Kvantum összefonódással támogatott közeghozzáférés

Prakfalvi András

2017.10.27.

Tartalomjegyzék

1. Bevezetés

A kvantum-informatika és kommunikáció négy tudományterület - fizika, számítástudomány, információelmélet és kriptográfia - eredményeinek köszönhetően született meg. A következőkben ismertetem vázlatosan az egyes tudományterületek fejlődését és eredményeit melyek megalapozták ezt az új rohamosan fejlődő diszciplínát.

A huszadik század elején a tudósok a fizikát - leszámítva pár egyedi jelenség magyarázatát - befejezettnek gondolták. Az egyik ilyen jelenség a feketetest-sugárzás volt, a feketetest olyan fizikai objektum mely minden ráeső sugárzást elnyel, ezért nem verődik vissza róla semmi. Az ilyen test által kisugárzott elektromágneses hullámokat nevezzük feketetest-sugárzásnak, a tudósok azt figyelték meg, hogy meglepő módon a sugárzás spektrális eloszlása csak a test hőmérsékletétől függ. Sok próbálkozás történt arra, hogy ezt a jelenséget a klasszikus fizika fogalmaival lehessen megmagyarázni, de ezek mind zsákutcába vezettek. A megoldást végül Max Planck elmélete [1] jelentette melynek meglepő következménye volt, hogy a kisugárzott energiát diszkretizálta (kvantálta) ez a felvetés vezetett a fizika új, miden eddiginél pontosabb elméletének a kvantummechanikának a kialakulásához.

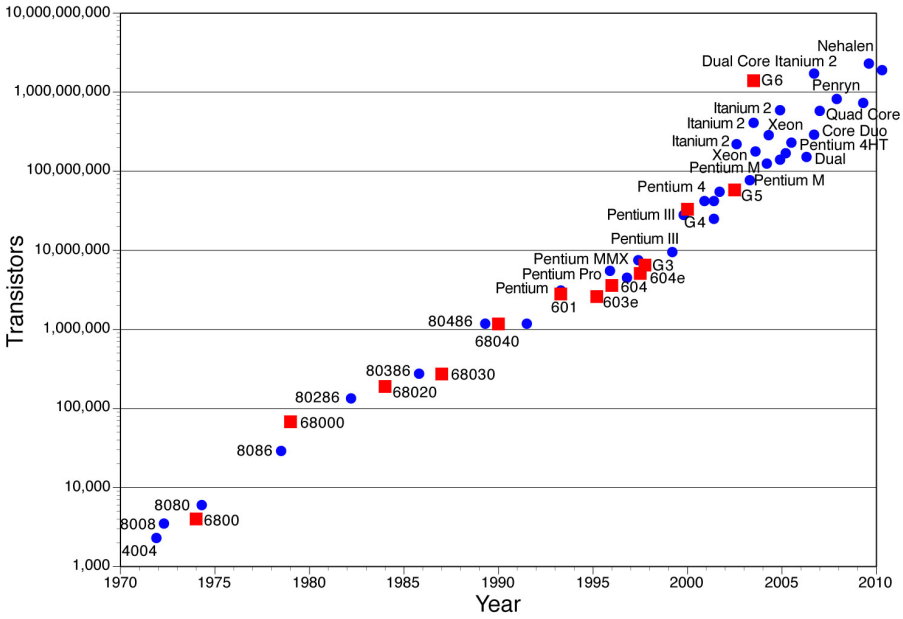
Az elmélet számos meglepő – az intuíciónak teljesen ellentmondó – elemet tartalmaz ilyenek például a hullám-részecske kettőség és az összefonódás jelensége, melyet a későbbiekben részletesen ismertetek (2.3). Alapja egy viszonylag egyszerű – lineáris algebrán alapuló – matematikai keretrendszer, nehézségét az újfajta látásmód jelenti. A jelenségek interpretációja (filozófiai értelmezése) a mai napig vita tárgyát képzi a tudományfilozófusok és a fizikusok körében.

A számítástudomány alapjait Alan Turing rakta le 1936-os cikkében [2] melyben definiálta az ún. Turing-gépet, mely az algoritmusok egy absztrakt modellje, sőt az akkoriban még nem létező számítógépek működését is leírja. Nem sokkal Turing cikkének megjelenése után Neumann János megfogalmazta [3] a róla elnevezett elveket, melyeken alapul a mai számítógépek többségének működése.

Az első számítógépek még elektroncsövekből épültek fel ezért méretükkel egész szobákat megtöltöttek. A nagy áttörést a méret terén Walter Brattain, John Bardeen és William Shockley 1947-es felfedezése a tranzisztor hozta el [4], mely eszköz a félvezetők tulajdonságait használja fel működéséhez és mérete már a kezdeti időszakban jóval kisebb volt mint az elektroncsöveké.

A technológia fejlődésének köszönhetően a tranzisztorokat sikerült egyre jobban lekicsinyíteni, ezen méret változás ütemére Gordon Moore 1965-ben [5] tett becslést, melyet ma Moore-törvényként ismerünk és azt állítja, hogy az egy chipre integrálható tranzisztorok száma kétévente megduplázódik, vagyis a méret csökkenés exponenciális ütemű (ld. 1. ábra). Ez a jósalt a mai napig megállja a helyét, jelenleg a legkisebb csíkszélesség 14 nanométer.

Hamarosan elérjük azt a határt ahol a tranzisztorok mérete oly kicsinnyé válik, hogy csak pár atomból fognak felépülni, ebben az esetben viszont működésük erősen befolyásolt lesz a kvantummechanika törvényei által. Ha nem sikerül ilyen méretű működőképes tranzisztorokat gyártani, az a gazdasági növekedés egyik alappillérét, a számítástechnikát fejlődésképtelenné tehetné. Az



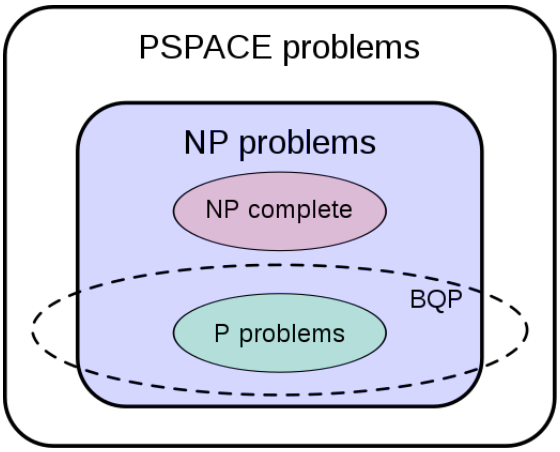
1. ábra. A Moore-törvény

említett méréthatár nagyjából 1 nanométer, amit a Moore-törvény alapján a közel jövőben elérünk. A probléma fontossága miatt a kutatók alternatív megoldásokat keresnek, az egyik ilyen a kvantumszámítógép.

Először Richard Feynmanban fogalmazódott meg a gondolat [6], hogy a kvantumeffektusok nem hátrányt, hanem előnyt jelenthetnek számítástechnikai szempontból, az ő ötlete az volt, hogy építhetnénk olyan számítógépeket, melyek a kvantummechanika elvei alapján működnek és ezek segítségével modellezhetnénk olyan fizikai folyamatokat, melyeket klasszikus számítógépekkel nem tudunk.

A következő nagy lépést a kvantuminformatika elméleti megalapozásában David Deutsch tette 1985-ben [7]. Ő az úgynevezett Curch-Turing tézist kutatta, mely sejtés azt állítja, hogy bármely algoritmikus folyamat megoldható Turing-géppel vagyis a Turing-gép egy univerzális modellje a különböző elven működő számítógépeknek. Ezen sejtést formailag sosem sikerült igazolni viszont tapasztalati tényként Turing ideje óta megállja a helyét. Deutsch ötlete a kvantummechanika posztulátumain alapuló számítógép megalkotása volt, ezt a felvetést a 2.1 részben tárgyalom.

Deutcsh felvetéséből kiindulva születtek kvantumalgoritmusok, melyek jelenlegi tudásunk szerint klasszikus számítógépekkel effektíven nem megoldható problémákra alkalmazhatóak. Az effektív ebben az estben azt jelenti hogy az algoritmus futási ideje a probléma nagyságának polinomiális függvénye. Ezeket a problémákat nevezzük **P** típusúnak a bonyolultságelméletben. Az egyik ilyen algoritmus Peter Shor nevéhez fűződik [8] aki megmutatta hogy a kvantumszá-



2. ábra. A problémaosztályok viszonya

mítógép képes polinomiális idő alatt prímtényezőkre bontani egész számokat. 2012-ben ezen algoritmus segítségvel sikerült a 21-et prímtényezőkre bontani [9]. A kvantumszámítógéppel szemben támasztott remények egyike, hogy képes lesz az ún. **NP-teljes** problémákat polinomiális idő alatt megoldani. Ezen problémák számos esetben előfordulnak a mindennapi gyakorlatban ilyen például a tőzsde folyamatainak előrejelzése vagy az útvonal tervezés - az ún. utazó ügynök probléma - sőt a matematikai bizonyítások is ebbe az osztályba tartoznak. Bár már létezik a problémaosztály megoldását gyorsító kvantumalgoritmus, az ún. Grover-algoritmus [10], egyenlőre polinomiális megoldást nem sikerült találni, sőt vannak olyan szakértők, akik úgy gondolják nem is lehet ezeket semmilyen eszközzel effektíven megoldani. Scott Aaronson 2005-ös publikációjában [11] felvetette, hogy az energiamegmaradás törvényéhez hasonlóan axiómában kellene megfogalmazni az **NP-teljes** problémák polinomiális idő alatti megoldhatatlanságát. A kvantumalgoritmusokkal megoldható problémákat az ún. **BQP** osztályba soroljuk melynek viszonya a **P** illetve **NP** osztályokkal még nem tisztázott (ld. 2. ábra).

