A „TÖRPÉK" VALÓSÁGOS ÉS VIRTUÁLIS VILÁGA

Csurgay Árpád
az MTA rendes tagja, egyetemi tanár,
Budapesti Műszaki Egyetem, Elméleti Villamosságtan Tanszék

I. Az egyszerû és a bonyolult a virtuális valóságban

A digitális számítógépeink képernyőjén életre keltett ***virtuális*** tárgy a matematikai modelljeinket jeleníti meg. Nemcsak a valóság megmérhető adatainak egy részét tükrözi, de visszaad valamit a valóság ritmusából és harmóniájából is. A virtuális tárgyak mint új metaforák kiegészítik kommunikációnk eszköztárát. Jó segítőtársak, megtévesztően hasonlíthatnak a valós tárgyakra, sőt alkalmasak a tárgyakon a jövőben végzett mérésekbe történő bepillantásra is.

A modellek életre keltéséhez a szimulátor gépnek időre van szüksége. Az a tény, hogy van modellünk, és egy számítógép elvben kezelni tudja a modellt, még nem jelenti azt, hogy a virtuális tárgyat meg is tudjuk jeleníteni, ugyanis a számításhoz szükséges idő esetleg nagyon hosszú lehet. Ezért oly fontos tudnunk, hogy mennyire bonyolult programot kell írnunk számítógépeinkre ahhoz, hogy a kiválasztott tárgyat leíró matematikai modellt életre kelthessük. A bonyolultság (complexity), amiről e cikkben szólni szeretnék, a virtuális tárgy tulajdonsága, nem a valóságos tárgyé. Arra ad választ, hogy adott szimulátor gépen hány műveletre van szükség a virtuális tárgy életre keltéséhez, pontosabban a mögöttes algoritmus lefuttatásához. Ez a bonyolultság nemcsak a matematikai modelltől, hanem a szimulátor-géptől is függ.

A valós tárgyat szigorúan körülhatárolt kísérleti körülmények között (experimental frame) mérésekkel faggatjuk, matematikai modellt alkotunk róla, majd a méréseket (nemcsak a ténylegesen elvégzetteket, de a jövőben végrehajtandókat is) számítógépeinken szimuláljuk [1]. Mesterséges környezetünk tervezése és építése nem volna lehetséges, ha a virtuális tárgy szimulációja nem megfelelően jósolná meg a valós tárgy jövőbeli működését.

Csak csodálkozhatunk azon, hogy a viszonylag egyszerű matematikai modellek jól közelítik jövőbeli méréseink eredményeit. Azon pedig különösen csodálkoznunk kell, hogy rendkívül egyszerű modellekből is nagyon bonyolult tulajdonságok bontakozhatnak ki (chaotic behavior, emerging phenomena stb.). A klasszikus fizikából kölcsönzött dinamikai modellekre épülő digitális világ virtuális valósága lenyűgöző, de a nanoelektronikában érzékeljük ennek korlátait is.

A nanotechnológia (nanos görögül törpét jelent), a ***törpék*** világát: az atomok és molekulák kvantumeffektusait próbálja munkára fogni. A tér-időben adott erők hatására mozgó „oszthatatlan" testekhez szokott szemléletünk e nanojelenségeket ***kísértetiesnek*** (spooky) véli [2]. Werner Heisenberg írja: „Emlékszem, hogy volt egy beszélgetésem Niels Bohrral, amikor ő kétségbe vonta, hogy egyáltalán fog-e találni a jelenségek számára adekvát matematikai leírást. Úgy

érezte, hogy a természet esetleg annyira irracionális, hogy egyszerűen semmiféle matematikai leírás kereteibe nem szorítható bele. Így teljesen meg volt lepve, amikor az derült ki, hogy igenis van matematikai leírás ...” [3]. Van matematikai leírás, de ennek a digitális gépeken történő pontos megjelenítése szinte lehetetlen az algoritmusok exponenciálisan növekvő bonyolultsága következtében [4, 5].

