meg Bécsben, ahol az összefonódás segítségével állították elő a titkosításhoz szükséges véletlenszámokat. Továbbá nem csak összefonódott párokról beszélhetünk, hanem további tagokat hozzáfonódtatva a rendszerhez létre tudunk hozni összefonódott hármasokat, négyeseket és így tovább.

Lehetséges kvantuminformatikai alkalmazások

A kommunikáció során két fél továbbít egymásnak üzeneteket egy kommunikációs csatornán, és mindezt úgy, hogy az eljárás minél hatékonyabb és biztonságosabb legyen. Miután a felek megosztoztak az összefonódott párokon, a Bennett és Wiesner által 1992-ben leírt szupersűrűségű algoritmus segítségével egy kvantumbitet felhasználva két klasszikus bitnyi információt tudnak átküldeni a kommunikációs csatornán. (Az algoritmusnak klasszikus esetben két bitet kellene átküldenie, kvantumosan csak egy kvantumbit kerül átküldésre, innen a szupersűrű elnevezés.) A kvantumteleportáció során előre megosztott összefonódott pár használatával egy kvantumbitet teleportálunk, úgy, hogy a csatornán csak két klasszikus bitet küldünk át. Meghökkentő? Bizony, a teleportáció során mindössze két klasszikus 0 vagy 1 értéket küldünk át a kommunikáló felek között, és a fogadó fél képes előállítani a küldőnél lévő, tetszőleges állapotú kvantumbitet. A Bennett által 1993-ban leírt ötlet működését 1997-ben kísérletileg is igazolták, 2010-ben pedig már szabad légkörben 16 kilométeres távolságot hidaltak át vele kínai kutatók. Kvantumbitek másolására nem lehet azonban felhasználni, mert az eredeti kvantumbit megsemmisül az algoritmus során. (A teleportáció szó ellenére nincs szó fénynél gyorsabb kommunikációról, hiszen a két klasszikus bitet át kell küldenünk valahogyan, ezt pedig maximum fénysebességgel tehetjük meg.)

Nem csak a kommunikáció területén használhatunk kvantum alapú megoldásokat. A Grover által készített algoritmus, amely rendezetlen adatbázisban keres, a klasszikus keresőalgoritmusoknál jóval eredményesebb. (Amíg a klasszikus megoldások a rendezetlen adatbázis elemszámával arányos lépésben találnak rá a keresett elemre, addig a Grover-algoritmus lépésszáma az elemszám gyökével arányos). Az 1996-ban publikált algoritmust 1998-ban már implementálták is. A kvantuminformatika

a prímfaktorizációban is áttörést jelent. A faktorziáció során egy adott szám törzstényezős felbontását keressük, és az amerikai Shor megoldása kiválóan alkalmas arra, hogy nagyon nagy számok esetében is nagyon gyorsan meghatározza, melyik két prímszám szorzatából állítható elő. Az informatikai biztonság területén pedig a nyilvános kulcsú titkosítás elve pont azon alapszik, hogy a faktorizáció egy lassan elvégezhető folyamat. 2009-ben egy 232 számjegyű számot klasszikus számítógépekkel próbáltak meg feltörni, a kísérletre fordított összesített gépidő 2000 év volt. Ezzel szemben a Shor-algoritmus segítségével másodpercek alatt törhetővé válik ez a szám. Azonban a gyakorlati implementációval még számos probléma van, 2009-ben még csak a 15-ös számot feltörő rendszert készítettek.

Nehézségek

A kvantummérnökök élete több okból is nehéz. A „No Cloning Theorem" értelmében egy tetszőleges állapotú kvantumbitről nem lehet tökéletes másolatot készíteni. Vagyis a bázisállapotokat (pl. a hagyományos nullának és egynek megfeleltethető kvantumbitet) tudjuk másolni, de a cikkben már többször említett tetszőleges értékű kvantumbitet már nem. Másrészt az önálló kvantumbit határozott kvantumállapotára nagyon hamar hatást gyakorol a környezete (ez a dekoherencia), így a kvantumbitek fizikai megvalósítását két, egymásnak látszólag ellenmondó szempont is nehezíti. Egyrészt szeretnénk, ha a kvantumbitek nem lépnének kapcsolatba a környezettel, másrészt azonban két kvantumbitnek egymással mégis csak interakcióba kellene lépnie. Továbbá jó lenne, ha a kvantumbitek hosszú ideig megőriznék állapotukat. Az is gond, hogy a qubitek leggyakoribb kvantumoptikai megvalósításában használt fotonpárokat nehéz egymás közelségében tartani.