A kvantumszámítógépek megalkotásának nehézségét az ún. dekoherencia jelensége okozza mely a környezettel való összefonódást jelent, vagyis a kvantumrendszerünket nem sikerül elszigetelnünk rendesen a külső hatásoktól, melyek befolyásolják, elrontják működését. Jelenleg többféle elképzelés létezik ezen probléma áthidalására, ilyen például az IBM által fejlesztet 17 kvantumbites processzor ami a szupravezetés jelenségét használja fel működéséhez. Egy másik, a Deutcsh-féle architektúrától eltérő modell, az adiabatikus kvantumszámítógép, mely lassú és folytonos transzformációkon keresztül változtatja a rendszer állapotát úgy, hogy a végső állapot tartalmazza a keresett megoldást [12]. Ezen rendszerek az alagúteffektus segítségével képesek olyan állapotátmenetekre, melyek klasszikusan nem lehetségesek, ilyen elven működik a Dwave 2000Q, mely rendszer 2048 kvantumbitet tartalmaz, viszont vita tárgyát képzi a kutatók kö-

rében, hogy képes-e gyorsabban megoldani problémákat mint egy hagyományos elveken működő számítógép [13].

A kvantummechanika jelenségein alapuló másik technológiai terület a kvantumkommunikáció melynek alapjait a klasszikus információelmélet szolgáltatta. Claude Shannon 1948-as publikációjában [14] matematikai úton definiálta az információ fogalmát , megfogalmazta a zajmentes illetve a zajos csatorna kódolási tételeit. Az első tétel – forráskódolási tétel – megadja a forrás tömöríthetőségének alsó határát, illetve bebizonyítja, hogy ezen határ alkalmas kódolással tetszőleges mértékben megközelíthető. A második tétel - csatornakódolási tétel – arról szól, hogy zajos csatornán hogyan lehet sérülés nélkül információt átvinni, ehhez Shannon megalkotta az ún. hibajavító kódolást és megadta azt a védelmi határt, melyet elméletileg el lehet érni ezen kódokkal.

A kvantum-információelmélet hasonló fejlődési pályát járt be, 1995-ben Benjamin Schumacher megalkotta a kvantum forráskódolási tételt [15]. A csatornakódolási tételnek ez idáig nem született kvantum analógja viszont a kvantum hibajavítást – melynek segítségével a kvantumszámítógépek működőképesek lehetnek majd zajos környezetben illetve lehetségessé válik a kommunikáció zajos kvantum csatornákon - már megalkották a kutatók.

A terület egyik fontos eredménye az ún. szupersűrűségű tömörítés, mely módszerrel két bitnyi információ vihető át egyetlen kvantumbit segítségével.

A kriptográfia többek között az üzentek titkosításával foglalkozik. A kriptográfia eljárásokat két csoportba sorolhatjuk a nyilvános illetve a privát kulcsú titkosítások.

Privát kulcs esetén a kommunikációban résztvevő felek megosztanak egymás között egy kulcsot mely segítségével titkosítják illetve megfejtik a küldött üzeneteket. A módszer nehézségét a kulcskiosztás okozza - vagyis a kulcs eljuttatása egyik féltől a másikig - hiszen ha megszerzi egy harmadik fél akkor illetéktelenül elolvashatja a titkosított üzeneteket.

1984-ben Charles Bennett és Gilles Brassard dolgozta ki [16] a kvantum kulcskiosztást melynek lényege, hogy ha valaki leakarja hallgatni a kvantumcsatornát miközben azon átküldik a kulcsot ahhoz mérést kell végeznie – bekell avatkoznia a rendszer viselkedésébe - a csatornán áthaladó kvantumbiteken, aminek következtében a rendszer állapota megváltozik, tehát a kulcs eltulajdonítása detektálható a kommunikációs felek által.

A nyilvános kulcsú titkosítások esetében az egyik kommunikációs fél (Bob) publikussá tesz egy kulcsot mely mindenki számára nyilvános. A másik fél (Alice) ha üzenetet szeretne Bobnak küldeni akkor ezzel a kulccsal titkosítja azt egy speciális módón úgy, hogy Bob csak a nyilvános kulccsal szorosan összefüggő, titkos kulccsal tudja megfejteni az üzenetet. Egy harmadik fél aki nem birtokolja ezt a titkos kulcsot elméletileg feltudja törni a kódot de ez olyan nagy számítási kapacitást venne igénybe ami nem állhat rendelkezésére. Ilyen titkosítási protokoll az RSA mely eljárás a nagy számok prímtényezőkre való bontásának nehézségén alapul, melyre az előzőkben említett Shor-algoritmus kínál megoldást polinomiális időben, vagyis a kvantumszámítógép megjelenése ezen titkosítási típusok elavulását eredményezheti.

Dolgozatom első fejezetében bemutatom a kvantuminformatika elméleti alap-

jait, majd ismertetek egy újfajta, kvantum jelenségek alapján működő protokollt, melynek kidolgozásában én is segédkeztem. A dolgozatom utolsó része a protokoll működésének kiértékelése az általam készített szimulációk alapján.

2. Kvantuminformatika

A következőekben tárgyalom a kvantummechanika posztulátumait (2.1) majd a (2.2) részben a posztulátumok alapján megalkotható kvantuminformatikai fogalmakat (pl.: kvantumbit, kvantumkapu stb.) ismertetem. A (2.3) részben a kvantum-összefonódás jelenségét mutatom be, a (2.4) részben pedig felvázolom egy általános kvantum algoritmus működését. Ezt a fejezetet a [17] [18] irodalmak felhasználásával készítettem el.

2.1. Kvantummechanika posztulátumai

A kvantuminformatikai rendszerek a kvantummechanika posztulátumain alapulnak, melyek a következők:

Első Posztulátum: Bármely zárt rendszer aktuális állapota jellemezhető egy $\mathbf{v}$ állapotvektorral a V Hilbert térben. A $\mathbf{v}$ vektor egység hosszúságú és együtthatói komplex számok.

Második Posztulátum: Bármely zárt fizikai rendszer időbeli változása leírható egy unitér transzformációval mely csak az időbeli változás kezdő- és végpontjától függ.

Harmadik Posztulátum: Bármely kvantum mérés leírható mérő operátorok halmazával $\{M_m\}$ ahol m a mérés lehetséges kimenetele. Annak a valószínűsége, hogy m-et mérünk ha a rendszerünk $\mathbf{v}$ állapotban van:

$$P(m \mid \mathbf{v}) = \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}, \tag{1}$$

ahol † az adjungált operátor. A mérés után a rendszer a következő állapotba kerül:

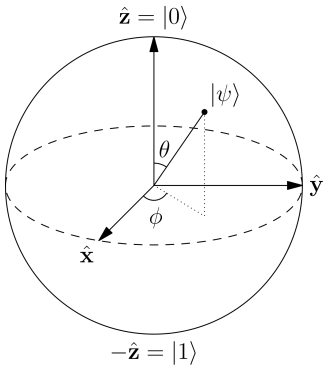
$$\mathbf{v}' = \frac{M_m \mathbf{v}}{\sqrt{\mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}}}. \tag{2}$$

Mivel a klasszikus valószínűségszámítás megköveteli, hogy:

$$\sum_m P(m \mid \mathbf{v}) = \sum_m \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v} \equiv 1, \tag{3}$$

ezért az operátoroknak ki kell elégítenie a következő teljességi relációt:

$$\sum_m M_m^\dagger M_m \equiv I. \tag{4}$$



3. ábra. Egy kvantumbit megjelenítése az ún. Bloch-gömb segítségével

Negyedik Posztulátum: Egy W összetett fizikai rendszer állapottere meghatározható az önálló rendszerek állapotterének tenzor szorzataként $W = V \otimes Y$. Továbbá $\mathbf{v} \in V$ és $\mathbf{y} \in Y$ esetén az összetett fizikai rendszer összekapcsolt állapota $\mathbf{w} = \mathbf{v} \otimes \mathbf{y}$.

2.2. A posztulátumok következményei

Az információ legkisebb egysége a bit, melynek értéke lehet 0 vagy 1. Az első posztulátum a bit kvantuminformatikai megfelelőjét a kvantumbitet (angol irodalomban: qbit) definiálja. Az ún. Dirac-féle jelölést alkalmazva ahol $|\cdot\rangle$ (ejstd: ket) az oszlopvektort jelöli, a számítási bázisok, melyek a kétdimenziós Hilbert tér bázisai: $|0\rangle$ és $|1\rangle$. Ezek az állapotok a klasszikus bit két állapotának feleltethetők meg, oszlopvektoros alakban felírva őket:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ és } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{5}$$

Egy tetszőleges $|x\rangle$ kvantumbit felírható a bázisok lineáris kombinációjaként

$$|x\rangle = a\,|0\rangle + b\,|1\rangle\,. \tag{6}$$

Ahol a és b az ún. valószínűségi amplitúdók, amikre igaz, hogy

$$|a|^2 + |b|^2 = 1. \tag{7}$$

A kvantumbit tehát egy kétdimenziós állapotvektor a Hilbert térben, fizikai megvalósítása lehet pl. egy elektron spinje. A klasszikus bittel ellentétben nem csak két különböző állapotot vehet fel, hanem egyszerre létezhet az összes lehetséges állapot szuperpozíciójában. Mérés hatására a kvantumbit az egyik bázisállapotba kerül - ezt nevezik a hullámfüggvény összeomlásának - a valószínűségi amplitúdók négyzetei megadják melyik bázisállapotba milyen valószínűséggel.

A második posztulátum alapján definiálhatók a kvantumkapuk, melyek a kvantumszámítógépet felépítő legkisebb alapegységek. A kapuk unitér operátorokkal jellemezhetők, melyek mátrixa kvadratikus ezért a kapuk ki és bemenetének száma megegyezik. A Pauli-X, Pauli-Y és a Pauli-Z kapuk mátrixai a következők:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{8}$$

ahol j a képzetes egység. Ezen kapuk segítségével a kvantumbitet az ún. Bloch-gömb x, y, z tengelye körül forgathatjuk. A Bloch-gömb a kvantumbit 3 dimenziós reprezentálásra szolgál, a negyedik dimenziót egy globális fázis segítségével vehetjük figyelmen kívül (ld. 3. ábra).