Úgy tűnik, hogy a kellően felszerelt megfigyelő számára nincs egyszerűbb vagy bonyolultabb valós tárgy. Sokat emlegetett példa egy tömegpont gravitációs térbeli mozgása. Erről Newton almája jut eszünkbe, amint az alma éppen Sir Isaac Newton fejére esik. Ez a klasszikus mechanika legegyszerűbb példája. Pedig az alma egy biológus számára igencsak bonyolult szerves rendszer. Ugyanakkor nem az egyetlen elektron a legegyszerűbb test? Ha valóban az volna, akkor hogyan lehet, hogy a relativisztikus kvantum-térelmélet kutatói Nobel-díjakat kaptak a megismeréséért? Minden valós tárgy egyformán bonyolultnak tűnhet. Attól függően, hogy mi, mint megfigyelők mit akarunk vizsgálni, és ehhez milyen műszereink vannak, a tárgyakat – az elemi részektől a növényeken és állatokon át a bolygókig vagy a teljes Univerzumig – hasonló bonyolultságú modellekkel írhatjuk le [6, 7].

A bonyolultságot nem magában a valós tárgyban, hanem a megfigyelő „szemében”, azaz az általa szigorúan kijelölt kísérleti körülményekben kell keresnünk. Ugyanazt a tárgyat attól függően, hogy mi a célunk vele, milyen kísérleti körülmények között kívánjuk ***látni*** vagy ***működtetni***, aszerint modellezzük [8]. „A tudomány nem próbál végső magyarázatot adni, fogalmakat értelmezni is alig. A természettudomány modelleket alkot. Modell alatt egy olyan matematikai struktúra értendő, amelyik – bizonyos szóbeli interpretáció hozzáfűzésével – leírja a jelenséget. Egy ilyen matematikai struktúra létjogosultságát az adja, hogy sikeresen látja előre a jelenségeket, tehát működik.” – írta Neumann János.

A nanoelektronika matematikai modelljeinek és algoritmusainak legnagyobb része megszokott számítógépeinken fut. Fontos előrelépést jelent majd az analogikai elven működő processzorok várható elterjedése is [9, 10], de úgy tűnik, hogy a ***kísérteties*** kvantumjelenségek valós időbeli megjelenítését csak a kvantumszámítógépektől várhatjuk.

II. Modellek, szimulátorok, algoritmusok

A szimulátorok szigorúan kijelölt kísérleti keretek között működő fizikai rendszerek. Intuitíve minden olyan fizikai rendszer szimulátornak tekinthető, amelyben kijelöltük a bemenetnek tekintett állapotváltozókat, ezeket a processzálás kezdeti időpontjában megfelelően beállítottuk, és kijelöltük azokat az állapotváltozókat is, amelyeket a rendszer egy meghatározott idejű dinamikai mozgását követően mint kimeneteket méréssel meghatározunk. A bemenet jellegét megkülönböztetjük a kimenetétől, mert a bemenetet mint kezdeti feltételt ***beállítjuk***, a kimenetet viszont a dinamika lezajlása után ***mérjük***.

Ha a bemenetet két csoportba osztjuk, és az egyik csoportot ***programnak*** nevezzük, megkülönböztetve az adat jellegű bemenettől, akkor a fizikai rendszert programozhatónak nevezzük. Rögzített program esetén a fizikai rendszer a különböző bemeneti adatokat különböző kimeneti adatokba képezi le, egy függvényt valósít meg. Ha változtatjuk a programot, akkor az adott fizikai rendszer különböző függvényeket tud kiszámolni. Egy kijelölt programú, adott bemenetű és kimenetű fizikai rendszer (a hardver) a programjától függően függvények sokaságát tudja kiszámolni. Ez a függvényhalmaz jellemzi az adott hardver szimulációs képességét. Hogyan bővíthetjük e

halmazt? Ha egyszerűen mellé teszünk egy másik hardvert, amely olyan függvényeket is ki tud számítani, amelyeket az eredeti hardver még nem tudott, és a két gépet egynek tekintjük, akkor a bővített géppel kiszámítható függvények halmaza a két géppel külön-külön kiszámítható függvényhalmazok uniója lesz.