Kulcsszétosztás

A szép számú kísérleti eredmény ellenére a kvantuminformatika elmélete sok esetben jóval előrébb tart, mint a tényleges implementációk. Egy szerencsés kivétel ez alól a titkosítás, ahol már kulcsrakész kereskedelmi termékek kaphatóak. Ahhoz, hogy a kommunikációnk biztonságos legyen, az üzeneteket titkosítani kell. A klasszikus titkosításra igaz a következő: ha mind a két fél ugyanazt a kulcsot használja a kódoláshoz és dekódoláshoz, és a kulcs hossza megegyezik az üzenet hosszával, továbbá egy kulcsot csak egyszer használnak fel, akkor a titkosítás feltörhetetlen. Ezt szimmetrikus kulcsú titkosításnak nevezzük (utalva arra, hogy a titkosításhoz és visszafejtéshez használt kulcs azonos). A kritikus kérdés csupán az, hogyan jutnak hozzá ehhez a kulcshoz a felek. Egy lehetőség, hogy személyesen találkoznak és egyeztetik, de az informatika világában ennél automatizáltabb (és költségkímélőbb) megoldásokra van szükség. Ezek a kulcsszétosztó protokollok, amelyekből nagyon sok létezik a klasszikus világban. Természetesen vigyázni kell, hogy egy támadó ne változtassa meg a kulcsot miközben egyeztetjük, másrészt ne hallgatózhasson észrevétlenül. Ha egy illetéktelen fél lehallgatja a kulcscserét, akkor tudni fogja az üzeneteink titkosításához használt kulcsot, és nem lesznek titkaink előtte. Ebben nyújt hatalmas segítséget a kvantum alapú kulcscsere (angol szakszóval quantum key distribution, rövidítve QKD). Korábban említettük, hogy tetszőleges kvantumbit tökéletes másolása nem lehetséges, és ezt a tulajdonságot alaposan kihasználják a kvantum alapú eljárások. Egy támadó csak úgy tudja lehallgatni a kulcscsere során a kulcsot, ha a két fél közé ékelődve egyesével elkapja a kvantumbiteket, majd továbbküldi. Mivel lemásolni nem tudja magának, meg kell mérnie – a mérés azonban (amennyiben nem ismeri a bázisokat, amelyekben mérnie kell), valószínűségi alapon működik csak, így pontatlan eredményt kap, nem fogja megtudni a kulcsot. Ráadásul a támadó jelenlétéről azonnal értesülnek a kommunikáló felek is. Ez a Bennett és

Brassard által 1984-ben publikált BB84 algoritmus alapgondolata, amelyet azóta további kulcscserélő protokollok követtek, mint például a szintén Bennett által 1992-ben közölt B92, az összefonódást is felhasználó E91 (Ekert, 1991) vagy S09 (Serna, 2009). BB84 esetén az eddig elért legnagyobb sebesség 1 Mbps volt 2008-ban. 2007-ben egy svájci népszámlálás adatait védték kvantum eszközökkel, míg 2008-ban egy bécsi konferencián hat pont között hoztak létre egy QKD-val védett számítógéphálózatot.

