Eötvös Loránd Tudományegyetem,
Természettudományi Kar

Szakdolgozat

Mérésekkel befolyásolt kvantumdinamika qubiteken és a káosz megjelenése

Tóth László Dániel
III. éves fizika Bsc.

Témavezető: **Kiss Tamás**, PhD (tudományos főmunkatárs)
Szilárdtestfizikai és Optikai Kutatóintézet
Kvantumoptikai és Kvantuminformatikai Osztály

Belső konzulens: **Cserti József**, C.Sc. (egyetemi docens)
Eötvös Loránd Tudományegyetem, Természettudományi Kar
Komplex Rendszerek Fizikája Tanszék

Budapest, 2010.05.27.

FIGYELEM! A DOLGOZAT HIHETETLEN MENŐ ÁBRÁKAT TARTALMAZ. HA ÖNNEK BÁRMILYEN TÍPUSÚ ÉRZÉKENYSÉGE VAN EZEKRE (PÉLDÁUL EPILEPSZIÁS ROHAMOK KIEMELKEDŐ ESZTÉTIKAI ALKOTÁSOK MEGTEKINTÉSE KÖZBEN), AKKOR A DOLGOZAT ELOLVASÁSA ELŐTT KONZULTÁLJON KEZELŐORVOSÁVAL.

Kivonat

A qubit egy kurrens terület, a kvantuminformatika alapegysége, a klasszikus bit kvantummechanikai általánosítása. Egy egyszerű, fizikailag is megvalósítható kvantumoptikai transzformáció qubiteken, ha mérés eredményétől is függővé tesszük, nemlineáris dinamikát eredményezhet. Iteratív ismétlések során a dinamika kaotikussá válhat és már az egy qubites rendszer esetében is gazdag viselkedéshez vezet. A dolgozat fő célja ennek a viselkedésnek a bemutatása és feltérképezése, analitikus és numerikus eszközökkel. Egy qubit esetét Bloch-reprezentációban is vizsgáljuk, mely a kevert állapotok leírására alkalmas. A több qubites esetben vizsgáljuk a transzformáció tisztító protokollokra való alkalmazását, mely kvantuminformatikai felhasználás szempontjából bír jelentőséggel. Kitérünk az általánosítási lehetőségekre is.

Tartalomjegyzék

1. Bevezetés

> "Anyone who uses words "quantum" and "chaos" in the same sentence should be hung by his thumbs on a tree in the park behind the Niels Bohr Institute."
>
> Joseph Ford

A kvantummechanika és a káosz kapcsolatának feltárása és körüljárása - a nagy érdeklődés és lelkesedés ellenére vagy talán pont ezen okokból - mindig is meglehetősen nehézkes feladatnak bizonyult és heves vitákat váltott ki fizikus és matematikus körökben, sőt ihletet adott egyéb - nem csak természettudományhoz tartozó - diszciplínáknak is. Bár a bevezető idézet kapcsán - melynek relevanciáját nyilvánvalóan a dolgozat címe adja - felmerülhet az igény, hogy a "kvantumkáosz" problémájába részletesebben belemenjünk, ezt mégsem tesszük meg. Egyrészt, mert a témának mára rendkívül kiterjedt irodalma van, és az ez iránt érdeklődőket igényes összefoglaló munkákhoz irányítjuk [6, 9]. A másik, ennél nyomósabb tényező, hogy az általunk vizsgált káosz sok szempontból különbözik attól, amire általában "kvantumkáoszként" hivatkoznak.

A káosz fő jellemzője és klasszikus meghatározása a kezdeti feltételekre való exponenciális érzékenység, melynek vizsgálata már a XIX. század végén megkezdődött (Poincaré, 1892 [24]). Zárt kvantummechanikai rendszerekben az időfejlődés azonban unitér, ami megtiltja az állapotok exponenciális távolodását, ha a távolság alatt az állapotok természetes Hilbert-terében vett távolságot értjük. A kvantumkáosz kifejezés általában a klasszikusan kaotikus jelleget mutató rendszerek kvantált megfelelőire vonatkozik.

A kvantummechanikai mérés - és itt nem megyünk bele a kvantummechanikai interpretációk kiterjedt méréselméleti vitáiba - azonban megtöri az unitér fejlődést és nemlineáris dinamikát eredményezhet. Ha például a rendszer folytonos mérésnek van alávetve (mely egy jó modellje lehet a környezet által okozott dekoherenciának), akkor ez már egy nemlineáris, sztochasztikus Schrödinger-egyenlet szerint fejlődik időben. Az ilyen rendszerekről a közelmúltban bebizonyították (Habib et al, 2006 [10]), hogy kaotikus viselkedést mutathatnak kvantumos tartományban - azaz a klasszikus limesztől távol - is. Numerikus eszközökkel megmutatták, hogy a helyoperátor várható értékére vett Ljapunov-exponens pozitív. Abban az irányban is kutatás folyik, hogy kimutassák a káoszt olyan rendszerekben, melyeken csak gyenge mérést engedünk meg, de a mérési eredményt visszatáplálhatjuk, amely effektív nemlinearitást eredményezhet [14]. A kaotikus jelleg szigorú bizonyítása ilyen feltételek mellett eddig nem sikerült.

A dolgozatban azonban ezektől eltérő káoszt mutatunk be. Kvantuminformatikai felhasználásban gyakran előforduló eljárás, hogy a mérést rendszerek (például qubitek) sokaságán végezzük és a mérési eredménytől függően a rendszer egy részét leválasztjuk. Ilyen procedúrán alapulnak például az állapottisztító protokollok [7, 15]. Ez a feltételes dinamika (ahol a feltételességet a mérési eredménytől való függésre értjük) eredetileg lineárisan fejlődő rendszerekbe nemlinearitást hoz be és káoszhoz vezethet [13]. A dinamikát ilyen esetekben, ahogy azt meg fogjuk mutatni, egy nemlineáris $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$ leképezés jellemzi, ezért erre komplex káoszként hivatkoznak [12]. Ez a tulajdonság, azaz hogy a leképezés értelmezési tartománya a (kiterjesztett) komplex számok halmaza, a klasszikus esettől való különbözőséget is mutatja. Nem ismerünk más olyan fizikai rendszert, ami expliciten ilyen típusú dinamikát valósítana meg.

A dolgozat felépítése a következő. A 2. fejezetben áttekintjük az általunk - és a kvantuminformatikában általában - használt formalizmust és a későbbiekben is vizsgált mennyiségek jelölésmódját és hátterét. A 3. fejezetben rátérünk annak a transzformációnak a vizsgálatára, mely a dolgozat fő témáját alkotja. Az egy qubites tiszta esetben a részletes analitikus vizsgálat mellett, melynek főbb eredményei az irodalomban megtalálhatók [13, 12], numerikus szimulációt is készítettünk a kaotikus jelleg szemléltetésére (ehhez kapcsolódó néhány további szimulációs eredmény a koherencia kedvéért az A függelékben található). A Bloch-reprezentáció segítségével analitikus megközelítést adunk a kevert állapotok leírására is, melyet az irodalomban még nem vizsgáltak. A két qubites eset már egy jóval nagyobb paramétertartománnyal rendelkezik, így a megfelelő reprezentáció keresése jelentőssé válik. Megmutatjuk, hogy ebben az esetben a transzformáció alkalmas paraméterekkel állapottisztító protokoll megvalósítására használható (az állapottisztítás motivációjának illusztrálására a B függelékben két, az irodalomban már jól ismert kvantumkommunikációs protokollt mutatunk be). Vizsgáljuk a protokoll stabilitását a paraméterekre. A dolgozat utolsó részében az ismertetett transzformáció általánosítását tárgyaljuk.