Az információtechnika történetére máig hat Alan Turing 1936-ban közzétett eredménye. Megmutatta, hogy a számítást végző eszközök hardverjének bővítése nem sokáig gazdagítja a kiszámítható függvények körét. Igen hamar eljuthatunk egy olyan gépig, amely ki tud számítani minden, egyáltalán kiszámítható függvényt. Állítását egy „univerzális gép", a róla elnevezett Turing-gép konstrukciójának megadásával bizonyította. A Turing-gép minden bináris (0-ból és 1-ből álló) sorozatot bináris sorozatba leképző kiszámítható függvényt ki tud számolni. Turing bebizonyította, hogy ami gépével véges számú lépésben nem számolható ki, azt semmilyen gép sem tudja véges számú lépésben kiszámítani. A kiszámíthatóság maga nem elég a virtuális valóság életre keltéséhez. Nem mindegy, hogy az életre keltés ideje hogyan függ a valós mérés idejétől.

A nanoelektronikában virtuálisan szeretnénk megjeleníteni az atomok és molekulák „kísérteties" jelenségeit is. Richard Feynman már 1982-ben megmutatta, hogy ***összefont*** (entangled) állapotú kvantumfizikai objektumok tökéletesen (ez alatt elfogadható idejű számítási időt értett) csak összefont állapotra is képes kvantum-objektumokkal szimulálhatók, klasszikus digitális számítógépekkel nem, mert a mérést szimuláló algoritmusok bonyolultsága exponenciálisan nő a mérés idejének függvényében, ami ellehetetleníti a megjelenítést. Gondot jelent a kvantummechanikai mérés problematikája is. Kiszámítani csak valószínűségeket tudunk. Amit mérni fogunk, azt nem. Felmerült, hogy a determinisztikus Turing-gép (DTM: Deterministic Turing Machine) helyett próbálkozzunk a nem-determinisztikus Turing-géppel (PTM: Probabilistic Turing Machine). Vannak feladatok, amelyekben a PTM hatékonyabb, mint a DTM, de a klasszikus fizika „előítéletei" mindkettőbe be vannak építve, a PTM sem gyorsítja meg az összefont kvantumállapotok megjelenítését.

Úgy tűnik, hogy a mikrovilág törvényeit követő valós tárgyak megjelenítéséhez olyan új gépekre van szükség, amelyek maguk is a mikrovilág törvényei szerint működnek.

III. Az univerzális kvantum Turing-gép (QTM: Quantum Turing Machine)

Feynman 1986-ban felvázolta a kétállapotú atomsoron mint regiszteren működtethető kvantumszámítógépre vonatkozó elgondolását [11]. A gép memóriája egy atomsor alkotta regiszterből és egy programvezérlést végző segédregiszterből áll. A gondolatkísérletben folyó számítás úgy zajlik, hogy a regiszterek állapota egy unitér operátor által előírt módon időlépésről időlépésre halad a végállapot felé, amit a regiszter a lépéssorozat végén vesz fel. Az eredményt a regiszter végállapotának mérésével olvashatjuk ki. Minden elemi utasítás az atomsoron végrehajtott unitér, tehát invertálható művelet. E gépen minden program visszafelé is lefuttatható. De tetszőleges n bitből álló bemenetet a kimenetre leképző függvény invertálhatóságának szükséges feltétele az, hogy a kimenet bitjeinek száma megegyezzen a bemeneti bitek számával. Ez felesleges bitek kiszámítását igényli. A számítás eredményei között ott van, amit ki akartunk számítani, de egy sor más adat is, amelyek lehetővé teszik, hogy a számítást fordított irányban is végrehajthassuk. Mennyi felesleges információ kiszámításával és tárolásával fizetünk az invertálhatóságért? Nagy memóriára van szükség ahhoz, hogy megőrizzük a számítás ***történetét***, hogy aztán visszafelé is végrehajthassuk?