Az alapkapuk közé tartozik még a Hadamard-kapu melynek mátrixa:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{9}$$

A kapu bemenetére a bázis állapotokat adva:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{10}$$

adódik, a kapott állapotokban a valószínűségi amplitúdók egyformák, vagyis a két bázisállapot mérésének valószínűsége egyenlő, hiszen a valószínűségi amplitúdók négyzete $\frac{1}{2}$.

Az alapkapuk közé tartozik még az úgynevezett fázisforgató kapu melynek mátrixa:

$$P(\alpha) = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix}. \tag{11}$$

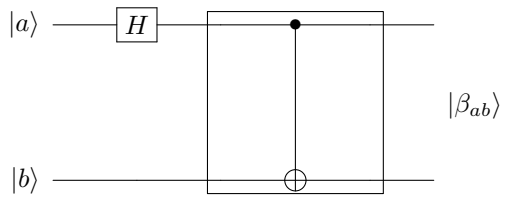
Két bemenettel rendelkezik az ún. CNOT kapu melyek az adat és a kontroll bementek, a kapu mátrixa:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{12}$$

Ha a kontroll bementen $|0\rangle$ állapot van, akkor az adatbemenet változatlanul jelenik meg az adatkimeneten, ha a kontroll bement $|1\rangle$ akkor az adatbemenet invertálva jelenik meg a kimeneten.

A harmadik posztulátum teremt kapcsolatot a klasszikus világunk - miden ami egy nanométernél nagyobb - és a kvantum világ között. A mérések nem reverzibilis folyamatok ezért nem is írhatóak le unitér operátorokkal. A posztulátum alapján látható, hogy maga a mérés megváltozatja a rendszerünk állapotát. A teljességi reláció segítségével ellenőrizhetjük, hogy egy mérés során az összes lehetséges kimenti állapotot figyelembe vettük-e.

A negyedik posztulátum alapján definiálhatók a kvantum regiszterek melyek több kvantumbit együtteseként adódnak. N darab kvantumbitből álló kvantum



4. ábra. Bell-állapotok előállítása

regiszter tartalma felírható a kvantumbitek tenzor szorzataként:

$$|x\rangle = |qbit_{N-1}\rangle \otimes |qbit_{N-2}\rangle \otimes ... \otimes |qbit_0\rangle \,. \tag{13}$$

Egy kvantumbit képes a két bázisállapotban lenni egyszerre, vagyis (13) alapján 500 darab kvantumbitből álló kvantum regiszter 2^{500} állapotban képes egyszerre lenni, ami több mint az ismert univerzum részecskéinek a száma.

2.3. A kvantum-összefonódás

A kvantummechanika egyik nehezen interpretálható (ld. EPR-paradoxon [19]) jelensége az összefonódás, mely lényegében két részecske közötti azonnali - tehát fénysebességnél gyorsabb - hatást jelent, ráadásul a sebessége független a részecskék távolságától. Fontos megjegyezni, hogy fénysebességnél gyorsabb kommunikációt, nem tudunk a segítségével megvalósítani, viszont a kvantuminformatikában széleskörűen alkalmazható jelenségről van szó.

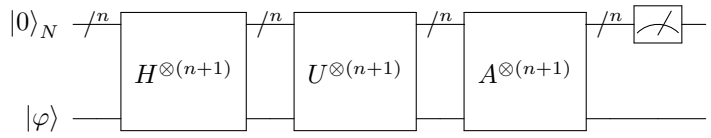
Összefonódott párok létrehozhatók egy Hadamard és egy CNOT kapu segítségével a 4. ábrán látható módon. A bementre adható állapotok a $\{|0\rangle, |1\rangle\}$ halmazból kerülnek ki. A kimenetet általánosan felírva:

$$|\beta_{ab}\rangle = \frac{|0,b\rangle + (-1)^a\,|1,NOT(b)\rangle}{\sqrt{2}}, \tag{14}$$

ahol a,$b \in \{0,1\}$ a bemeneti bázisállapotoknak megfelelően. A (14) formula az ún. Bell-állapotok - kétdimenziós összefonódott párok - általános leírására szolgál. Vegyük pl. a $|a\rangle = |0\rangle$ és $|b\rangle = |0\rangle$ bemeneteket, ekkor a kapott kimenet:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{15}$$

ezt az állapotot azért nevezzük összefonódottnak, mert nem tudjuk - a kvantum regisztereknél látott módon - kvantumbitek tenzor szorzatára dekomponálni. Fizikailag ez azt jelenti, hogy az egyik részecskén végzett mérés determinálja a másik részecske állapotát, és ezen hatás azonnal bekövetkezik. A Bell-állapotok ortonormális bázist alkotnak a 4-dimenziós Hilbert térben. Léteznek három (GHZ) és több dimenziós összefonódott állapotok is, ilyen speciális állapot a későbbiekben használt W állapot.



5. ábra. Általános kvantum algoritmust végző kvantum-áramkör blokkvázlata

2.4. Általános kvantumalgoritmus

Az előzőekben bemutatott alapkapuk és az összefonódás jelensége segítségével építhetők fel az összetettebb kvantumalgoritmusokat végző kapcsolások.

Egy ilyen kapcsolás felépítése az 5. ábrán látható. A hálózat bemenete $|0\rangle_N$ ami egy N dimenziós - $n = ld(N)$ kvantumbites - nullvektor és egy $|\varphi\rangle$ segéd kvantumbit. $|0\rangle_N$-ből a Hadamard-kapu segítségével előállítható egy olyan szuperpozíció ahol az N dimenziós Hilbert tér összes lehetséges bázisa egyenlő együtthatókkal - valószínűségi amplitúdókkal - szerepel. A következő lépésben az U transzformáció magát a műveletet végzi el, a párhuzamosságnak köszönhetően egy lépésben az összes lehetséges bázisállapoton.

A következő blokkrész az amplitúdó erősítésért felel, az előzőekben minden lehetséges állapotra elvégeztük a kívánt műveletünket, de a keresett választ ez alapján még nem tudjuk meghatározni, mivel minden állapot azonos valószínűségi amplitódóval szerepel. Ezért az amplitúdó-erősítés feladata csak azon bázisállapot amplitúdójának felerősítése, mely az U művelet értelmében a keresett válasz.

Utolsó lépésként a mérés következik, mivel a keresett válaszunk amplitúdóját felerősítettük, ezért nagy valószínűséggel ezt az állapotot fogjuk mérni. Egyes algoritmusok estén az amplitúdó erősítés nem ad 100%-os biztosítékot arra, hogy a mérés során a megfelelő állapotot kapjuk, annak csak a valószínűségét növeli. Ezért az algoritmust egymás után többször is lefuttatva határozható meg a keresett válasz.

Valójában a kvantumalgoritmusok megalkotásának nehézségét az okozza, hogy a párhuzamosított feladatmegoldás után valahogyan ki kell szűrni a keresett választ az amplitúdó-erősítés segítségével.

3. Csatornakiosztás összefonódással

A következő részben a közeghozzáférési problémáról és annak megoldásairól lesz szó. Először ismertetem a problémát és annak két klasszikus megoldását a sima illetve a réselt ALOHA protokollokat (3.1) ezen rész megírásához a [20] irodalmat használtam fel. Ezt követően (3.2) egy új a kvantummechanikai jelenségeken alapuló protokollt ismertetek, melyhez [21] még nem publikált cikket illetve a saját számításaimat használtam fel.

3.1. Közeghozzáférés klasszikus esetben

Az olyan hálózatokat melyekre több felhasználó csatlakozhat és mindegyikük küldhet adatot adatszóró csatornáknak nevezzük. Az ilyen hálózatok estén egy fontos megoldandó probléma hogy melyik felhasználó nyerje el a csatornahasználat jogát versenyhelyzetben, amikor egyszerre több állomás szeretne adni. A hagyományos rendszerekben az adatkapcsolati réteg alrétege az ún. MAC-alréteg (Medium Access Control) felelős a közeghozzáférés vezérléséért. Az alréteghez tartozó protokollok két csoportba - dinamikus és statikus - sorolhatóak.

Statikus esetben a csatornát felosztják a felhasználók között ez a felosztás lehet időszerinti (Time Division Multiplexing, TDM) ilyenkor miden felhasználó mindig ugyanabban a fix hosszúságú időrésben adhat mely a csomópontok számnak megfelelően periodikus, a felosztás lehet frekvencia szerinti (Frequency Division Multiplexing, FDM) ebben az esetben a csatorna sávszélességét a felhasználók számának megfelelően egyenlő méretű sávokra osztják és miden állomást hozzárendelnek az egyik sávhoz. A statikus csatornakiosztást alkalmazó protokollok hatásfoka alacsony hiszen ha egy felhasználó nem akar adni a csatornán akkor az időrése vagy frekvenciasávja kihasználatlanul marad.

A dinamikus csatornakiosztásra több megoldás is létezik, a következőekben az ún. ALOHA protokoll két típusát az egyszerű (pure) illetve a réselt (slotted) ALOHA-t ismertetem.

A protokollt az 1970-ben Norman Abramson alkotta meg [22], aki a Hawaii-szigetek közötti rádiós kommunikációt oldotta meg vele. A felhasználók akkor küldhetnek amikor akarnak, ha több felhasználó egyszerre küld akkor ütközés következik be és a csomagok elvesznek, erről a küldők a csatorna figyelésével értesülnek. Az ütközés után az elveszett csomagokat küldő felhasználók véletlen ideig várakoznak majd újra küldik a csomagjukat ezt addig ismétlik amíg a küldés sikeres nem lesz.