3. Kvantuminformatikai alapok

3.1 Bloch gömb

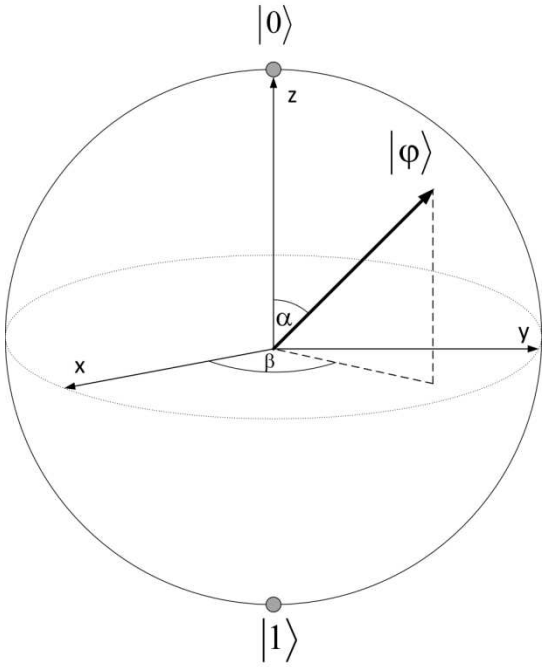
A Bloch-gömb egy kvantumbit geometriai reprezentációja. Emlékeztetőül, egy kvantumbit az alábbi:

$$|\varphi\rangle = a|0\rangle + b|1\rangle \tag{2}$$

ahol $a,b \in C$, *és* $|a|^2 + |b|^2 = 1.$ Írjuk fel ezt a kvantumbitünket a következő alakba:

$$|\varphi\rangle = e^{j\gamma}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{j\beta}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right] \tag{3}$$

ahol $\alpha,\beta,\gamma \in \Re$, és $e^{j\gamma}$ az úgynevezett globális fázis. Mivel a globális fázis abszolút értéke 1, ezért nem befolyásolja a mérési statisztikát. Éppen ezért a globális fázist legtöbbször elhanyagoljuk (nem tüntetjük fel a levezetésekben), vagy ha egy levezetés úgy egyszerűbb, minden további nélkül megváltoztathatjuk a fázisszöget.



1. ábra: Kvantumbit ábrázolása a Bloch-gömbön

3.2 Kvantumregiszter

Egy kvantumregiszter a klasszikus világban ismert regiszterrel azonos szerepet tölt be, míg klasszikus esetben biteket tárol egy regiszter, eddig a kvantum világban qubiteket. A fő különbség az adott méretű regiszterekben tárolható adatmennyiségben van. A klasszikus n bites regiszterben 2^n érték közül tárolhatunk egyet. Viszont egy *n* qubites kvantumregiszterben a 2^n lehetséges érték mindegyike lehet egyszerre. Tegyük fel, hogy van egy 2 qubites kvantumregiszterünk, a tárolt érték a 4 lehetséges állapot szuperpozíciójában lehet ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$), például a következőképpen:

$$|\varphi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle . \tag{4}$$

3.3 Kvantumkapuk

Az elektronikában, digitális technikában használt logikai kapukhoz hasonlóan a kvantuminformatikában is beszélhetünk hasonló szerepet betöltő egységekről. A kvantumregisztereken, kvantumbiteken végezhetünk valamilyen műveletet alkalmazásukkal, kombinálásukkal. Logikai kapuk egymás utáni alkalmazásával kvantum áramköröket építhetünk.

Pauli-X kapu

Bemenet	**Kimenet**	**Mátrix**	**Alkalmazása**
1 qubit	**1 qubit**	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$X\|\varphi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = b\|0\rangle + a\|1\rangle$

Szerepe: Az egyes bázisállapotok valószínűségi amplitúdói felcseréli, emiatt szokás bit-flip kapunak is hívni.

Pauli-Z kapu

Bemenet	**Kimenet**	**Mátrix**	**Alkalmazása**
1 qubit	**1 qubit**	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$Z\|\varphi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = a\|0\rangle - b\|1\rangle$

Szerepe: A $|1\rangle$ -hez tartozó amplitúdót invertálja. .

Pauli-Y kapu

Bemenet	**Kimenet**	**Mátrix**	**Alkalmazása**
1 qubit	**1 qubit**	$\begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}$	$Y\|\varphi\rangle = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = -jb\|0\rangle + ja\|1\rangle$

P kapu

Bemenet	Kimenet	Mátrix	Alkalmazása
1 qubit	**1 qubit**	$\begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix}$	$P(\alpha)\|\varphi\rangle = P(\alpha)(a\|0\rangle + b\|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = a\|0\rangle + e^{j\alpha}b\|1\rangle$

Szerepe: Fáziseltolásra használják.