2. Formalizmus

2.1. Kevert állapotok és sűrűségoperátor

Elevenítsük fel a kvantummechanika néhány alapvető gondolatát, axiómáját. A fizikai állapotok terét egy $\mathcal{H}$ Hilbert-téren értelmezzük. Egy zárt rendszer időfejlődése mindig leírható egy unitér operátorral. Egy adott $B = \{|\varphi_i\rangle \in \mathcal{H}\}$ ortonormált bázisra nézve egy $|\psi\rangle = \sum \alpha_i |\varphi_i\rangle$ állapoton végrehajtható egy (von Neumann-féle) mérés, melynek eredménye a $|\varphi_i\rangle$ állapot $|\alpha_i|^2$ valószínűséggel és a mérés az állapotot $|\varphi_i\rangle$-ben hagyja.

Ha tehát ismert a $|\psi\rangle \in \mathcal{H}$ állapot, akkor a rendszerről teljes információnk van (koppenhágai értelmezés). Felmerül a kérdés, hogy milyen formalizmust érdemes bevezetni, ha az állapotvektort nem tudjuk, csak az állapotok valószínűségi eloszlása ismert, azaz

$$\{(|\psi_k\rangle, p_k)\}_{k=1,2,\ldots} \qquad 0 \le p_k \le 1 \qquad \sum_k p_k = 1 \tag{1}$$

Ilyen esetben kevert állapotról beszélünk. Itt tegyük fel, hogy $|\psi_k\rangle$ lineárisan független, ortonormált elemek. Egy tetszőleges A fizikai mennyiséghez rendelt
$\hat{A} : \mathcal{H} \to \mathcal{H}$ operátor várható értékét ebben az esetben a kvantummechanikai és a statisztikai átlagolás egymásutánjaként definiálhatjuk, azaz

$$\langle \hat{A} \rangle = \sum_k p_k \langle \psi_k | \hat{A} | \psi_k \rangle \tag{2}$$

A kevert állapot jellemzése (1) szerint nehézkes, mivel nagyon sok paraméterre van szükségünk. Ezért konstruálunk egy matematikai objektumot, mely alkalmas a számolásra és a fenti információkat magában foglalja: a $\hat{\rho}$ sűrűségoperátort. Ezt úgy definiáljuk, hogy sajátvektorai (1)-ben szereplő $|\psi_k\rangle$ vektorok, sajátértékei pedig az ezekhez tartozó p_k értékek legyenek, azaz

$$\hat{\rho} |\psi_k\rangle = p_k |\psi_k\rangle \tag{3}$$

Ez projektorfelbontással tehető meg:

$$\hat{\rho} \equiv \sum_k p_k |\psi_k\rangle\langle\psi_k| \tag{4}$$

Könnyen ellenőrizhető, hogy ez valóban tudja az elvárt (3) egyenletet. Ennek segítségével

(2) egyszerű formára módosul:

$$\langle \hat{A} \rangle = Tr(\hat{\rho}\hat{A}) \tag{5}$$

A konstrukcióból következően a sűrűségoperátornak hasznos tulajdonságai vezethetők le:

1. $\hat{\rho} = \hat{\rho}^\dagger$ (hermitikus), mivel $p_k \in \mathbb{R}\ \forall\ k$
2. $\langle\psi|\hat{\rho}|\psi\rangle \geq 0\ \forall\ |\psi\rangle$ (pozitív), mivel $p_k \geq 0\ \forall\ k$
3. $Tr(\hat{\rho}) = 1$, mivel $\sum_k p_k = 1$

Ez a három tulajdonság definiál egy sűrűségoperátort; egy tetszőleges, a feltételeket teljesítő operátor a rendszer egy lehetséges sűrűségoperátora. Említsünk meg még két tulajdonságot, melyek az előzőekből könnyen levezethetők és a későbbiekben is használni fogjuk ezeket.

I $Tr(\hat{\rho}^2) \leq 1$ és az egyenlőség csak tiszta állapot esetén áll fenn. Ez a tulajdonság tehát felhasználható az állapot tisztaságának az eldöntésére.

II Ha egy U unitér operátort hattatunk egy kezdetben ρ sűrűségoperátorral jellemzett kevert állapotra, akkor ez az operáció után $\rho' = U\rho U^\dagger$ sűrűségoperátorral jellemzett állapotba megy át.

Vegyük észre, hogy az I. tulajdonság alkalmas annak eldöntésére, hogy az állapot tiszta-e vagy kevert, a kevertség számszerű jellemzésére azonban nem. Erre általában a von Neumann entrópiát érdemes bevezetni [31]:

$$S(\rho) \equiv -Tr(\rho \log_2 \rho) = -\sum_i p_i \log_2 p_i \tag{6}$$

ahol p_i-vel jelöltük ρ sajátértékeit. A második tag a klasszikus Shannon-entrópia a sajátértékekre nézve.

2.2. Qubitek reprezentálása

Az érdeklődés a kétállapotú kvantumos rendszerek vizsgálata iránt a kvantummechanikával egyidős. Ez a terület az utóbbi időben új lendületet és megvilágítást kapott, ahogy kiszélesedtek a perspektívák a kvantummechanika alkalmazásait illetően. Ilyen rendszereknek számos realizációja létezik (például az elektron spinje, egy atom alap és gerjesztett állapota, a foton kétféle polarizációja) és röviden és összefoglalóan ezeket - kvantuminformatikai kifejezéssel - qubitnek szokás hívni (ezt a terminust Benjamin Schumacher vezette be 1995-ben [25]). A qubitek széleskörű felhasználásával felmerül tehát az igény, hogy a qubiteknek megfelelően szemléletes, jól kezelhető reprezentációkat keressünk.

2.2.1. Riemann-féle paraméterezés

Egy tiszta qubit állapotát egy komplex egységvektor jellemez a 2 dimenziós Hilbert-térben, mely általánosan

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1 \tag{7}$$

alakban írható, ahol $\{|0\rangle, |1\rangle\}$ legyenek ortonormált bázisvektorok. Kiemelve β-t és bevezetve $z = \alpha/\beta \in \tilde{\mathbb{C}}$ jelölést az állapot felírható egy paraméter segítségével, ahol $\tilde{\mathbb{C}} = \mathbb{C} \cup \infty$ a kiterjesztett komplex sík (vagy Riemann-gömb):

$$|\psi\rangle = N\left(z|0\rangle + |1\rangle\right) \quad z \in \tilde{\mathbb{C}} \quad N = (1 + |z|^2)^{-1/2} \tag{8}$$

Ebben a formában $z = \infty$ felel meg a $|0\rangle$ állapotnak. Ez a qubit Riemann-féle paraméterezése [30, 22].

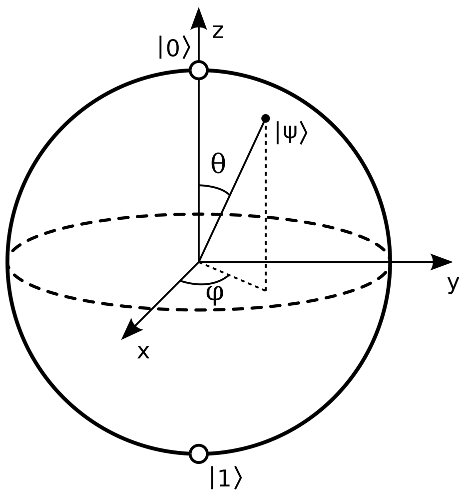
2.2.2. Bloch-gömb és Fano-alak

Vizsgáljuk tovább az eredeti (7) alakot. A mérési axiómát figyelembe véve az állapotvektor csak egy globális fázis erejéig meghatározott, azaz $|\psi\rangle$ és $e^{i\varphi}|\psi\rangle$ állapotokat ekvivalensnek tekintjük. Így (7) átírható

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{9}$$

alakra, ahol $\varphi \in [0, 2\pi)$ és $\theta \in [0, \pi]$. θ helyett a következőkben megmutatott szemléletesség és az ábrával való egyezés kedvéért írunk $\theta/2$-t. A két komplex paraméterről tehát áttértünk valós gömbi paraméterezésre, az állapot egyértelműen jellemezhető az $\mathbb{R}^3$-beli gömb (Bloch-gömb) felszínének egy pontjával.