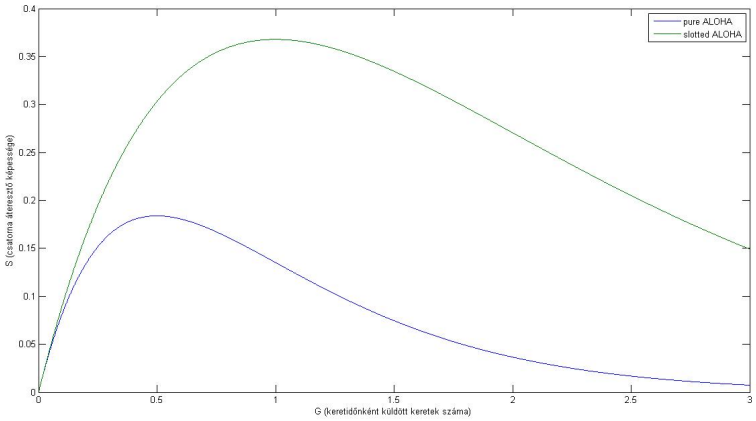
Az ALOHA protokoll hatékonyságának vizsgálatához vegyünk végetlen számú felhasználót akik fix méretű kereteket szeretnének küldeni a csatornán. Az egy keret átviteléhez szükséges időt nevezzük keretidőnek mely egyenlő a keret hosszának a bitsebességgel vett hányadosával. Tegyük fel, hogy a felhasználók a kerteket Poisson-eloszlás szerint állítják elő , keretidőnként átlagosan N keretet. Ha $N > 1$ akkor a küldött keretek nagy része elveszik, hiszen ilyenkor átlagosan egynél több felhasználó szeretne egyszerre küldeni, ezért ahhoz hogy elfogadható legyen a csatorna áteresztőképessége N-nek a [0,1] intervallumba kell esnie.

A csatornán az új keretek mellett az újra küldött keretek is közlekedhetnek, tegyük fel, hogy az új és régi keretek összege is Poisson-eloszlást mutat keretidőnként, melynek középértéke G (G>=N). Az áteresztőképességet (S) a sikeres átvitel valószínűségének (P_0) és az aktuális terhelésnek a szorzata adja

$$S = GP_0. \tag{16}$$

A Poisson-eloszlás alapján meghatározható annak a valószínűsége, hogy egy keretidő alatt k keretet szeretnének küldeni a felhasználók:

$$P_k = \frac{G^k e^{-G}}{k!}. \tag{17}$$



6. ábra. Az egyszerű illetve a réselt ALOHA protokollok áteresztőképessége a forgalom függvényében

Ebbe a képletbe $k = 0$-át behelyettesítve e^{-G} kapunk, mely annak a valószínűsége, hogy egy keretidő alatt senki sem akar küldeni. Az ún. kritikus szakasz azaz intervallum melyben ha két vagy több felhasználó egyszerre küld akkor ütközés következik be, ennek hossza két keret hosszúsággal egyezik meg mivel a már elküldött kerettel akkor nincsen ütközés ha legalább egy keretidővel előbb küldték illetve a következőnek küldött kerettel akkor nincs ütközés ha azt egy keretidővel később küldik. Tehát a sikeres küldés valószínűsége, vagyis hogy két keretidőn belül nincs más forgalom e^{-2G} . Ezt beírva (16)-ba a következőt kapjuk:

$$S = Ge^{-2G}. \tag{18}$$

Ha megnézzük a 6. ábrát, akkor jól látható, hogy az áteresztőképesség maximuma $G = 1/2$-nél van , értéke körülbelül 18%. Ennek az értéknek a javítására dolgozták ki a réselt ALOHA protokollt, ebben az esetben az időt diszkrét szeletekre osztják ezek az ún. slotok és hosszuk megegyezik egy keretidővel.

A felhasználók nem kezdhetnek el bármikor adni meg kell várniuk az új időrés kezdetét, emiatt szinkronizációra van szükség, mivel minden felhasználó számára egyértelműnek kell lennie mikor kezdődnek és mikor végződnek az időszeletek. Az egyszerű ALOHA diszkretizálásával a kritikus keretidő a felére csökken, így a sikeres küldés valószínűsége e^{-G} lesz, ezt beírva (16)-ba a következőt kapjuk:

$$S = Ge^{-G}. \tag{19}$$

A 6. ábrán láthatóan az új megoldás estén a csatorna áteresztőképességnek maximuma közel kétszeresére – nagyjából 37%-ra – nő az eredeti esethez képest. A fenti levezetésben a felhasználók száma végtelen volt, más megfontolásokból kiindulva levezethető a (20) képlet amely a csatornakapacitást a felhasználók számának függvényében adja meg, a függvény maximumát két felhasználó

esetén éri el, értéke 50%. Ha tartunk n-nel a végetlenhez akkor eredményül visszakapjuk a már levezetett 37%-os kapacitást:

$$S = \left(1 - \frac{1}{n}\right)^{n-1}. \tag{20}$$

3.2. Közeghozzáférés kvantum összefonódás segítségével

3.2.1. Az alapötlet

Kiindulásként vegyünk két felhasználót akik egy-egy kvantumbitet birtokolnak, majd hozzunk létre közöttük összefonódást a következő módon:

$$|w_2\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}}. \tag{21}$$

Ebben az esetben ha a felhasználók megmérik a tulajdonukban lévő kvantumbitet akkor az egyik $|0\rangle$-át fog mérni, míg a másik $|1\rangle$-et. Ráadásul egy adott felhasználó ugyanakkora valószínűséggel mérhet $|0\rangle$ illetve $|1\rangle$ értéket. Ha a $|1\rangle$ állapothoz hozzárendeljük a csatornahasználat jogát akkor a két felhasználó ugyanakkora valószínűséggel adhat a csatornán és teljes mértékben elkerülhető az ütközés. A (21) állapot n kvantumbites általánosítása:

$$|w_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |2^i\rangle \,. \tag{22}$$

Ebben az esteben minden felhasználó birtokol egy kvantumbitet az összefonódott állapotból, mivel a valószínűségi amplitúdók megegyeznek ezért minden felhasználónak egyenlő esélye van a csatornahasználat jogát megkapni.

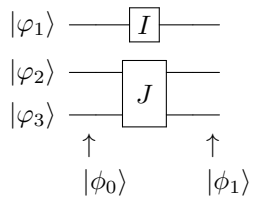
3.2.2. Új felhasználó esete

Felmerül a kérdés, hogy mi történik akkor ha egy új felhasználó szeretne csatlakozni a hálózathoz anélkül, hogy az összes többi csomóponttal találkozna. Ehhez induljunk ki a (21) állapotból, vagyis amikor két felhasználó tartózkodik a hálózaton. Célunk az, hogy az újonnan létrejövő állapot a (22) formula 3 kvantumbites alakja legyen:

$$|w_3\rangle = \frac{|100\rangle + |010\rangle + |001\rangle}{\sqrt{3}}. \tag{23}$$

A 7. ábrán $|\varphi_1\rangle$ és $|\varphi_2\rangle$ a már összefonódott pár tagjai, $|\varphi_3\rangle$ pedig az újonnan csatlakozó felhasználó kavntumbitje, kiindulási értéke $|0\rangle$. Az így kialakuló bemeneti állapot:

$$|\phi_0\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|100\rangle + |010\rangle}{\sqrt{2}}. \tag{24}$$



7. ábra. Harmadik falhasználó csatlakozik a hálózathoz

A 7. ábrán az I jelű kvantumkapu az úgynevezett idnetitás transzformáció mely nem változtat a bemenő kvantumbit állapotán, a J jelű kvantumkapu (JOIN) a csatlakozásért felelős, ennek szeretnénk meghatározni a mátrixát. Ha felhasználjuk a szuperpozíció elvét a következőt kapjuk:

$$\begin{aligned}(I \otimes J)\,|\phi_0\rangle &= \frac{1}{\sqrt{2}}(I \otimes J)\,|100\rangle + \frac{1}{\sqrt{2}}(I \otimes J)\,|010\rangle \\ &= \frac{1}{\sqrt{2}}(I\,|1\rangle \otimes J\,|00\rangle) + \frac{1}{\sqrt{2}}(I\,|0\rangle \otimes J\,|10\rangle).\end{aligned} \tag{25}$$

A (25) eredményeként szeretnénk megkapni a (23) állapotot. Ez sajnos nem lehetséges, mert az összeg első tagjából a (23) állapot egyetlen tagja, $|100\rangle$ állítható elő az identitás transzformáció miatt. Ez nem meglepő eredmény hiszen ez azt jelenti, hogy annak a felhasználónak aki nincs jelen az új csomópont csatlakozásánál nem változtatható meg az állapota, ha másképpen lenne akkor az fénysebességnél gyorsabb kommunikációt eredményezne. Tehát ezen felhasználó csatornahozzáférési valószínűsége - a valószínűségi amplitúdója abszolút értékének a négyzete mely jelen esetben $\left|1/\sqrt{2}\right|^2 = 1/2$ - nem változtatható meg. Azonban a (25) összeg másik tagjából előállítható a (23) szuperpozíció másik két tagja nevezetesen: $|010\rangle$ és $|001\rangle$. Ha a következő mátrixot alkalmazzuk:

$$J = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{26}$$

akkor a következő eredményt kapjuk:

$$|\phi_1\rangle = (I \otimes J)\,|\phi_1\rangle = \frac{1}{\sqrt{2}}\,|100\rangle + \frac{1}{2}\,|010\rangle + \frac{1}{2}\,|001\rangle\,. \tag{27}$$