Megmutatták (lásd például [12, 13, 14]), hogy mindig elegendő a bemenet mellett annyi felesleges bitet felvenni, amennyi a keresett kimenet bitjeinek száma. Ha az a feladatunk, hogy az *s* bitsorozatot az ***f (s)*** bitsorozatra képezzük le (nem feltétlenül visszafordíthatóan), akkor mindig elegendő, hogy a bemenet az *s* bitjein kívül az ***f (s)*** bitjeinek számával megegyező számú 0-t visszafordíthatóan képezzen le az *s*-ből és az ***f (s)***-ből álló kimenetre. Az $s \Rightarrow [s, f(s)]$ leképzés mindig invertálható, tehát $s \Leftrightarrow [s, f(s)]$, és soha nincs szükség több felesleges bit megőrzésére, mint a kimenet bitjeinek száma.

Ez a gondolatmenet vezetett a reverzibilis Turing-géphez (RTM). Feynman e gondolatkísérletéből arra a következtetésre jutott, hogy a természetben működhetnek, és talán hamarosan mesterségesen is előállíthatók lesznek olyan számítógépek, amelyekben az elemi memóriacella egy-egy atom (vagy molekula), és amelyekben az elemi kölcsönhatások a mikrovilág kvantumjelenségeinek törvényeit követik. Megmutatta, hogy e gépek elvben óriási memóriakapacitással, petaflopnak megfelelő sebességgel és rendkívül kis fogyasztással működhetnek.

Amíg egy kétállapotú mikrofizikai objektummal megvalósított memóriacella (például a Feynman-féle kétállapotú atom) minden számítási lépés végén 1 valószínűséggel veszi fel az egyik vagy másik sajátállapotát – azaz a cella minden számítási lépés során egyik sajátállapotából a másik sajátállapotába megy át (vagy nem megy át) –, addig a jelprocesszor bináris működésű, klasszikus vagy kvantumfizikai dinamikájától függetlenül bitsorozatokat képez le bitsorozatokba, így nem nyújt többet, mint a reverzibilis Turing-gép. Nem bővíti a tökéletesen szimulálható fizikai objektumok körét, és nem változtat a számítási feladatok komplexitási osztályain sem.

Feynman továbblépett. Mi történne – kérdezte –, ha sikerülne a kétállapotú memóriacellában a két sajátállapotot ***összefonva*** fenntartani? Mi történne, ha ezeken az összefont állapotú biteken (qubit=kvantum bit) a bitekhez hasonlóan tudnánk műveleteket, számításokat végezni, ha tudnánk olyan gépet építeni, amelyben az információt nem bitek (legalábbis nem ***csak*** bitek), hanem qubitek is hordozzák?

E kérdések aktív elméleti kutatások egész sorát motiválták. Sokan tettek és tesznek kísérletet qubiteket hasznosító gépek – kvantumszámítógépek építésére is. A qubiteket is a maga szolgálatába állító információtechnika ugyanis nagyon sokat ígér. Nemcsak a számítási kapacitás növelését ígéri, de két szempontból merőben új lehetőségeknek is utat nyit. Ahogy 1936-ban Turing felvázolta az univerzális digitális jelprocesszorban rejlő lehetőségeket, ugyanúgy 1985-ben David Deutsch megadta az univerzális kvantumszámítógép (ahogy ő elnevezte, a Quantum Turing Machine, QTM) konstruktív definícióját [15], és megmutatta, hogy az univerzális QTM-gép minden véges fizikai rendszer ***tökéletes*** szimulátora, tehát megvalósítója minden véges fizikai rendszerrel egyáltalán megvalósítható leképzésnek.

A QTM az információt qubitek formájában tárolja. Minden kétállapotú rendszer, amelyben két stacionárius állapot összefonódhat (például az atommagok mágneses spinje), alkalmas arra, hogy qubitet reprezentáljon. Ugyanakkor minden lineárisan poláros foton továbbíthat összefont vertikális és horizontális, a cirkulárisan poláros pedig balra és jobbra is forgó összefont polarizációjú fényt. Minden atom vagy kvantumpötty (quantum dot) alapenergiájú stacionárius állapota és első gerjesztett állapota is összefonódhat. A mikrofizika sok lehetőséget kínál qubitek megvalósítására.