A állapot Descartes-koordinátái a gömbön $(x, y, z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ szerint adhatók meg és ezt a vektort Bloch-vektornak (vagy polarizációs vektornak)



1. ábra. Az állapot reprezentálása a Bloch-gömbön

hívjuk. Vezzesük be az ún. Pauli-operátorokat:

$$\hat{\sigma_I} \equiv \hat{I} \quad \hat{\sigma_x} \equiv \hat{X} \equiv |0\rangle\langle 1| + |1\rangle\langle 0| \quad \hat{\sigma_y} \equiv \hat{Y} \equiv i\left(|1\rangle\langle 0| - |0\rangle\langle 1|\right) \quad \hat{\sigma_z} \equiv \hat{Z} \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$$

A Bloch-vektor koordinátái ezeknek az operátoroknak a várható értékével számolhatók és az explicit összefüggések az (7) alak paramétereivel:

$$x = \langle\hat{\sigma_x}\rangle = 2Re(\bar{\alpha}\beta) \quad y = \langle\hat{\sigma_y}\rangle = 2Im(\bar{\alpha}\beta) \quad z = \langle\hat{\sigma_z}\rangle = |\alpha|^2 - |\beta|^2 \tag{10}$$

Terjesszük ki ezt a reprezentációt kevert állapotokra is. Ehhez vegyük észre, hogy a Pauli-operátorok az 1 qubiten ható unitér operátorok terét kifeszítik. Egy tetszőleges unitér operátor hatása a Bloch-vektor forgatásával írható le; az x-, y- és z-tengelyek körüli forgatások a Pauli-operátorok segítségével könnyen felírhatók [20]. Figyelembe véve (4), (9) és bevezetve a formális $\vec{\hat{\sigma}} = (\hat{\sigma_x}, \hat{\sigma_y}, \hat{\sigma_z},)$ vektort, minden 1 qubites sűrűségoperátor kifejezhető:

$$\hat{\rho} = \frac{1}{2}(\hat{I} + \vec{r} \cdot \vec{\hat{\sigma}}) \tag{11}$$

ahol $\vec{r}$ a Bloch-vektor. A kevert állapotok már a teljes Bloch-gömböt kitöltik ("Bloch-labda"). A Bloch-vektor hossza tehát a kevertség mértékére jellemző: a labda centrumához a maximálisan kevert állapot tartozik, míg $|\vec{r}| = 1$ esetén az állapot tiszta. Megjegyezzük, hogy $|\vec{r}|$ kifejezhető $\hat{\rho}$ sajátértékeivel:

$$|\vec{r}| = 1 - 4\tau_1\tau_2 \tag{12}$$

ahol τ_1, τ_2 $\hat{\rho}$ sajátértékei [23].

Ez a reprezentáció n darab qubit esetén (melyet Fano-alaknak [3] is hívnak)

$$\rho = \frac{1}{N} \sum_{\alpha_1, \cdots, \alpha_n} c_{\alpha_1 \dots \alpha_n} \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_n} \tag{13}$$

alakban írható (az operátorok jelölésekor a kalapot a továbbiakban elhagyjuk), ahol N a normálási faktor: $N = 2^n$. A $c_{\alpha_1 \dots \alpha_n}$ együtthatókat

$$c_{\alpha_1 \dots \alpha_n} = Tr(\sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_n} \rho) \tag{14}$$

módon számolhatjuk. A normálási feltételből ($Tr(\rho) = 1$) következik, hogy $c_{I \dots I} = 1$ Az általánosított Bloch-vektort, mely ρ hermiticitásából következően valós vektor lesz, definiáljuk

$$\vec{b} = \{b_\alpha\}_{\alpha=1,\dots,N^2-1} \qquad b_\alpha \equiv c_{\alpha_1 \dots \alpha_n} \qquad \alpha \equiv \sum_{k=1}^{n} i_k 4^{n-k} \tag{15}$$

módon, ahol $i_k = 1, 2, 3, 4$-t $\alpha_k = x, y, z, I$-nak megfelelően vezettük be. Ez a definíció a Bloch-vektor komponenseinek a rendezésére szolgál és könnyen megérthető például a 2 qubites esetre felírva. Ekkor az $N^2 - 1 = 15$ komponens (15) szerint

$$\vec{b}^T = (b_1, b_2, ..., b_{15}) = (c_{xx}, c_{xy}, c_{xz}, c_{xI}, c_{yx}, c_{yy}, c_{yz}, c_{yI}, c_{zx}, c_{zy}, c_{zz}, c_{zI}, c_{Ix}, c_{Iy}, c_{Iz}) \tag{16}$$

sorrendben követi egymást.

A Bloch-féle reprezentáció a kvantumoptikában és kvantuminformatikában gyakran használatos és mint láttuk, számos előnye van. Az 1 qubites esetben egy szemléletes képet ad, és általánosan vizsgálhatók vele a kevert állapotok. Az állapotot egy valós vektorral, a Bloch-vektorral írhatjuk le, melynek hosszával jellemezhetjük az állapot kevertségét is. A valós vektorokkal való számolás numerikus szempontból is előnyös lehet. Sajnos a több qubites általánosításának azonban kényelmetlenségei is vannak. Már 2 qubitnél sem egyértelmű a valódi állapotok terének a geometriája (ami 1 qubitnél a teljes $\mathbb{R}^3$-beli egységgömb volt) és a sűrűségoperátorok tulajdonságai csak bonyolult összefüggésekkel fejthetők vissza a reprezentációból [4]. Mivel a később vizsgált dinamika garantálja, hogy sűrűségoperátor a transzformáció során sűrűségoperátor marad, ezzel nem kell foglalkoznunk. Egy másik, súlyosabb hátrány lehet, hogy ez a reprezentáció expliciten nem fejezi ki az összefonódottság mértékét, ami pedig a kvantuminformatikában nagy jelentőséggel bír, ezért ezt külön kell számolni.

2.2.3. Schmidt-féle reprezentáció

Természetesen léteznek összefonódottságérzékeny reprezentációk is, melyek általában tiszta állapotokra vonatkoznak. Ilyen például az ún. Hopf-fibrálás, mely topológiai szempontból általánosítja a Bloch-reprezentációt két qubit esetére [21].

Egy másik érdekes és használható leírás a Schmidt-tételt és a Bloch-formalizmust kombinálja és a reprezentáció egyik paramétere expliciten kifejezi az összefonódottság mértékét.

Tétel (Schmidt) *Legyen $|\psi\rangle \in H$, ahol $H = H_A \otimes H_B$, akkor létezik egy olyan ortonormált bázisa H_A-nak ($\{|\varphi_i^A\rangle\}$) és H_B-nek ($\{|\varphi_i^B\rangle\}$), és nemnegatív valós számok $\{p_i\}$, hogy*

$$|\psi\rangle = \sum_i \sqrt{p_i}|\varphi_i^A\rangle\ |\varphi_i^B\rangle \tag{17}$$

Legyen adott egy 2 qubites tiszta állapot. A tételt kihasználva ez mindig felírható [27]

$$|\psi\rangle = e^{-i\beta/2}\cos(\alpha/2)|\mathbf{n}\rangle_1|\mathbf{m}\rangle_2 + e^{i\beta/2}\sin(\alpha/2)|-\mathbf{n}\rangle_1|-\mathbf{m}\rangle_2 \tag{18}$$

alakban, ahol $\mathbf{n}$ és $\mathbf{m}$ az egyes qubitek Bloch-vektora. Az α paraméter ebben a formában expliciten kifejezi az összefonódás mértékét: $\alpha = 0$ és $\alpha = \pi$ szorzatállapotoknál, $\alpha = \pi/2$ teljesen összefonódott állapotoknál áll fenn. A Bloch-gömb analógiájára itt is bevezethetünk egy gömbi paraméterezést az α és β paraméterekkel;ezt Schmidt-gömbnek hívjuk. Legyen $\mathbf{e} = (\sin\alpha\cos\beta, \sin\alpha\sin\beta, \cos\alpha)$. Az ortogonális állapotokra a feltétel így $\langle -\mathbf{e}|\mathbf{e}\rangle$. A két qubites tiszta állapot így egyértelműen jellemezhető az $(\mathbf{n}, \mathbf{m}, \mathbf{e})$ vektorokkal. A továbbiakban ezt a paraméterezést csak a kitekintésben említjük meg.