A (27)-ből azt a következtetést vonhatjuk le, hogy a legjobb eredmény amit elérhetünk az, ha megfelezzük a valószínűséget az új csomópont és a kommunikációban eddig résztvevő felhasználó között, ezáltal a csatornakiosztás valószínűsége aszimmetrikussá válik. Megjegyzendő, hogy ebből előnyünk is származik hiszen így a csatorna használati jogok nem manipulálhatóak illetéktelenül. Mivel $|\phi_1\rangle \neq |w_3\rangle$ ezért bekell vezessük (22) állapot egy általánosított alakját:

$$|\tilde{w}_n\rangle = \sum_{i=0}^{n-1} a_{n-i}\left|2^i\right\rangle, \tag{28}$$

ahol a_{n-i} az $(n-i)$-dik felhasználó adási jogához tartozó állapot valószínűségi amplitúdója - az indexelés formája azt a célt szolgálja hogy az egyes sorszámú csomóponthoz tartozzon azaz állapot, melyben a legfelső helyiértéken áll az egyes - melyből a csomópont közeghozzáférési valószínűsége a következő módon számítható:

$$p_i = |a_i|^2 , \tag{29}$$

ezen valószínűségekre a klasszikus valószínűségszámítás megkötései alapján igaznak kell lennie a következő összefüggésnek:

$$\sum_{i=1}^{n} p_i = 1. \tag{30}$$

3.2.3. Prioritás beállítások

A csatorna használat jogát szándékosan is asszimterikussá tehetjük ha valamely felhasználónak nagyobb hozzáférési valószínűséget szeretnénk biztosítani vagyis prioritási beállításokat is implementálhatunk. Ehhez induljunk ki a (28) állapot két kvantumbites alakjából és vizsgáljuk meg hogyan lehetne a (31) $\tilde{J}$ operátor mátrixának elemeit úgy módosítani, hogy az adott felhasználó valószínűségének csak egy adott részét adja át az újonnan csatlakozó csomópontnak.

$$\tilde{J} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -j_2 & j_1 & 0 \\ 0 & j_1 & j_2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{31}$$

Tehát a bemeneti állapotunk:

$$|\phi_0'\rangle = |\tilde{w}_2\rangle \otimes |0\rangle = a_1 \overset{1.2.3.}{|100\rangle} + a_2 \overset{1.2.3.}{|010\rangle}, \tag{32}$$

ahol a számozás az adott sorszámú felhasználó kvantumbitjét jelöli. Ha erre alakalmazzuk az $I \otimes \tilde{J}$ transzformációt - az identitás operátor azért kell, mert a valószínűség átadás a 2. és a 3. felhasználó kvantumbitjei között megy végbe az első csomópont változatlan marad- akkor a következőt kapjuk:

$$\begin{aligned} (I \otimes \tilde{J}) |\phi_0'\rangle &= a_1 I |1\rangle \tilde{J} |00\rangle + a_2 I |0\rangle \tilde{J} |10\rangle \\ &= a_1 |100\rangle + a_2 j_1 |001\rangle + a_2 j_2 |010\rangle , \end{aligned} \tag{33}$$

vagyis a felhasználók valószínűségei a következőképpen alakulnak:

$$\begin{aligned} p_1 &= |a_1|^2 , \\ p_2 &= |j_2|^2 |a_2|^2 , \\ p_3 &= |j_1|^2 |a_2|^2 . \end{aligned} \tag{34}$$

Feladatunk a j_1 és a j_2 paraméterek megválasztása, ehhez vegyük a második és a harmadik felhasználó valószínűségének a hányadosát:

$$R_J = \frac{p_2}{p_3}. \tag{35}$$

A (35) képlet egy arányszámot határoz meg vagyis azt, hogy milyen mértékben ossza fel a valósíznűségét a második felhasználó önmaga és az új csomópont között. Ebbe a képletbe behelyettesítve a (34) eredményeit illetve felhasználva a $\tilde{J}$ operátor unitér jellegét - vagyis, hogy minden oszlopa egység hosszúságú - a következő egyenletrendszert kapjuk:

$$\begin{aligned} R_J &= \frac{|j_2|^2}{|j_1|^2}, \\ 1 &= |j_1|^2 + |j_2|^2. \end{aligned} \tag{36}$$

Ebből kifejezve j_1-et és j_2-t a következőt kapjuk:

$$j_1 = \sqrt{\frac{1}{R_J + 1}}, j_2 = \sqrt{\frac{R_J}{R_J + 1}}. \tag{37}$$

Tehát az így kapott mátrixunk a következő alakú:

$$\tilde{J} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{R_J}{R_J+1}} & \sqrt{\frac{1}{R_J+1}} & 0 \\ 0 & \sqrt{\frac{1}{R_J+1}} & \sqrt{\frac{R_J}{R_J+1}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{38}$$

Ha (38)-ba $R_J = 1$-et behelyettesítünk - vagyis $p_1 = p_2$ - akkor visszakapjuk az eredeti J mátrixban található $1/\sqrt{2}$ értéket, tehát $\tilde{J}$ operátor a J transzformáció általánosítása.

3.2.4. Álatlánosítás n felhasználó esetére

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & u_1 & u_2 & 0 \\ 0 & u_3 & u_4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{39}$$

Az előzőekben levezetett eset három felhasználóra vonatkozott, felmerül a kérdés, hogy lehet-e általánosítani n csomópontra. Ennek a levezetéséhez a (39) U operátort fogjuk alkalmazni, mégpedig azért, mert ez az általánosítás vonatkozik az előzőekben levezetett JOIN és a későbbiekben ismertetett TRANSFER és LEAVE operátorokra is. Induljunk ki (28) állapotból és tegyük fel, hogy a transzformációt az $(n-1)$-edik és az n-edik csomóponton hajtjuk végre - valójában teljesen relatív kit tekintünk az $(n-1)$-dik illetve az n-dik felhasználónak, tehát ez a feltétel mindig fennáll - vagyis a következő transzformációt szeretnénk végrehajtani:

$$|\tilde{w}'_n\rangle = (I^{\otimes n-2} \otimes U) \, |\tilde{w}_n\rangle \, . \tag{40}$$

Felhasználva a szuperpozíció elvét a fenti kifejezés a következőképpen alakítható tovább:

$$\begin{aligned} |\tilde{w}'_n\rangle = a_1(I^{\otimes n-2} \, |100...0\rangle \otimes U \, |00\rangle) + a_2(I^{\otimes n-2} \, |010...0\rangle \otimes U \, |00\rangle) + ... \\ + a_{n-1}(I^{\otimes n-1} \, |000...0\rangle \otimes U \, |10\rangle) + a_n(I^{\otimes n-2} \, |000...0\rangle \otimes U \, |01\rangle). \end{aligned} \tag{41}$$

A fenti kifejezésből látható, hogy U operátornak csak az utolsó két tagban van $|00\rangle$-től különböző bemenete, tehát csak a $|000...10\rangle$ illetve a $|000...01\rangle$ állapotok valószínűségeit tudjuk megváltoztatni, vagyis beláttuk, hogy a módszer általánosítható tetszőleges számú felhasználóra.

3.2.5. Inverz transzformáció

Természetesen a csomópontok nem csak csatlakozhatnak hanem ki is léphetnek a hálózatból, ilyenkor a távozó felhasználónak átkell adnia a valószínűségét a hálózat egyik tagjának, ehhez meg kell alkossunk egy LEAVE (L) operátort. Induljunk ki a (28) három kvantumbites alakjából melyből a 3-ik csomópont ki szeretne lépni vagyis:

$$(I \otimes L) |\tilde{w}_3\rangle = |\tilde{w}_2\rangle |0\rangle . \tag{42}$$

Ha a fenti egyenletet összehasonlítjuk a következővel:

$$(I \otimes \tilde{J}) |\tilde{w}_2\rangle |0\rangle = |\tilde{w}_3\rangle , \tag{43}$$

akkor megállapítható, hogy a kilépés az új csomópont csatlakozásának az inverz művelete:

$$L = \tilde{J}^{-1}. \tag{44}$$

Mivel a kvantumkapukat leíró transzformációk unitér operátorok ezért felhasználhatjuk azon tulajdonságukat, hogy inverzük megegyezik a Hermite-féle transzponáltjukkal (a mátrix elemenkénti konjugáltjának transzponáltja):

$$\tilde{J}^{-1} = (\tilde{J}^T)^* = \tilde{J}^\dagger, \tag{45}$$

továbbá mivel a $\tilde{J}$ mátrixa szimmetrikus és minden eleme valós (ún. hermetikus mátrix) ezért igaz rá, hogy:

$$\tilde{J} = \tilde{J}^\dagger. \tag{46}$$

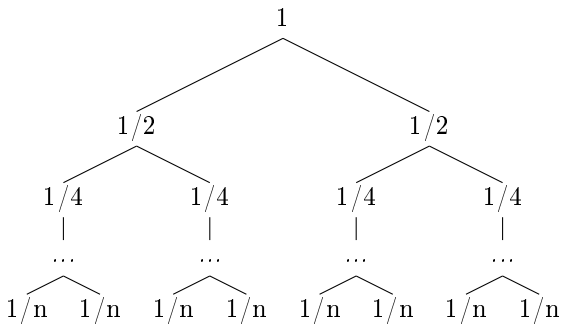
A (44), (45) és (46) összefüggéseket felhasználva:

$$L = \tilde{J}, \tag{47}$$

vagyis a LEAVE illetve a JOIN operátorok megegyeznek:

$$L = \tilde{J} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{R_L}{R_L+1}} & \sqrt{\frac{1}{R_L+1}} & 0 \\ 0 & \sqrt{\frac{1}{R_L+1}} & \sqrt{\frac{R_L}{R_L+1}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{48}$$

A fenti kifejezésben R_L ismét a két csomópont valószínűségének aránya ld. (35) viszont ebben az esetben a valószínűségek fix értékek továbbá azon felhasználó számára aki beállítja R_L értékét ismertnek kell lenniük, ez könnyen megoldható ha midenki tárolja egy memóriában a saját aktuális valószínűségét melyet minden adandó alkalommal frissít.



8. ábra. Valószínűségek alakulását reprezentáló fa

3.2.6. A szimmetrikus csatornakiosztás valószínűsége

Mint azt az előzőekben láthattuk tetszőleges számú csomópont csatlakozhat a hálózathoz és ha nem alkalmazunk prioritási beállításokat, akkor a legjobb lehetőség ha megfelezzük a valószínűséget egy régi és az új felhasználó között. Ennek alapján felrajzolható egy fa mely a valószínűségek alakulását ábrázolja, a 8. ábrán egy olyan fa látható melynek minden szintje egy adott számú populációra – mely mindig kettő hatványa kell hogy legyen – a szimmetrikus csatornakiosztást ábrázolja.