A kvantumregisztert ilyen, egymás mellé helyezett kétállapotú elemekből építhetjük meg, ugyancsak „összefonva" őket. A

kvantumregiszter egy qubit lánc [16], melynek állapota két stacionárius sajátállapot koherens szuperpozíciója

$$|\Psi\rangle = c_0|\Psi_0\rangle + c_1|\Psi_1\rangle \equiv \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

ahol c_0 és c_1 komplex számok, melyeknek abszolút érték négyzete megadja, hogy állapotmérés esetén milyen valószínűséggel találjuk a rendszert egyik vagy másik sajátállapotában. Mivel mérés esetén csak a két sajátállapot valamelyikében találhatjuk a rendszert, ezért: $|c_0|^2 + |c_1|^2 = 1$

A kvantummechanika szuperpozíció elve értelmében az összefonódott kvantumállapotok egyidejűleg tartalmazzák a két sajátállapotot. Ez klasszikus fizikai rendszerekben nem fordulhat elő, mert a dekoherencia jelensége igen rövid idő alatt valamelyik sajátállapotba viszi át a rendszert. A legegyszerűbb esetben, egy kétállapotú qubitet megvalósító rendszer esetén, az állapot időfüggését szemléltethetjük egy egységnyi sugarú gömb felületére mutató vektorral.

Általános esetben a c_0, c_1 komplex számokból álló vektor a gömb felületére mutat, a vertikális koordináta-tengelyre eső vetülete jellemző arra, hogy az összefonódott $|\Psi_0\rangle$ és $|\Psi_1\rangle$ sajátállapotok milyen mértékben vesznek részt az eredő állapotban. A vertikális tengely körüli elforgatást mutató szög felel meg az állapot „fázisának". Ez a fázis ugyan nem befolyásolja a sajátállapotok részesedését, de meghatározó szerepet játszik a kvantuminterferencia jelenségében. Így az eredő állapotban a 0 és az 1 sajátállapot részesedése lehet ugyan azonos, a komplex amplitúdók mégis különbözőek, mert fázisuk különböző.

A választott fizikai realizáció determinálja a $|\Psi_0\rangle$ és $|\Psi_1\rangle$ bázist, ezért az állapotot a c_0, és c_1 komplex amplitúdók határozzák meg, melyeket egy oszlopvektorral adhatunk meg. Az oszlopvektor a sajátállapotok esetén

$$|\Psi_0\rangle \equiv |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{és} \quad |\Psi_1\rangle \equiv |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

A kvantumregiszter összefonódott qubitekből épül fel. Két összefonódott qubit állapotát a qubitek állapotainak direkt szorzata adja meg

$$|\Psi^{(1)}\rangle \otimes |\Psi^{(2)}\rangle = |\Psi^{(1,2)}\rangle.$$

Komplex amplitúdó vektorokkal a következő módon reprezentálhatjuk az állapotokat:

$$|\Psi^{(1)}\rangle \otimes |\Psi^{(2)}\rangle = \begin{pmatrix} c_0^{(1)} \\ c_1^{(1)} \end{pmatrix} \otimes \begin{pmatrix} c_0^{(2)} \\ c_1^{(2)} \end{pmatrix} =$$

$$= \begin{pmatrix} c_0^{(1)} c_0^{(2)} \\ c_0^{(1)} c_1^{(2)} \\ c_1^{(1)} c_0^{(2)} \\ c_1^{(1)} c_1^{(2)} \end{pmatrix} = |\Psi^{(1,2)}\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

Két összefonódott qubitnek négy saját állapota van: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ ahol

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

és a két qubitből álló regiszter állapota általános esetben a következő:

$$|\Psi^{(1,2)}\rangle = c_{00}|00 + c_{01}|01 + c_{10}|10 + c_{11}|11$$

Hasonlóan állíthatjuk elő az n qubitből álló kvantumregiszter állapotát is. Figyeljük meg, hogy 2-qubites regiszter négy különböző klasszikus 2-bites sztring szuperpozícióját, a 3-qubites regiszter nyolc hárombites sztring, és egy n-qubites regiszter 2^n darab n-bites sztring szuperpozícióját tartalmazza *párhuzamosan*.