Hadamard kapu

Bemenet	Kimenet	Mátrix	Alkalmazása
1 qubit	**1 qubit**	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$H\|\varphi\rangle = H(a\|0\rangle + b\|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \frac{a+b}{\sqrt{2}}\|0\rangle + \frac{a-b}{\sqrt{2}}\|1\rangle$

Szerepe: Klasszikus bemeneti állapotból az összes szuperpozíció előállítására használják.

Például: $H\|0\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$, vagy $H\|1\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$

A kapu alkalmazható több kvantumbites bemenet esetén is, ekkor minden kvantumbit egy külön Hadamard kapuhoz kapcsolódik, de az egyszerűség kedvéért $H^{\otimes n}\|\varphi\rangle$ –vel jelöljük.

4. A mérésről - beugró

A mérésen való részvétel feltétele a mérési útmutató tanulmányozása és az alábbi két rövid videofilm megtekintése:

http://www.youtube.com/watch?v=g_IaVepNDT4

http://www.youtube.com/watch?v=7SMcf1MdOaQ

A mérésen nem lesz beugró, helyette beszélgetni fogunk a fenti két rövid videofilmről, így ellenőrizve, hogy mindenki eleget tett-e a felkészülési feltételeknek.

5. A mérésről – használt környezet

A mérés során szabad felhasználású programokat fogunk használni. Ezeket a programokat nem kell a hallgatóknak telepítenie, a mérés gépein rendelkezésre állnak, és a mérés során mindegyikkel meg fogunk ismerkedni. Jelen útmutatóban azonban megadjuk a letöltési helyüket, így ha valakit jobban érdekel valamelyik program, a mérés után saját maga is tud ismerkedni vele.

4. 1. Kvantumbitek és műveletek a Bloch gömbön

Bloch Sphere Simulator

A Bloch Sphere Simulation programot Stephen Shary és Dr. Marc Cahay készítette a University of Cincinatti-n. A Java nyelven készült program futtatásához JVM version 1.5-ös (vagy magasabb) környezet szükséges. A program segítségével kvantumbiteket tudunk megjeleníteni a Bloch-gömbön, és azokon különböző műveleteket elvégezni. Freeware program.

4. 2. Kvantumhálózat - teleportálás

QCircuit

QCircuit egy általános célú kvantumáramkör-tervező és szimulátor program, amely a BME Mobil Kommunikáció és Kvantumtechnológiák Laboratóriumban készült egy hallgatói diplomadolgozat keretében. A program segítségével több bemenetű kvantumhálózatot tudunk felépíteni a legkülönbözőbb kapuk felhasználásával. Freeware program.

http://www.cs.bme.hu/~peresz/qc/

4. 3. Kulcsszétosztás és a BB84 protokoll

Quantum Information processes Simulator

A program egy doktori disszertáció számára készült 2010-ben, Microsoft Visual Studio 2005 környezetben C# nyelven. Freeware program.

http://dotqcf.sourceforge.net/

6. A mérésről – feladatok

A vezetett mérés során az alábbi feladatokat kell megoldani.

1. **Vektorok a Bloch gömbön**
    a. A mérésvezető útmutatásával ismerkedjenek meg a Bloch gömbbel, ábrázolva rajta különböző kvantumbiteket.
2. **Műveletvégzés a Bloch gömbön**
    a. A mérésvezető által megadott kvantumbiteken végezzenek el megadott transzformációkat.
    b. Mutassák meg, hogy bizonyos (megadott) transzformációk egymásutánja ekvivalens egymással.
3. **Kvantumhálózat - teleportálás**
    a. A mérésvezető útmutatásával tekintsék át a kvantumteleportációt.
    b. Készítsék el a kvantumteleportálás áramkörét, és vizsgálják meg a protokoll működését lépésről lépésre.
4. **BB84 protokoll működése**
    a. A mérésvezető útmutatásával tanulmányozzák a BB84 kulcsszétosztó protokollt. Értelmezzék a protokoll működését lépésről-lépésre, támadó jelenléte nélkül és támadó jelenlétével egyaránt.
    b. Válasszanak egy tetszőleges szöveget, és kódolva küldjék át egy ideális (zajmentes) csatornán.
    c. Ismételjék meg ugyanezt a küldést, de most a csatorna zaját erősítsék fel. Ki tudják mutatni a támadó jelenlétét?