Felmerül a kérdés, hogy mi a valószínűsége annak, hogy minden csomópontnak megegyezik a valószínűsége abban az esetben, ha n darab felhasználó csatlakozik egyesével a kommunikációhoz. Természetesen a csatorna használati jog csak $n = 2^m$ esetén lehet szimmetrikus. Továbbá feltesszük hogy egy új felhasználó egyenlő valószínűséggel választ a kommunikáció tagjai közül.

Elsőként kiszámítjuk, hogy hányféle fát alakíthat ki n felhasználó. Két felhasználó egyféleképpen tud egymáshoz csatlakozni, a harmadik kétféleképpen, a negyedik háromféleképpen az n-ik felhasználó, pedig $n-1$ féleképpen, tehát:

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) = (n-1)! \; . \tag{49}$$

Ezen fák közt vannak olyanok, melyek megegyeznek egymással, ezek a szimmetrikus közeghozzáférését reprezentálják, számuk megállapításához azt kell ki találnunk hányféleképpen alakulhatnak ki. Vegyünk egy olyan n-1 felhasználóból álló fát, melyből létrejöhet a szimmetrikus kiosztást reprezentáló fa az n-ik felhasználó csatlakozásával, a célunk megállapítani hány ilyen fa létezik. Ezen fák biztosan tartalmazzák a szimmetrikus csatornakiosztást reprezentáló fát 2^{m-1} felhasználó estére, mely fából

$$k = 2^m - 2^{m-1} - 1 \tag{50}$$

felhasználó csatlakozásával a fentebb említett n-1 felhasználót tartalmazó fát

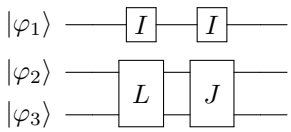
$$i = 2^m - 2^{m-1} = 2^{m-1} = \frac{n}{2} \tag{51}$$

féleképpen kaphatjuk meg, tehát az utolsó felhasználó i féle olyan fához tud csatlakozni, melyből megkapjuk a szimmetrikus csatornakiosztást reprezentáló fát n felhasználó estére, vagyis i darab egymással megegyező fát kaphatunk. Végeredményben a szimmetrikus csatornakiosztás valószínűségét n felhasználó esetében a szimmetrikus közeghozzáférést reprezentáló fák és az összes lehetséges fa hányadosa adja:

$$p = \frac{n/2}{(n-1)!} \,. \tag{52}$$

A fenti képlet csak akkor ad helyes értéket, ha n kettő valamely hatványa.

3.2.7. Szimmetrikus csatornakiosztás létrehozása



9. ábra. A TRANSFER operátor úgy is felfogható, mint a LEAVE és a JOIN operátorok szorzata

Az előzőekből láthatóan az új felhasználók csatlakozásával egyre jobban torzulnak a csatornahasználati jogok és annak a valószínűsége, hogy kiegyenlítődnek sok felhasználó esetén igen csekély, ezért bevezetünk egy új TRANSFER (T) transzformációt melynek feladata a már a hálózatra csatlakozott felhasználók valószínűségeinek módosítása.

Ezt úgy érjük el, hogy két csomópont találkozása estén bizonyos arányban megosztják egymás között a valószínűségeiket, valójában a folyamat úgy is felfogható, mintha az egyik csomópont kilépne és teljes valószínűségét átadná a másik felhasználónak, majd újra belépne és a két csomópont adott arányban osztozna a valószínűségen (ld. 9. ábra). Tehát:

$$T = L(R_L)\tilde{J}(R_J), \tag{53}$$

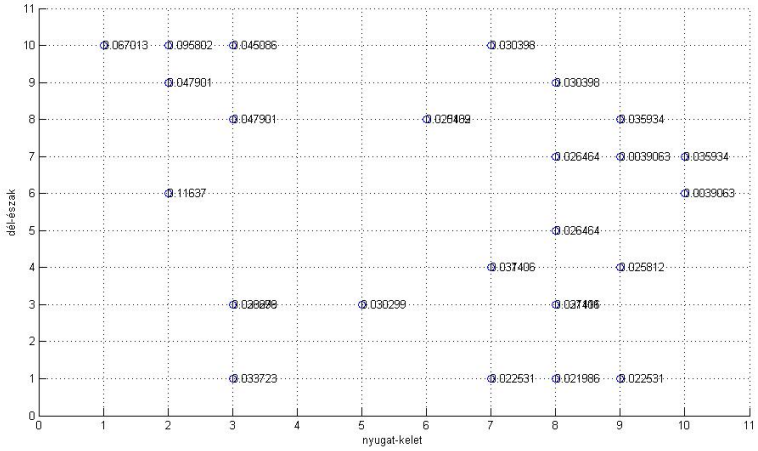
vagyis T operátor mátrixa felírható a következő alakban:

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & t_2 & -t_1 & 0 \\ 0 & t_1 & t_2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{54}$$

ahol a t_1, t_2 paraméterek az (53) mátrix szorzásból kaphatóak meg, az R_J illetve az R_L paraméterek alkalmas megválasztásával.

4. Szimulációs eredmények

A protokoll működésének teszteléséhez készítettem egy szimulációs környezetet, mellyel egy adott számú populáció viselkedését lehet megfigyelni. Maga a



10. ábra. A szimulált terület

modell több paraméterezhető elemet tartalmaz: állítható a csomópontok száma, a terület nagysága, a mozgás modell paraméterei illetve a ki és belépési valószínűségek

A mozgás szimulálásához a területet egy nxn-es raszterként modelleztem, ahol a szereplők minden szimulációs lépésben egy raszter távolságot léphetnek illetve várakozhatnak (ld. 10. ábra). A mozgás modellezéséhez véletlen bolyongásokat használtam, melyek jól alkalmazhatóak különböző egyedek mozgásának modellezésére [23].

A véletlen bolyongás legegyszerűbb formája az ún. egyszerű véletlen bolyongás mely esetben a csomópont egyenlő valószínűséggel választ, hogy melyik irányba lépjen (előre, hátra, jobbra, balra) és ez a döntés független az eddigi lépésektől. A modell egy bonyolultabb verziója a korrelált véletlen bolyongás mely esetben a következő lépés irányát befolyásolja az előző lépés iránya - ha az előző lépésben északi irányban haladt, akkor a következő lépésben is nagyobb valószínűséggel észak felé fog haladni - vagyis ez a módszer egy irányultságot ad a mozgásnak, viszont ha sok lépést átlagolunk akkor a lépések száma minden irányban ugyanakkora lesz, vagyis nincsen globális irányultság.

A 10. ábrán látható a terület raszterenkénti felosztása, illetve a felhasználók akiket karikák jelölnek. Minden felhasználó mellett megtalálható a csatornahozzáférési valószínűsége. A területhez fix irányok - észak, dél, kelet és nyugat - tartoznak, emellett minden csomópontnak van egy saját irányrendszere: jobbra, balra, előre és hátra. Tehát a csomópontnak mindig van egy szubjektív előre iránya, ami a négy fix irány közül bármelyik lehet. A mozgás modell paramétereivel az állítható, hogy mekkora valószínűséggel lépjen tovább a felhasználó a saját fő irányába (előre) illetve, hogy milyen valószínűséggel változtassa meg azt és váljék így az új irány a preferált iránnyá. Egyszerű bolyongás esetén ezek a

valószínűségek megegyeznek. A terület határára érve a csomópontok új főirányt választanak különben, a populáció a terület szélén csoportosulna.

A szimuláció kezdetén egy felhasználó birtokolja az összes valószínűséget. Minden egyes szimulációs lépésben az összes csomópont kisorsolja a mozgás modellnek megfelelően, hogy melyik irányban lép tovább egy rasztert. Ha egy raszteren tartózkodik olyan felhasználó aki rendelkezik valószínűséggel, illetve olyan felhasználó aki nem rendelkezik, akkor kettőjükre alkalmazzuk a JOIN operátort méghozzá úgy, hogy megfelezzük kettőjük között a valószínűséget.

Ha a raszteren két olyan felhasználó tartózkodik akiknek már van valószínűsége de azok nem egyeznek meg, akkor alkalmazzuk rájuk a TRANSFER operátort úgy, hogy összegezzük a valószínűségeiket majd megfelezzük közöttük azt. Ha egyszerre többen tartózkodnak egy raszteren akkor mindegyikük valószínűségét összeadjuk (ha valakinek nincsen akkor nullával számolunk) majd ezt átlagoljuk a szereplők számának megfelelően és szétosztjuk.

A modell egy bonyolultabb verziójában a LEVAE operátort is felhasználtam. A felhasználók egyik része aktív (tagja a hálózatnak) a másik része passzív (nem tagja a hálózatnak) illetve a csomópont lehet a két állapot közötti átmenetben, vagyis ha nem tagja a hálózatnak de csatlakozni szeretne hozzá, vagy tagja a hálózatnak de kiszeretne lépni belőle, mindkét esetben a csomópontnak addig kell várakozni míg találkozik egy másik felhasználóval akitől elvehet vagy akinek átadhat valószínűséget.

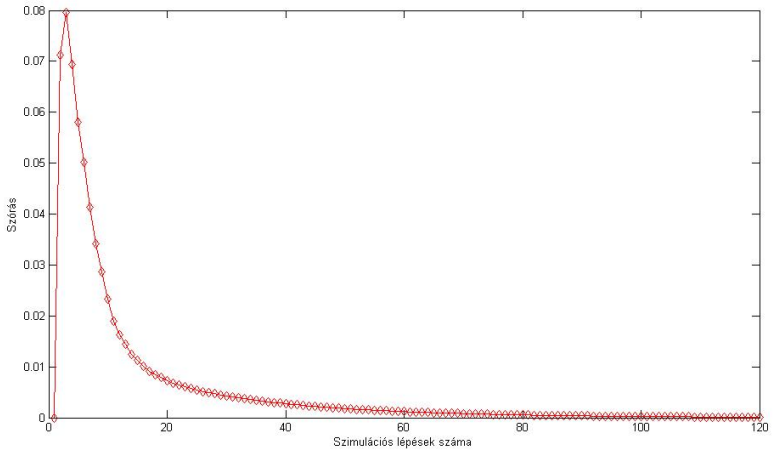
Az aktív csomópontok minden körben sorsolnak, hogy ki akarnak-e lépni a hálózatból, a passzív csomópontok pedig miden körben arról sorsolnak, hogy be szeretnének-e lépni a hálózatba. Ezen ki- illetve belépési valószínűségek állíthatóak. A maradék felhasználók akik éppen két állapot (aktív, passzív) között váltanak nem sorsolnak addig, amíg ezen állapotváltás be nem következik, vagyis míg ki nem lépnek (átadják valakinek a valószínűségüket) vagy be nem lépnek (valaki ad nekik valószínűséget) a hálózatból.