2.3. Kvantumállapotok közelségének mérőszáma

Kommunikációelméletben gyakran felmerülő probléma két jel vagy jelsorozat összehasonlítása és ennek számszerű jellemzése. Erre alapvető motivációt az ad, hogy transzmittáláskor mindenképp számolnunk kell hibákkal; ezek adódhatnak a tömörítésből, a kommunikációs csatorna zajosságából vagy a vevőkészülék tökéletlenségéből. Az átvitel jóságának definiálásához tehát szükségünk van a jelek kvantitatív összevetésére. Klasszikus információelméletben a téma széleskörűen tárgyalt [5].

Kvantuminformatikai megközelítésben ezzel analógnak tekinthető a kvantumállapotok összehasonlításának problémája. Az erre bevezetett mennyiséget a továbbiakban

F-fel jelöljük és átmeneti valószínűségnek hívjuk. Megjegyezzük, hogy az angol szakirodalomban több kifejezést használnak erre a mennyiségre (*fidelity, transition probability*) és a definíció sem teljesen egységes (összefoglalásért lásd [18]); az utóbbi időben ebben a kontextusban a *fidelity* terjedt el, azonban fordítási szempontok miatt az utóbbit használjuk. Legyenek adottak ρ_1, ρ_2 kvantumállapotok (véges dimenziós Hilbert-térben). Abban a speciális esetben, ha mindekét állapot tiszta, azaz $\rho_1 = |\psi_1\rangle\langle\psi_1|$ és $\rho_2 = |\psi_2\rangle\langle\psi_2|$, F-re egy intuitív definíció adódik a természetes átmeneti valószínűségből:

$$F(\rho_1, \rho_2) = F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|) \equiv |\langle\psi_1|\psi_2\rangle|^2 \tag{19}$$

F-nek tehát azt a valószínűséget választjuk, amellyel összetéveszthetjük a két állapotot, ha végrehajthatunk pontosan egy mérést a rendszeren, mely a két állapot egyikében van preparálva. A kifejezés könnyen általánosítható, ha az egyik állapot kevert (ρ_2):

$$F(\rho_1, \rho_2) = F(|\psi_1\rangle\langle\psi_1|, \rho_2) \equiv \langle\psi_1|\rho_2|\psi_1\rangle \tag{20}$$

mely egyszerűen (19) átlaga az összes olyan tiszta állapotok sokaságára nézve, melynek ρ_2 a sűrűségoperátora. Ennek fizikai interpretációja megegyezik a tiszta állapotok esetében felírt képletével: F annak valószínűsége, hogy ρ_2 állapoton végrehajtva egy mérést $|\psi_1\rangle$ állapotot kapjuk. A kvantuminformatikában legtöbbször (és a dolgozatban kizárólag) elegendően általános a (20) kifejezés, mivel tisztító eljárásoknál a vizsgált - zajoktól és egyéb hibáktól terhelt - állapotot egy adott tiszta állapottal (azzal a célállapottal, amely felé tisztítani akarunk) hasonlítjuk össze. Az teljesség igénye által vezérelve mégis tovább megyünk az általánosításban és bevezetjük a mennyiséget két kevert állapot esetén is. Az eddigieket figyelembe véve az általános átmeneti valószínűségtől követeljük meg az alábbi természetes tulajdonságokat.

A1 $0 \leq F(\rho_1, \rho_2) \leq 1$ és $F(\rho_1, \rho_2) = 1$ akkor és csak akkor, ha $\rho_1 = \rho_2$

A2 $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$

A3 Ha az egyik állapot tiszta, akkor álljon fenn (20)

A4 $F(\rho_1, \rho_2)$ legyen invariáns az állapotok unitér transzformációjára

Vegyük észre, hogy (19) és (20) is $F(\rho_1, \rho_2) = Tr(\rho_1\rho_2)$ alakban írható. Ez a definíció azonban nem tenne eleget A1 tulajdonságnak (vegyük például $\rho_1 = \rho_2 = I/2$: ekkor

$Tr(\rho_1\rho_2) \neq 1)$. Ebben az esetben bonyolultabb definíciót kell bevezetni [11, 29]:

$$F(\rho_1, \rho_2) \equiv \left(Tr \left[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} \right] \right)^2 \tag{21}$$

Belátható, hogy ez már kielégíti az összes kívánt tulajdonságot.

3. Komplex dinamika qubiteken

3.1. A transzformáció ismertetése

A következőkben bemutatjuk azt a qubiteken értelmezett transzformációt, amelyet a későbbiekben vizsgálni fogunk és amely a dolgozat gerincét alkotja.

A kvantummechanika alapvető műveletei - unitér transzformációk és projekciók - lineárisak. A kvantumállapotokkal végzett nemlineáris transzformációk azonban gyakoriak; ez a nemlinearitás a gyakorlatban szelektív operációkkal érhető el, azaz olyanokkal, melyek egyik lépése valamilyen szűrési eljárást tartalmaz. Ezek a transzformációk általában véges valószínűséggel sikertelenek [28].

Vizsgáljunk egy qubitet. Ennek sűrűségmátrixa általánosan

$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \tag{22}$$

írható, ahol természetesen kikötjük, hogy ρ teljesítse a sűrűségmátrix általános tulajdonságait. Tekintsük a következő transzformációt:

$$\rho^{ki} = \mathcal{S}\rho^{be} \qquad \mathcal{S} : \rho_{ij} \to \rho_{ij}^2 \tag{23}$$

amelynek hatása az egy qubites sűrűségmátrixra:

$$\rho^{be} = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \xrightarrow{\mathcal{S}} \rho^{ki} = \begin{pmatrix} (\rho_{11})^2 & (\rho_{12})^2 \\ (\rho_{21})^2 & (\rho_{22})^2 \end{pmatrix} \tag{24}$$

Első megfontolásra a transzformáció egzotikusnak tűnhet, és fizikai megvalósítása is kérdéses; megmutatjuk azonban, hogy ez egyszerű elemek alkalmazásával - melyek a mai technológiai szinten már a laborban is rendelkezésre állnak - realizálható [2]. Látható, hogy a transzformáció nem nyomtartó; ez pusztán arra utal, hogy egyes bitek elvesznek a művelet során. Az újranormálás minden további nélkül megtehető.

A megvalósításhoz először is tegyük fel, hogy egy adott ρ^{be} állapotról rendelkezésünkre áll egy tökéletes másolat. Az első lépés a qubitek párba állítása:

$$\rho^{be} \longrightarrow \rho^{be} \otimes \rho^{be} \tag{25}$$

Ez nem nehéz feladat, hiszen fizikailag nem történik semmi. A második lépés már nehezebben megvalósítható, az ún. CNOT (*controlled-NOT*) kapu vagy másnéven kvantum-XOR kapu. Ez egy qubitpárokon ható operátor, mely megcseréli a második qubitet (*target bit*, mi a cél bit kifejezést használjuk), ha az első qubit (*control bit* vagy *source bit*, a dolgozatban a kontroll bit fog szerepelni) 1 és úgy hagyja az állapotot, ha az első qubit 0, azaz:

$$|00\rangle \xrightarrow{XOR} |00\rangle, \quad |01\rangle \xrightarrow{XOR} |01\rangle, \quad |10\rangle \xrightarrow{XOR} |11\rangle, \quad |11\rangle \xrightarrow{XOR} |10\rangle \tag{26}$$

vagy mátrixalakban írva

$$\mathbb{U}_{XOR} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \sigma_x & 0 \\ 0 & \mathbf{1} \end{pmatrix} \tag{27}$$

ahol σ_x a már bevezetett Pauli-mátrix, $\mathbf{1}$ a 2×2-es egységmátrix. Megjegyezzük, hogy a XOR kapu a kvantuminformatikában alapvető jelentőségű (bővebben lásd 4.1. fejezet) és fizikailag is implementálható. A harmadik lépés megint csak egyszerű: mérjük meg a második qubitet, és tartsuk meg a párt akkor és csak akkor, ha az eredmény 0 (tehát véges valószínűsége van annak, hogy a qubitpárt ki kell dobni és a transzformáció sikertelen). Az operáció a kontroll bitet $\rho^{be}_{kontroll} \longrightarrow \rho^{ki}_{kontroll}$ transzformálja, míg a cél bit mindig a $|0\rangle$ állapotban marad:

$$\rho^{be}_{cél} \longrightarrow \rho^{ki}_{cél} = |0\rangle\langle 0| = \mathbb{P}_0$$