A kvantumregiszter legfontosabb tulajdonsága éppen az, hogy a kvantum-szuperpozíció jelenségét kiaknázva exponenciális mennyiségű klasszikus információt tárol polinom számosságú qubitben.

IV. Mûveletek kvantumszámítógépeken

A kvantumregiszter tartalmát olyan vektorokkal reprezentáljuk, amelynek elemei komplex számok. Az egyes állapotokhoz különböző energiaszintek tartoznak. A vektorok „hossza” (az elemek abszolút értékeinek négyzetösszege) minden állapotban eggyel egyenlő. A legkisebb energiájú állapot ($|0\rangle$, $|00\rangle$, $|000\rangle$, …) vektora is egységnyi hosszúságú. Mindaddig, amíg a kvantumregiszteren mérést nem végzünk, a regiszterben jelen lehet az összes sajátállapot szuperpozíciója is. Ez azt jelenti, hogy a vektor végpontja az egységnyi sugarú gömbön bárhová mutathat. Ha a legkisebb energiájú $|0000\rangle$ állapotból indulunk, és a rendszer dekoherenciáját sikeresen megakadályozzuk (jól elszigeteljük a rendszert a hőtartályoktól, és mérést nem végzünk), akkor külső erővel (például a Rabi-oszcillációt előidéző elektromágneses impulzusokkal) a vektor végpontját az egységnyi sugarú gömb felületén folyamatosan mozgathatjuk. A külső erő a rendszer Hamilton-operátorát teszi időfüggővé, ami a zárt kvantummechanikai rendszernek az egyik állapotból a másikba való evolúcióját váltja ki. A gömb felületén egy adott számítás bemenő adataihoz is, eredményéhez is jól meghatározott pontok tartoznak. A jó kvantumalgoritmus a számítás végén olyan pontot állít be a gömbön, amely biztosítja, hogy mérés esetén a keresett eredmény valószínűsége közel egy, minden más bináris adat valószínűsége közel nulla legyen.

A kvantumalgoritmusokat elemi műveletekre bontjuk fel. Egy-egy művelet a kvantumregiszter állapotát változtatja meg, „operációt” hajt rajta végre. Megmutatható, hogy egyetlen qubiten végzett műveletekből nem minden operáció építhető fel, de egyedi qubiteken és összefonódott qubit párokon végrehajtott elemi műveletekkel az n qubitből álló kvantumregiszter bármely állapotából bármely másik állapotába eljuthatunk. Az n dimenziós egységgömbön is szemléltethetjük ezt az állítást: egyedi qubitekre és összefonódott qubit párokra alkalmazott műveletekkel a gömb bármely pontjára mutató vektort átforgathatjuk a gömb bármely másik pontjára. Ha teljesülnek a rendszer zártságára vonatkozó feltételek, akkor a műveletek lineárisak, és az állapotot reprezentáló komplex elemű vektorokat unitér négyzetes mátrixok viszik át egyik állapotból a másikba.

Ha a kvantumregiszter n kétállapotú qubitből áll, akkor a regiszteren működő operátor $2^n \times 2^n$ dimenziójú mátrixszal reprezentálható. Ha egy operátor egyetlen qubiten működik, akkor 2×2-es unitér mátrix alakban írható fel.

Bináris vektort összefonódott állapotba viszi át például a

$$U(\vartheta) = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$

unitér mátrixszal reprezentált operátor.

A logikai kapuk is operátorok. A NOT operátor mátrixa például

$$\mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Már említettük, hogy a zárt kvantumrendszerek dinamikáját a Schrödinger-egyenlet határozza meg:

$$|\Psi(t)\rangle = e^{-j\frac{Ht}{\hbar}} |\Psi(0)\rangle = U(t) |\Psi(0)\rangle$$

ahol az úgynevezett $U(t)$ „evolúció” operátor mindig unitér, azaz minden ideális kvantumszámítógép unitér leképzést realizál, logikailag reverzibilis.