A kapott eredmények kiértékeléséhez a minta szórását használtam fel, mely az átlagtól való eltérés átlaga. Képlettel:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(p_i - m)^2}{N-1}}, \tag{55}$$

ahol p_i az i-dik felhasználó valószínűsége, m a valószínűségek átlaga, N pedig az akítv csomópontok száma.

A vizsgálatokat a ceteris paribus elv alapján végeztem, vagyis mindig csak egy paramétert változtattam és annak a hatását vizsgáltam. Az alap szimulációs beállítások (melyeket külön-külön változtattam) a következők: 100 darab csomópont, populációsűrűség 1 fő/raszter, nincs ki- illetve belépés a hálózatba, a mozgás modell korrelált bolyongás (50%-ban előre 20-20% jobbra illetve balra 5%-ban hátra lép illetve 5% eséllyel várakozik). Ezt az alap modellt vagy kicsit módosított verzióját minden esetben szimulálom hogy az összehasonlítás alapját nyújtsa. Minden szimulációt százszor futattam le és ezen eredményeket átlagoltam. A szimulációkat a Matlab segítségével készítettem el.



11. ábra. Kiegyenlítődés vizsgálata

4.1. Kiegyenlítődés

Ebben a szimulációban azt vizsgáltam, hogy a fent említett alap modell esetén létrejön-e a valószínűségek kiegyenlítődése.

A 11. ábrán láthatóan a szórás függvénye a nullába tart tehát a valószínűségek kiegyenlítődnek. Az elején található felfutását a függvénynek az eredményezi, hogy az első lépésekben csak pár felhasználó osztozik a valószínűségeken.

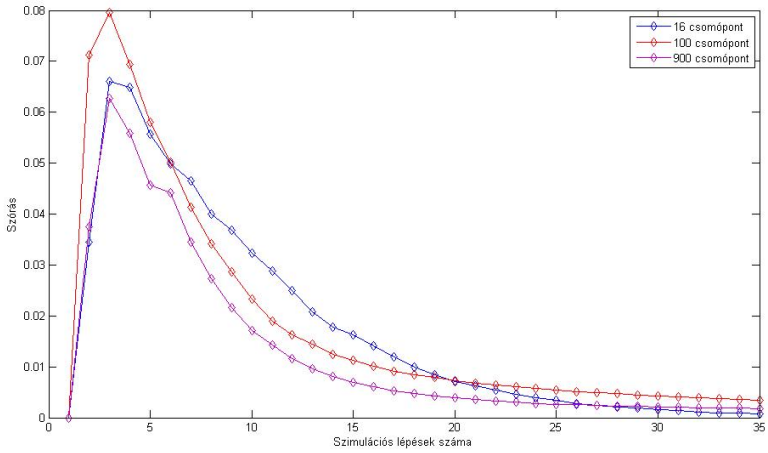
A szimuláció tanulsága, hogy a módszer működő képes vagyis a valószínűségek egy idő után kiegyenlítődnek így biztosítva minden csomópont számára az igazságos hozzáférést a csatornához.

4.2. Populáció nagysága

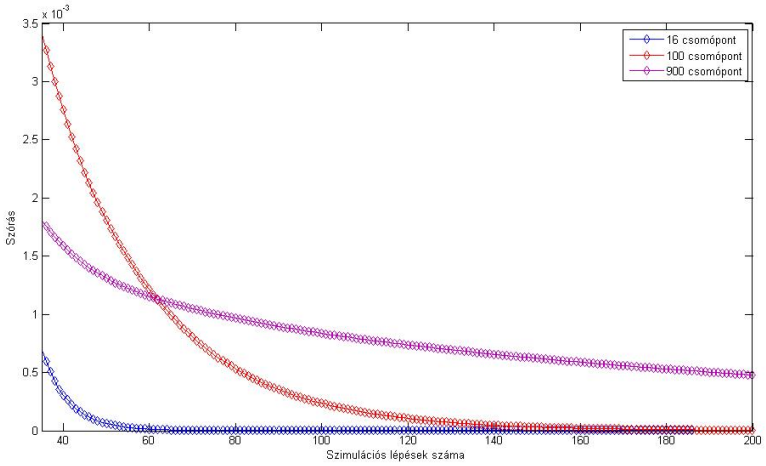
Ebben a szimulációban azt vizsgáltam, hogy a populáció létszáma milyen hatással van a valószínűségek kiegyenlítődésére. Három szimulációt futattam: 16, 100 és 900 darab felhasználóval. A populációsűrűség, vagyis az egy raszterre jutó felhasználók száma minden esetben egy volt. A használt mozgás modell korrelált véletlen bolyongás, nincsen ki- illetve belépés a hálózatba.

A 12. ábrán jól látható hogy mindhárom függvény a maximumát elérve aszimptotikusan tart a nullához, az is megfigyelhető hogy minél nagyobb a populáció létszáma annál meredekebb a függvény első szakasza, vagyis a valószínűségek kiegyenlítődése ebben a szakaszban annál gyorsabb minél több csomópontunk van.

A 13. ábra a 35-ik szimulációs lépéstől ugyanennek a három szimulációnak az alakulását ábrázolja, jól látható hogy a nagyobb felhasználó számú függvények kezdeti üteme csökken sőt minél többen vannak a felhasználók, annál lassabban közelíti a függvény aszimptotikusan a nullát.



12. ábra. Kiegyenlítődés vizsgálata a populáció függvényében

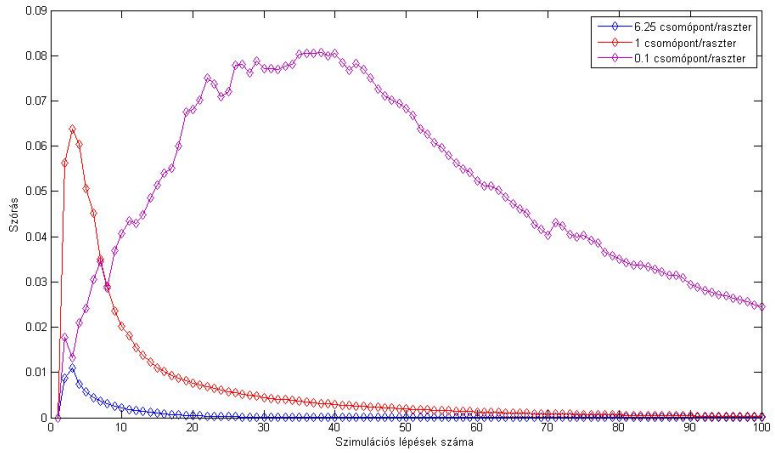


13. ábra. Kiegyenlítődés vizsgálata a populáció függvényében

4.3. Populációsűrűség

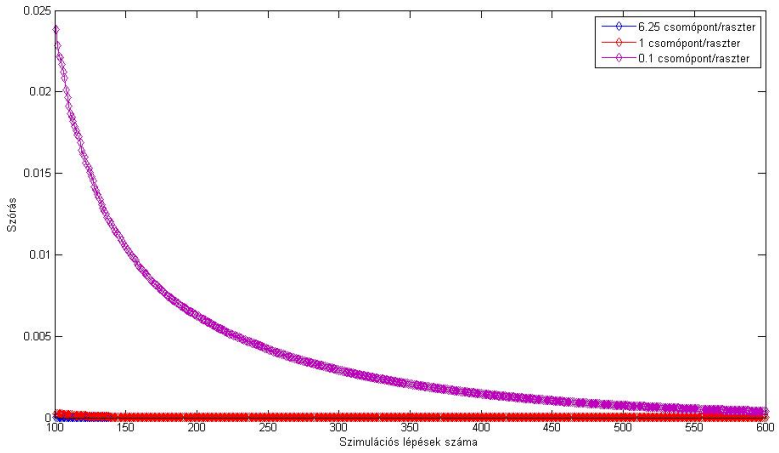
Ebben a szimulációban azt vizsgáltam, hogy a populációsűrűsége milyen hatással van a valószínűségek kiegyenlítődésére. Három szimulációt futattam: 6.25, 1 és 0.1 csomópont/raszter beállításokkal. A hálózat minden esetben 100 csomópontot tartalmazott. A használt mozgás modell korrelált véletlen bolyongás, nincsen ki- illetve belépés a hálózatba.

A 14. ábrán látható, hogy minél nagyobb a populációsűrűsége annál gyor-



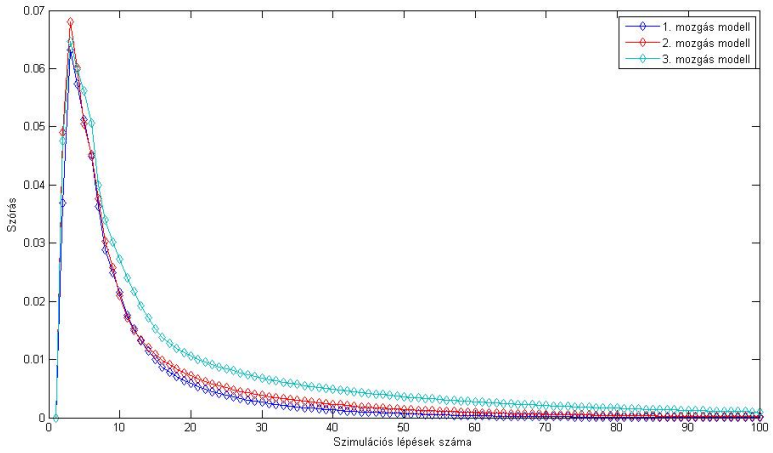
14. ábra. Kiegyenlítődés vizsgálata a populációsűrűségének függvényében

sabban egyenlítődnek ki a valószínűségek. Az ábrán az is megfigyelhető, hogy kicsi sűrűség esetén a függvény felfutási szakasza hosszabb lesz.