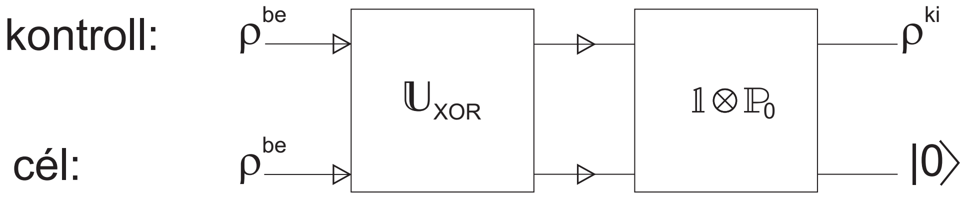
Végeredményben a transzformáció kompakt formában

$$(\mathbf{1} \otimes \mathbb{P}_0(\mathbb{U}_{XOR}(\rho^{be} \otimes \rho^{be})\mathbb{U}^{\dagger}_{XOR})\mathbf{1} \otimes \mathbb{P}_0) = \rho^{ki} \otimes \mathbb{P}_0 \tag{28}$$

írható, ahol ρ^{ki} valóban a (24)-nak megfelelő sűrűségmátrix. A 2. ábra a transzformáció sematikus elrendezését mutatja.

Ez a transzformáció a vizsgált dinamika első lépése, beleértve a normálást is (azaz $\rho^{ki} = \mathcal{S}\rho^{be} \qquad \mathcal{S} : \rho_{ij} \to N\rho^2_{ij}$, ahol $N = 1/\sum \rho^2_{ii}$). A dinamika második lépését egy lokális unitér transzformációként értelmezzük, melyet $U \in SU(2)$-nek választunk

$$U = \begin{pmatrix} \cos x & \sin x e^{i\varphi} \\ -\sin x e^{-i\varphi} & \cos x \end{pmatrix} \tag{29}$$



2. ábra. Az $\mathcal{S}$ transzformáció lépései. Két másolata ugyanazon qubitállapotnak először egy unitér kapun megy keresztül (egyéb kapukat is választhatunk, mint az $\mathbb{U}_{XOR}$), majd egy szűrőn. A szűrő kapu tartalmazza a mérést. A kontroll bit $\rho^{be}_{kontroll}$ a folyamat végén az új $\rho^{ki}_{kontroll}$ állapotban lesz, míg a cél bit mindig a $|0\rangle$ állapotban.

paraméterezéssel. Ez egy forgatást ír le a qubitek Hilbert-terén. A sűrűségmátrix transzformációja ebben a lépésben tehát:

$$\mathcal{R}\rho = U\rho U^\dagger \tag{30}$$

A teljes dinamika egy lépését az előbb ismertetett $\mathcal{S}$ és $\mathcal{R}$ transzformációk egymásutánjaént értelmezzük:

$$\rho' = \mathcal{F}\rho = \mathcal{R}\mathcal{S}\rho \tag{31}$$

Ennek a transzformációnak az iteratív alkalmazása tehát a qubiteknek egy diszkrét, feltételes dinamikájához vezet. A qubitsokaság mérete exponenciálisan csökken az iteráció során.

3.2. 1 qubites tiszta állapot vizsgálata

A továbbiakban rátérünk a bevezetett $\mathcal{F}$ transzformáció részletes vizsgálatára 1 qubites tiszta kezdőállapot esetén. Használjuk a 2.2-ben bevezetett Riemann-féle reprezentációt, azaz írjuk fel a kezdőállapotot (a sztenderd komputációs bázisban dolgozva)

$$|\psi\rangle = N\left(z|0\rangle + |1\rangle\right) = N\begin{pmatrix} z \\ 1 \end{pmatrix} \qquad z \in \hat{C} \quad N = (1+|z|^2)^{-1/2} \tag{32}$$

alakban. Erre hattatva $\mathcal{F}$-et:

$$|\psi\rangle \xrightarrow{\mathcal{S}} N'\begin{pmatrix} z^2 \\ 1 \end{pmatrix} \xrightarrow{\mathcal{R}} N'\begin{pmatrix} \cos x z^2 + \sin x \cdot e^{i\varphi} \\ \cos x - \sin x \cdot e^{-i\varphi} z^2 \end{pmatrix} = N'\begin{pmatrix} \frac{z^2+p}{1-p^* z^2} \\ 1 \end{pmatrix} \tag{33}$$

ahol bevezettük a $p = \tan x \cdot e^{i\varphi}$ jelölést. A transzformáció tehát tiszta állapotot tiszta állapotba visz át, és az állapotot jellemző z paraméter

$$z \to F_p(z) = \frac{z^2 + p}{1 - p^* z^2} \tag{34}$$

szerint transzformálódik.

Amit kaptunk, az egy $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$ nemlineáris leképezés, egy jellemző komplex paraméterrel. $F_p(z)$ másodrendű racionális törtfüggvény; ilyen típusú leképezéseknek a részletesebb vizsgálatát P. J. L. Fatou végezte el először az 1900-as évek elején, aki speciálisan a $z \to z^2/(z^2+2)$ leképezéssel foglalkozott [8]. Azóta a téma kiterjedt irodalommal rendelkezik, melyhez nagyban hozzájárult G. Julia és B. Mandelbrot munkássága, akik megmutatták, hogy már a legegyszerűbb nemlineáris komplex leképezések is gazdag struktúrát mutatnak (gondoljunk csak a Mandelbrot-halmazra, mely a $z \to z^2 + p$ egyszerűnek tűnő esettel van kapcsolatban). A legfontosabb definíciókat, tételeket és a leképezés tulajdonságait az alábbiakban ismertetjük. A komplex leképezésekről átfogó irodalom [16, 19].

Definíció *Legyen S egy Riemann-felület (egy dimenziós komplex sokaság), $f : S \to S$ egy (nem konstans) holomorf leképezés. Jelölje $f^{\circ n}(z)$ a leképezés n-szeri elvégzését. Legyen adott egy $z_0 \in S$ pont. Azt mondjuk, hogy z_0 **reguláris pont**, ha létezik U környezete, hogy $\{f^{\circ n}(z_0)\}_{n=1}^{\infty}$ leszorítva U-ra normális családot képez.*

A normális család egyszerűen szólva azt jelenti, hogy az iteráció konvergenciatulajdonságaira (konvergál-e, hova konvergál, konvergencia gyorsasága) nézve minden pontja hasonlóan viselkedik (ennek precíz definiálása messzire vinne, lásd [16]).