A kvantumszámítógépek azonban nemcsak binárisan reverzibilis működésűek, hanem minden unitér leképzést megvalósíthatnak. Láttuk, hogy a NOT és a C-NOT leképzések reverzibilisek, de még binárisak.

A kvantumszámítógépen megvalósítható

$$\begin{pmatrix} \frac{1+1}{2} & \frac{1-1}{2} \\ \frac{1-j}{2} & \frac{1+j}{2} \end{pmatrix}$$

leképzés viszont már nem bináris. Vegyük észre, hogy e leképzés négyzete nem más, mint a bináris NOT, ezért e leképezést $\sqrt{\text{NOT}}$ kapunak nevezzük.

V. A kvantumszámítógép mint szimulátor

A kvantumregiszter legfontosabb tulajdonsága éppen az, hogy a kvantum-szuperpozíció jelenségét kiaknázva exponenciális mennyiségű klasszikus információt tárol polinom számosságú qubitben. Kiolvasni ugyan csak egyetlen klasszikus bitsort tudunk, de mindaddig, amíg nem hajtunk végre mérést a regiszteren, minden utasítást az exponenciális mennyiségű klasszikus bitsoron párhuzamosan hajthatunk végre.

Ezt a lehetőséget eddig két nehéz, klasszikus probléma gyorsított megoldásában tudták kiaknázni. Peter Shor, az IBM kutatója a nagy számok prím-faktorizációjára adott polinom-rendű algoritmust kvantumszámítógépre [16], ami lehetővé tenné a titkosító kódok feltörését. Lov K. Grover, az AT&T munkatársa nagy adatbázisokban való keresést felgyorsító algoritmust adott [17]. Sikeresek és nagyon ígéretesek a kvantum-kriptográfiai kísérletek [18].

A *Science* folyóirat 2001 decemberében – áttekintve az év legfontosabb eredményeit – az év áttörésének nevezte a nanoáramkörök terén elért eredményeket, nevezetesen a molekulákból „összeszerelt" áramköröket (Service, 2001). Az IBM Almadel kutatóközpontjának honlapján 2001 decembere óta olvashatjuk a bejelentést: sikerült egy hét quantum-bitet (qubit) tartalmazó olyan kvantumszámítógépet megvalósító molekuláris áramkört építeni, amin lefuttatható Peter Shor 1994-ben közölt algoritmusa, amely egészszámok prím-faktorizációját a karakterek számától polinom rendben függő idő alatt végzi el (IBM's Test-Tube Quantum Computer Makes History: First Demonstration of Shor's Historic Factoring Algorithm). 2001-ben új lendületet kapott a molekulák atommagjainak „spin"-jeit qubitként hasznosító kvantumszámítógépek kutatása, és folytatódott az összes többi géptípus fejlesztése is.

A kvantumszámítógép megvalósítása előtt akadályok egész sora tornyosul. Az összefont kvantumállapotok dekoherenciája elleni küzdelem és a hibajavítás nehézségeinek feloldása az egyik kihívás, nagyszámú qubit (például 200) integrálása a másik, elfogadható architektúra és konstrukció kidolgozása a harmadik. Szkeptikusok szerint a sokat ígérő algoritmikus adta előnyökért a hardver bonyolultságával kell fizetnünk. A kvantumszámítógépek jelenleg szóba hozott architektúrája nem is hasonlít a logikai kapukból és memóriacellákból felépített számítógépekéhez. Semmiképpen sem versenytársa, legfeljebb lényeges kiegészítő processzora lehet a digitális elven működő gépeknek. A qubitek nem versenytársai, hanem segítői lesznek a biteknek.

Egy területen azonban a kvantumszámítógépek, éppen a kvantumjelenségeket hasznosító nanoelektronikában, nélkülözhetetlennek tűnnek. A kvantumszámítógép ugyanis a kvantumjelenségek természetes szimulátora, virtuális megjelenítésük természetes eszköze. Ahogy a digitális számítógépek új generációit a korábbiak alkalmazása nélkül lehetetlen lett volna kidolgozni, ugyanúgy a kvantumszámítógépek is csak „egymás vállán állva" nőhetnek fel feladataikhoz, a mikrovilág kvantumjelenségeinek valós idejű virtuális megjelenítéséhez.