5. **Kvantumszámítógép**
    Építsék meg a világ első univerzális kvantumszámítógépét, szabadalmaztassák alkotásukat, és az így befolyó jogdíj töredékéből belátásuk szerint vásárolják fel a Google-t vagy az Amazont (vagy egyéb céget esetleg egy-két országot), és közben ne feledkezzenek meg Alma Materükről sem.

7. Tovább is van…

Jelen méréssel csupán egy bevezetőt kívántunk adni a kvantuminformatika és a kvantumkommunikáció világába. A téma iránt érdeklődőknek szeretnénk figyelmébe ajánlani néhány további érdekességet.

7.1. Napi érdekességek és aktualitások - levelezőlista

Üzemeltetünk egy levelezőlistát, amelyen kvantuminformatikával kapcsolatos magyar és angol nyelvű, aktualitásokat tartalmazó híreket osztunk meg egymással. A levelezőlistával kapcsolatban további információ a mérésvezetőtől kérhető.

7.2. További információk – választható tárgyként

Bevezetés a kvantum informatikába és kommunikációba (BMEVIHIAV06) tárgyat minden tavaszi félévben hirdetjük meg, heti 2 órás, 2 kreditértékű választható tárgy formájában. Részletek a tárggyal kapcsolatban:

http://www.mcl.hu/quantum

7.3. Műholdas kvantum hálózat szimulálása

Quantum Satellite Channel Simulator

A BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium és a Nyugat-magyarországi Egyetem szakemberei által készített szimulációs program a világűrben zajló kvantum-kulcsszétosztás szimulálására. A programot Bacsárdi László, Galambos Máté és Imre Sándor útmutatása alapján Kiss András fejlesztette C# nyelven. Freeware program.

http://www.mcl.hu/quantum/qscs

7.4. Ajánlott irodalom

Ebben a fejezetben foglaljuk össze az ajánlott és felhasznált irodalmat.

Könyvek

S. Imre, F. Balázs, „Quantum Computing and Communications: An Engineering Approach”, Willey, 2005

S. Imre, L. Gyöngyösi, „Advanced Quantum Communications, An Engineering Approach”, Willey, 2012

L. Bacsárdi, „Efficient Quantum Based Space Communication”, Lambert Academic Publishing, 2013

M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information,” Cambridge University Press, 2000

John Gribbin, Schrödinger macskája - Kvantumfizika és valóság, Akkord, 2001

Cikkek

L. Bacsárdi, S. Imre, Kommunikáció mélyben és magasban, Természet Világa, 2013.

M. Galambos, S. Imre, “New Method for Representation of Multi-qubit Systems Using Fractals“. ICQNM 2011

Nicolas Gisin, et al., ’Quantum Cryptography’, Reviews of Modern Physics, (February 1, 2008)

Hanzo, L.; Haas, H.; Imre, S.; O'Brien, D.; Rupp, M.; Gyongyosi, L.: Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, Proceedings of the IEEE, Volume: 100 , Issue: Special Centennial Issue, pp. 1853-1888.

Kvantuminformatikai szimulátorok

Kvantuminformatikával és kvantumkommunikációval kapcsolatos szimulátorok gyűjtőhelye:

http://www.quantiki.org/wiki/List_of_QC_simulators

Neten elérhető előadássorozatok

Michael Nielsen bevezető előadássorozata a kvantuminformatikába:
http://www.youtube.com/watch?v=X2q1PuI2RFI&list=PL1826E60FD05B44E4

A Stanford Egyetem előadássorozata az összefonódásról:
http://www.youtube.com/playlist?list=PLA27CEA1B8B27EB67

A Stanford Egyetem előadássorozata a kvantummechanikáról:

http://www.youtube.com/playlist?list=PL84C10A9CB1D13841