Definíció *A reguláris pontok összességét f **Fatou-halmazának** (F_f) hívjuk, komplementerét pedig **Julia-halmaznak** (J_f).*

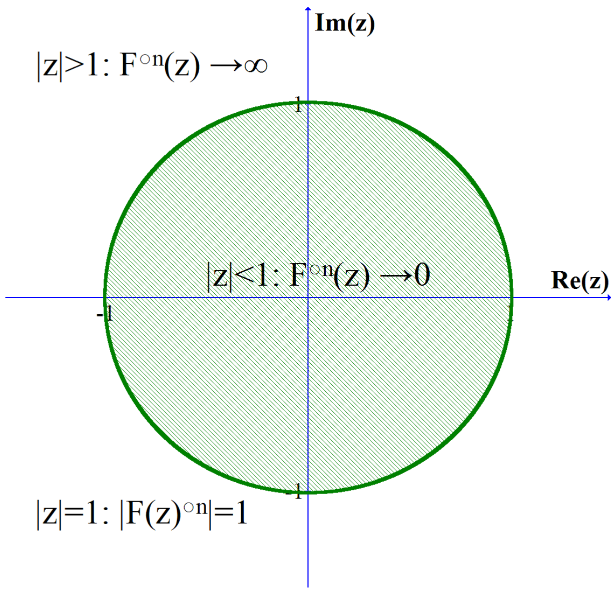
Belátható, hogy ha f legalább másodrendű racionális leképezés, akkor J_f nemüres és izolált pontja sincs. Az is megmutatható, hogy ha létezik belső pontja J_f-nek, akkor J_f az egész Riemann-gömböt kitölti. Egy további érdekes tétel az J_f összefüggőségére vonatkozik [17].

1. Tétel Ha f egy racionális, kvadratikus leképezés, akkor J_f vagy összekötött vagy teljesen szétesett; ez utóbbi pedig akkor és csak akkor, ha (a fogalmakat később definiáljuk)

a) a kritikus pályák egy közös vonzó ciklushoz konvergálnak, vagy

b) a kritikus pályák közös - kettes multiplicitású - ciklushoz konvergálnak, de egyik kritikus pálya sem éri el ezt a ciklust.

Vizsgáljuk meg azt az egyszerű esetet, amikor (34)-ban $p = 0$, azaz $F_p(z) = z^2$. Ez az eset azt jelenti, hogy nem alkalmazunk forgatást, a transzformáció csak a sűrűségmátrix elemeinek a négyzetre emelése. Könnyen látható, hogy ez az iteráció végtelenhez tart $|z_0| > 1$ esetén és 0-hoz $|z_0| < 1$ esetén. A Fatou-halmaz tehát a teljes $\hat{\mathbb{C}}$ kivéve a $|z| = 1$ pontokat, melyek a Julia-halmazt alkotják (mivel bármely pontnak létezik olyan környezete, amely környezeten belül találunk végtelenhez és 0-hoz konvergáló pontokat is). A Julia-halmaz ebben az esetben egy sima és összefüggő görbe, nevezetesen az egységkör az állapotot reprezentáló kiterjesztett komplex számsíkon (3. ábra). Fizikailag ez azt jelenti, hogy a qubit minden esetben az egyik bázisállapothoz fog tartani, kivéve, ha a kiindulás a teljesen kevert állapot volt. Ez utóbbi esetben a relatív fázis fog érdekes dinamikát követni [13].



3. ábra. A $F_p(z)$ Julia-halmazának szemléltetése abban az esetben, ha $p = 0$. A Julia-halmaz az egységkör.

Tekintsük át a periodikus pályákkal (vagy más néven ciklusokkal) és ezek stabilitásával kapcsolatos definíciókat. Periodikus pálya alatt a

$$z_0 \rightarrow F_p(z_0) = z_1 \rightarrow F_p^{\circ 2}(z_0) = z_2 \rightarrow \cdots \rightarrow F_p^{\circ(n-1)}(z_0) = z_{n-1} \rightarrow F_p^{\circ n}(z_0) = z_n = z_0$$

értjük, ahol tegyük fel, hogy $z_i \neq z_j$ ha $i \neq j$. Ekkor az $n \geq 1$ számot periódusnak hívjuk. Ezeket a pályákat a $F_p^{\circ n}(z) = z$ (n-ed rendű) sajátértékegyenlet megoldásával kaphatjuk meg, mely esetünkben (tekintve, hogy a leképezésünk másodrendű) $2^n + 1$ rendű egyenlet megoldását kívánja.

Definíció *Legyen adott egy pediodikus pálya n periódussal. Ekkor a*

$$\lambda = f'(z_1) \cdot f'(z_2) \cdots f'(z_n)$$

számot a pálya ***sajátértékének*** *nevezünk, ahol a vessző a deriválást jelöli.*

A sajátérték egy jóldefiniált komplex szám és segítségével a pálya stabilitás szempontjából négy kategóriába sorolható.

Definíció *Legyen adott egy periodikus pálya λ sajátértékkel. Ha $|\lambda| \leq 1$, akkor a pálya* ***vonzó****, $|\lambda| \geq 1$ esetben* ***taszító****, $|\lambda| = 1$ esetben* ***semleges****. $\lambda = 0$ esetben a pályát* ***szupervonzónak*** *hívjuk. Azokat a neutrális pályákat, amelyre λ egységgyök (továbbá az iteráció egyetlen tagja sem az identitás),* ***parabolikus*** *pályáknak nevezzük.*

Belátható, hogy minden vonzó ciklus a Fatou-halmaz része (sőt, a ciklusok teljes vonzási tartománya is, kivéve a határokat) és minden taszító ciklus a Julia-halmaz része. Ha egy racionális, komplex leképezés rendje d, akkor legfeljebb $d-2$ ciklusa lehet, ami nem taszító [26]. Azaz esetünkben 2 olyan ciklus lehetséges, mely vonzó vagy semleges (bármely p-re).

Definíció *Azokat a pontokat, melyre $F'(z_c) = 0$,* ***kritikus pontoknak*** *hívjuk.*

Esetünkben a kritikus pontok:

$$F_p'(z) = \frac{2z(1+|p|^2)}{(1-p^*z^2)^2} \stackrel{!}{=} 0 \longrightarrow z_{c1} = 0 \quad z_{c2} = \infty$$

A kritikus pontok tehát p-től függetlenek (feltéve, hogy $p \neq 0$). Ezek a pontok és pályájuk (kritikus pályák) a leképezésről sok mindent elárulnak. Belátható, hogy ha minden kritikus pálya véges (azaz periodikus; az ilyen leképezéseket p.c.f. [*post-critically finite*] vagy Thurston-leképezéseknek hívjuk), akkor f minden periodikus pályája vagy taszító, vagy szupervonzó. Továbbá a kritikus pontok iterálásával az összes vonzó ciklus megtalálható [17].

Definíció *Legyen adott* $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$, $d \geq 2$ *racionális leképezés. Ha* f *minden kritikus pontja vonzó ciklushoz konvergál, akkor* f ***hiperbolikus*** *leképezés.*

Megjegyezzük, hogy a hiperbolikus leképezés általánosan sokkal összetettebb fogalom és az előbbi definíció valójában tételként látható be a fenti tulajdonságokat teljesítő f-re.

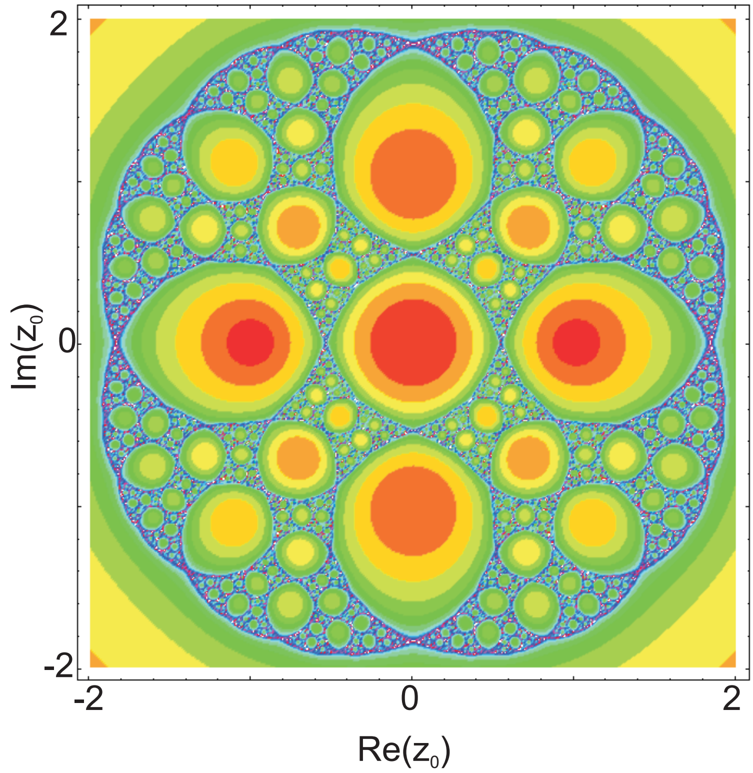
Az ismertetett definíciók és állítások tükrében tekintsük a $p = 1$ esetet. Ez az $\mathcal{R}$ transzformációra nézve egy $\pi/4$ szögű forgatást jelent a qubitek terében, például a bázisállapotokat a $1/\sqrt{2}(|0\rangle \pm |1\rangle)$ egyenlő szuperpozícióba viszi át. A leképezés tehát