A kvantumszámítógépek ha felnőnek feladataikhoz, számítógépeink képernyőjén életre kel majd a kvantumvilág, George Gamow *Wonderland*je, úgy, ahogy azt Mr.

Tompkins megálmodta. A kvantumjelenségek nem lesznek többé kísértetiesek. A mikrovilágot is olyannak látjuk majd, mint amilyen, mérhető adataival, *ritmusával* és *harmóniájával* együtt. Ki tudja, hogy képzeletünk milyen új metaforákat kölcsönöz majd a virtuális kvantum-valóságból, mivel és mennyiben gazdagítja majd ezzel kommunikációnkat?

Kulcsszavak: *nanotechnológia, kvantumszámítógépek*

IRODALOM

[1] Zeigler, Bernard P. (1976): *Theory of Modelling and Simulation*. John Wiley, New York,

[2] Weizsäcker, Carl Friedrich von (1985): *Aufbau der Physik*. Hasner, München

[3] Simonyi Károly (2000): *A fizika kultúrtörténete*. Gondolat, Budapest

[4] Feynman, Richard Phillips (1990): *The Strange Theory of Light and Matter.* Penguin Books, NY

[5] Feynman, Richard Phillips (1982): Simulating Physics with Computers. International Journal of Theoretical Physics. Vol. 21, No. 12. 467-488.

[6] Wheeler, John A. (1996): Time Today. In: Namiki, Mikio – Aizawa, Youji: *Quantum Physics, Chaos Theory, and Cosmology*. American Institute of Physics Press, New York

[7] Wheeler, John A. (1991): *Recent Thinking about Nature of the Physical World*. Paper presented at the First Andrei Sakharov International Physics Conference, Moscow, May 1991

[8] Makus, Robert (2001): Education in the Grip of Technological Thinking: An Analogical Hermeneutic of Heidegger's "Question Concerning Technology". *Existentia,* Vol. XI/2001/Fasc.3-4. 315-21.

[9] Chua, Leon O. (1998): *CNN: A Paradigm for Complexity*. World Scientific Series on Nonlinear Science, Series A, Vol 31. World Scientific, Singapore

[10] Roska Tamás – Chua, Leon O. (1995): *On a Framework of Complexity of Computations on Flow-Implemented on the CNN Universal Machine. Research report of the Analogical and Neural Computing Laboratory DNS-15-1995.* MTA SZTAKI, Bp.

[11] Feynman, Richard Phillips (1986): Quantum Mechanical computers. Foundations of Physics. June, 1986, Vol. 16. 507-531.

[12] Csurgay Árpád – Simonyi Károly (1997): *Az információtechnika fizikai alapjai*. Mérnöktovábbképző Intézet, Budapest

[13] Gershenfeld, Neil (2000): *The Physics of Information Technology*. Cambridge University Press, Cambridge

[14] Williams, Colin P. – Clearwater, Scott H. (1997): *Explorations in Quantum Computing*. Springer – TELOS, New York

[15] Deutsch, David (1985): Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proceedings of the Royal Society. Series A, 400, 97-117.

[16] Shor, Peter W. (1997): Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. October 1997. Vol. 26. 1484-1509.

[17] Grover, Lov K. (1996): *A Fast Quantum Mechanical Algorithm for Database Search*. Proceedings of the 28th ACM Symposium on Theory of Computing. Philadelphia. 212-219.

[18] Bouwmeester, Dirk – Ekert, Artur – Zeilinger, Anton (szerkesztők) (2000): *The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation.* Springer, Berlin

[19] Service Robert F. (2001): Breakthrough of the Year: Molecules Get Wired. Science. 294: 2442-2443.

[20] IBM's Test-Tube Quantum Computer Makes History. First Demonstration of Shor's Historic Factoring Algorithm.
http://www.research.ibm.com/resources/news/20011219_quantum.shtml