15. ábra. Kiegyenlítődés vizsgálata a populációsűrűségének függvényében

A 15. ábrán az látható, hogy bár lassabb ütemben de a kisebb sűrűségű populáció valószínűségeinek szórása is aszimptotikusan tart a nullába.



16. ábra. Kiegyenlítődés vizsgálata a mozgás modell függvényében

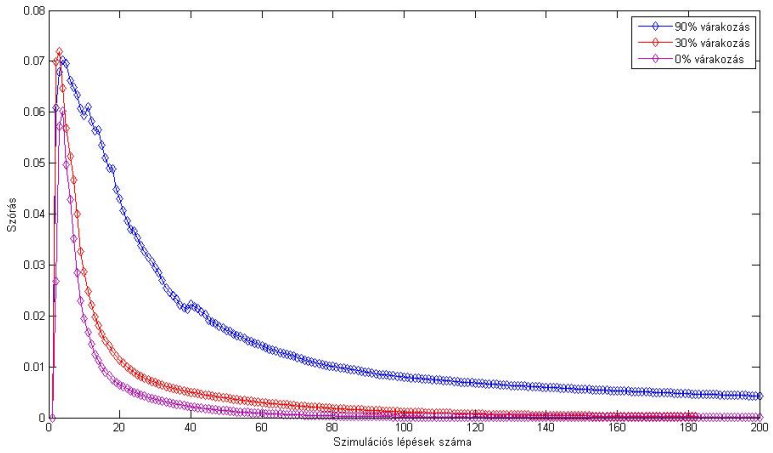
4.4. Mozgás modell

Ebben a szimulációban azt vizsgáltam, hogy a mozgás modell milyen hatással van a valószínűségek kiegyenlítődésére. Három szimulációt futattam: az első esetben igen erős a korreláció az egyes lépések között, a második modell az eddigiekben alkalmazott korrelációs bolyongás, a harmadik modell pedig egy egyszerű véletlen bolyongás, vagyis minden lépésben miden irányba ugyanakkora valószínűséggel mozdulnak el a csomópontok. A hálózat minden esetben 100 felhasználót tartalmazott, a populációsűrűség egy, nincsen ki- illetve belépés a hálózatba.

Az 16. ábrán jól látható, hogy a mozgás modell befolyásolja a kiegyenlítődés ütemét, minél nagyobb a korreláció az egyes lépések között annál gyorsabb a kiegyenlítődés. Megjegyzendő, hogy ez annak lehet a következménye, hogy a szimulációs terület egy zárt tér és az irányultság miatt a felhasználók a határvonalak felé mennek ahol számuk megsűrűsödhet.

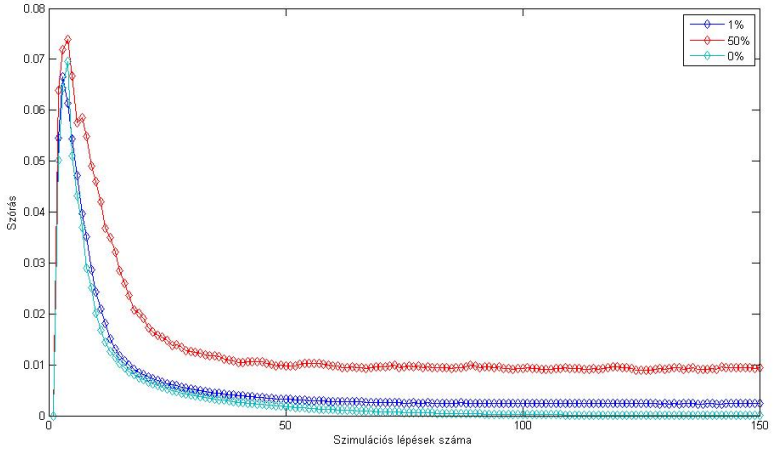
4.5. Várakozás

Ebben a szimulációban azt vizsgáltam, hogy a várakozás milyen hatással van a valószínűségek kiegyenlítődésére. Három szimulációt futattam: az első esetben 90% volt az esélye hogy egy csomópont lépes helyett várakozik, a második esetben 30% a harmadik esetben pedig nem volt várakozás. A hálózat minden esetben 100 felhasználót tartalmaz, a populációsűrűség egy, nincsen ki- illetve belépés a hálózatba. A 17. ábrán megfigyelhető hogy minél nagyobb annak a valószínűsége, hogy egy csomópont egyhelyben áll annál lassabban történik meg a kiegyenlítődés.



17. ábra. Kiegyenlítődés vizsgálata a várakozás függvényében

4.6. Szimmetrikus ki- illetve belépési valószínűség



18. ábra. Kiegyenlítődés vizsgálata a ki- illetve belépés intenzitásának függvényében

Ebben a szimulációban azt vizsgáltam, hogy a hálózatba való ki- illetve belépés milyen hatással van a valószínűségek kiegyenlítődésére. Három szimulációt futattam: az első esetben 1% volt az esélye hogy egy csomópont kilép a hálózatból ha eddig aktív volt illetve belép ha eddig passzív volt, a második esetben

50% a harmadik esetben pedig nem volt ki- illetve belépés. A hálózat minden esetben 200 felhasználót tartalmazott, a populációsűrűség egy, a mozgás modell pedig korrelált bolyongás volt. A 200 felhasználóból az első lépésben 100 aktív vagy csatlakozna a hálózathoz és 100 passzív, vagyis az első esetben átlagosan 1 felhasználó lép be illetve egy lép ki szimulációs lépésenként, míg a második esetben 50.

A 18. ábrán jól látható, hogy ha van ki- illetve belépés a hálózatba akkor a valószínűségek nem egyenlítődnek ki és szórásuk egy érték körül mozog. Minél nagyobb a be- illetve kilépés intenzitása annál nagyobb ez a szórás érték.

5. Összegzés

A kvantum kommunikációterületén az eddigi kutatások a kvantumbitek segítségével, kvantumcsatornán történő kommunikációval foglalkoztak. Jelen dolgozat témája egy olyan eljárás mely a klasszikus csatornán történő kommunikációnál alkalmazható.

A protokoll bizonyíthatóan jobb hatásfokú mint klasszikus társa a réselt ALOHA. Klasszikus esetben a hatékonyság függ a falhasználók számától, minél többen vannak annál rosszabb, ráadásul 100%-os áteresztőképesség nem érhető el a csak 50% és 37% közötti értékek. A réselt ALOHA ráadásul függ a küldési stratégiától vagyis, hogy hány keretet szeretnének a felhasználók átlagosan küldeni keretidőnként, sőt a csatornán nem csak ütközések hanem kihasználtan (üres) keretidők is előfordulnak.

Az új protokoll előnye, hogy nincsenek üres keretidők vagyis minden időrésben valaki csomagot fog küldeni, ráadásul ez a módszer ütközés mentes átvitelt biztosít, vagyis 100% hatékonyságú illetve nincs szükség újraküldésre és a csatornát se kell figyelni. További előny, hogy a módszer hatékonysága független a felhasználók számától, sőt a felhasználók tetszés szerint ki illetve beléphetnek a hálózatba. A protokoll nem igényel bázisállomást a kommunikáció levezényléséhez ezért biztonságosnak mondható, mivel nincs olyan csomópont melyet megtámadva az egész hálózat összeomlana.

A szimulációs eredmények alapján a protokoll működését bizonyos paraméterek befolyásolhatják, viszont ez a hatékonyságot nem érinti csak az egyes csomópontok adási jogait. Ezek az adási jogok csak extrém körülmények között (pl.: ha rengeteg új felhasználó csatlakozna illetve rengeteg új felhasználó lépne ki a hálózatból folyamatosan) módosulnak annyira, hogy a csatornahozzáférés igazságosságát jelentősen befolyásolnák.

6. Irodalomjegyzék

[1] M. Planck, *The Theory of Heat Radiation*. 1914.

[2] A. M. Turing, „On computable numbers, with an application to the entscheidungsproblem," 1936.

[3] J. Neumann, „First draft of a report on the edvac," 1945.

[4] W. B. Shockley, „Circuit element utilizing semiconductive material," 1948.

[5] G. E. Moore, „Cramming more components onto integrated circuits," 1965.

[6] R. P. Feynman, „Simulating physics with computera," 1982.

[7] D. Deutsch, „Quantum theory, the church-turing principle and the universal quantum computer," 1985.

[8] P. W. Shor, „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," 1995.

[9] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," 2012.

[10] L. K. Grover, „A fast quantum mechanical algorithm for database search," 1996.

[11] S. Aaronson, „Np-complete problems and physical reality," 2005.

[12] B. Nagy, *Új számítási paradigmák*. Typotex Kiadó, 2013.

[13] A. Cho, „Quantum or not, controversial computer yields no speedup," 2014.

[14] C. E. Shannon, „A mathematical theory of communication," 1948.

[15] B. Schumacher, „Quantum coding," 1995.

[16] C. H. Bennett and G. Brassard, „Quantum cryptography: Public key distribution and coin tossing," 1984.

[17] S. Imre and F. Balázs, *Quantum Computing and Communications An Engineering Approach*. John Wiley & Sons Ltd, 2005.

[18] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[19] A. Einstein, B. Podolsky, and N. Rosen, „Can quantum-mechanical description of physical reality be considered complete?," 1935.

[20] A. S. Tanenbaum and D. J. Wetherall, *Számítógép-hálózatok*. Panem kft., 2013.

[21] S. Imre and M. Bérces, „Entanglement-based competition resolution in distributed systems," 2017.

[22] N. Abramson, „The aloha system: another alternative for computer communications," 1970.

[23] E. Codling, M. Plank, and S. Benhamou, „Random walk models in biology," 2008.