$$z \to F_p(z) = \frac{z^2 + 1}{1 - z^2} \tag{35}$$

Egy periodikus ciklust észrevehetünk: $\{-1, \infty\}$. Az egyik kritikus pont z_{c2} ennek része. Kövessük z_{c1} pályáját: $0 \to 1 \to \infty$, azaz ugyanabba a periodikus ciklusba ment. Ebből arra következtethetünk, hogy

1. az egyetlen stabil ciklus $\{-1, \infty\}$
2. a leképezés hiperbolikus
3. a Julia-halmaz összekötött (mivel az 1. tétel b) része sérül).

A Julia-halmazok bonyolult szerkezetét numerikus szimulációval szemléltetjük. Ezek számolására legalább kvadratikus leképezések esetére általánosan nincsen algoritmus. A program a stabil ciklushoz való konvergencia gyorsaságát vizsgálja különböző z_0 kezdőállapotok esetén. A 4. ábrához a program részletesebb adatai: $Re(z_0) \in [-2, 2]$, $Im(z_0) \in [-2, 2]$, felosztás egysége: $0,01$. Egy adott bemeneti adatot addig iterál, amíg eléri a 100 iterációt vagy $|z| > 7$. A fraktálszerű szerkezet mutatja a kaotikus jelleget: a konvergenciatulajdonság tetszőlegesen kis skálán megváltozhat. A numerikus szimulációból látható a Julia-halmaz összekötöttsége is.

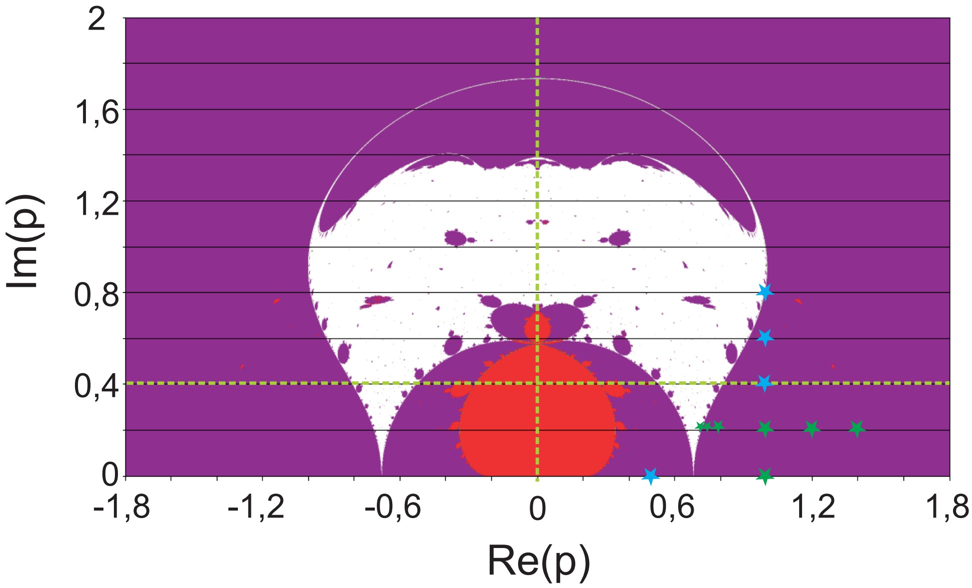


4. ábra. A Julia-halmaz szemléltetése $p = 1$ esetén. A konvergencia a piros tartományokban a leggyorsabb, a zöld tartományokban a leglassabb (a sárga közepes gyorsaságot jelent). A kék tartományokon (a programban megadott kritérium szerint) nem konvergál az iteráció. A Julia-halmaz teljesen összekötött. Egy stabil ciklus van: $\{-1, \infty\}$

Láttuk tehát, hogy (34) leképezés legfeljebb két stabil ciklussal rendelkezhet. A 5. ábrán a stabil ciklusok száma látható a p paramétertérben, melyeket a kritikus pályák segítségével, numerikusan határozhatunk meg.

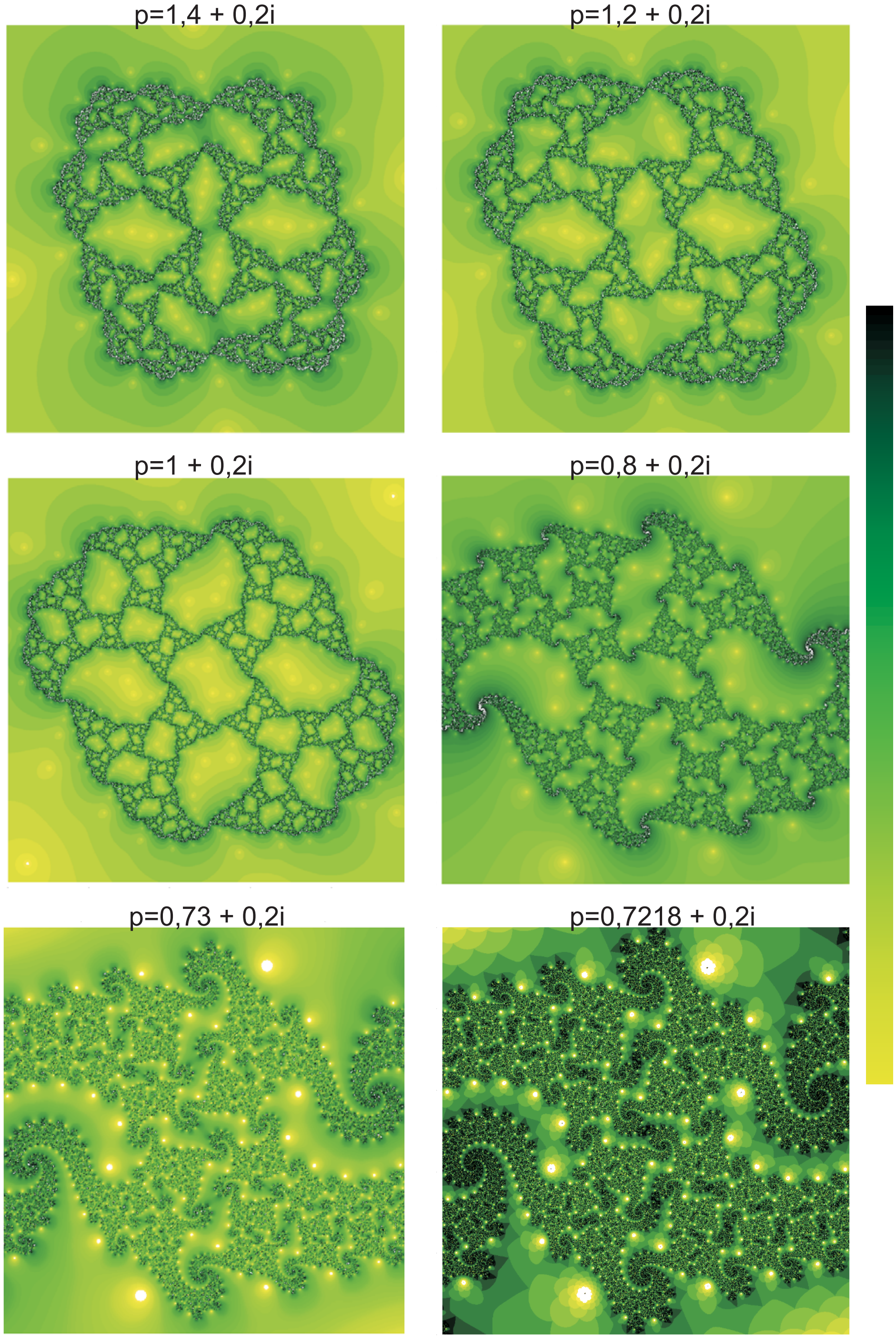
A 6. ábrasorozaton különböző p paraméterek mellett vizsgáljuk a Julia-halmazt (feltüntettük a színskálát is, melyet a továbbiakban használunk. A színskála alja gyors konvergenciát, a teteje lassú konvergenciát jelent). Látható, hogy $p = 1,4 + 0,2i$ és $p = 0,73 + 0,2i$ között a Julia-halmaz szerkezete kvalitatíven nem változik; ezután azonban már a paraméterek kis változtatására is jelentős változást tapasztalunk (lásd $p = 0,7218 + 0,2i$ eset). Ha a paraméter valós részét tovább csökkentjük, belépünk a kaotikus, stabil ciklussal nem rendelkező tartományba (vö. 5. ábra). A Julia-halmaz ebben az esetben már a teljes Riemann-gömböt kitölti, a szimuláció egy teljesen fekete képet eredménezne. További négy képet láthatunk az A függelékben. A $p = 1 + 0,6i$

(17. ábra) hasonlít a $p = 1$ esethez, a Julia-halmaz "deformációja" figyelhető meg. Ezen paraméterek mellett egy stabil ciklus van, mely hossza kettő. $p = 1 + 0,8i$-nél (18. ábra) ismét a kaotikus tartomány széléhez érkezünk. A 19. ábrán már az előzőektől kvalitatíven különböző képet láthatunk: a Julia-halmaz teljesen szétesett. Továbbra is egy stabil ciklus van, melynek hossza egy.

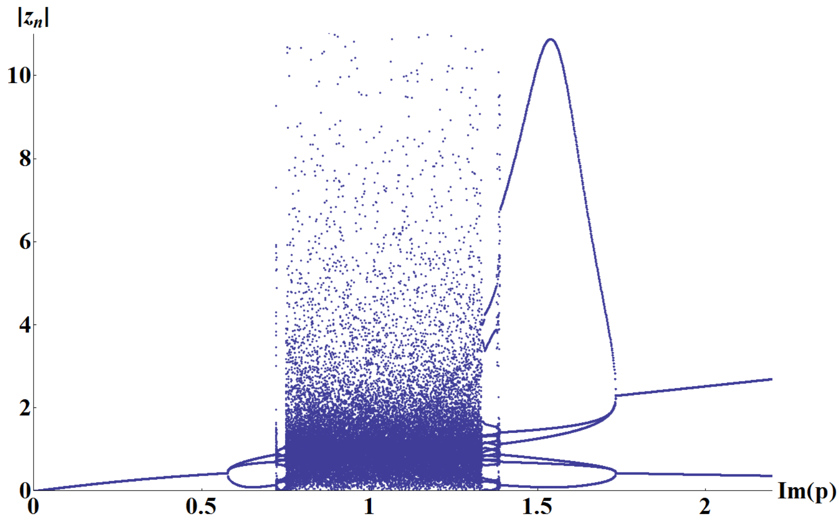


5. ábra. (34) leképezés stabil ciklusainak numerikus vizsgálata a p paraméter függvényében. A piros tartományban kettő, a lila tartományban egy, míg a fehér tartományban nulla a stabil ciklusok száma. A csillaggal jelölt p értékeknél a Julia-halmazt numerikusan szemléltettük (a kék csillaggal jelölt pontokban számolt ábrák az A függelékben találhatóak). A zöld szaggatott vonal mentén további numerikus vizsgálatot végeztünk (7. és 8. ábra).

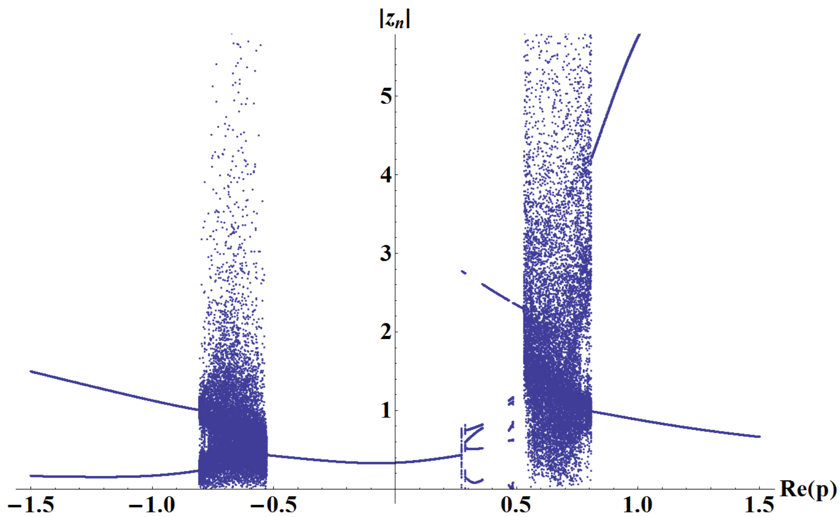
A 7. és 8. ábrán a p paramétert változtatva vizsgáljuk a ciklusokat és ellenőrizzük a káosz jelenlétét a 5. ábrán látható fehér tartományokban, azaz ahol nincs stabil ciklus. Ezt úgy tettük meg, hogy a $z_{c1} = 0$ kritikus pontból elvégeztünk 10000 iterációt, majd a következő 50 iterációs lépést ábrázoltuk. A p paramétert a 5. ábrán berajzolt szaggatott vonalak mentén változtattuk.



6. ábra. Magyarázatért lásd előző oldal.



7. ábra. A (7) leképezés numerikus vizsgálata. A $z_{c1} = 0$ kritikus pontból adott, tisztán képzetes p paraméter mellett (azaz a 5. ábrán látható függőleges szaggatott zöld vonal mentén) elvégeztünk 10000 iterációt, majd a következő 50 iterációs lépést tüntettük fel (az egyszerűség kedvéért z abszolút értéke van ábrázolva). Jól kivehetőek a stabil ciklusok és a kaotikus tartomány: $0,75 \lessapprox Im(p) \lessapprox 1,4$; itt nincs stabil ciklus.



8. ábra. A 8. ábrához hasonló szimuláció; a p paraméter valós részét változtattuk $[-1,5,\ 1,5]$ tartományban, állandó $Im(p) = 0,4$ mellett (a 5. ábrán látható vízszintes szaggatott zöld vonal mentén).

3.3. 1 qubites kevert állapot vizsgálata

A kevert állapotokat Bloch-reprezentációban fogjuk vizsgálni. Világos, hogy a kevert állapotok tere speciális esetként magában foglalja a tiszta állapotokat is. Legyen tehát adott az általános 1 qubites sűrűségmátrix (22)-nek megfelelően és ezt fejtsük ki (11) szerint, mely expliciten kiírva:

$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} = \frac{1}{2}(I + c_x\sigma_x + c_y\sigma_y + c_z\sigma_z) = \frac{1}{2}\begin{pmatrix} 1+c_z & c_x - ic_y \\ c_x + ic_y & 1-c_z \end{pmatrix} \tag{36}$$

ahol (c_x, c_y, c_z) a Bloch-vektor Descartes-koordinátái. Végezzük el először $\mathcal{S}$ transzformációt. Ekkor az új Bloch-koordinátákat megkaphatjuk (14) szerint vagy a következő egyenletrendszer megoldásával:

$$\frac{1}{4\left((1+c_z)^2 + (1-c_z)^2\right)}\begin{pmatrix} (1+c_z)^2 & (c_x - ic_y)^2 \\ (c_x + ic_y)^2 & (1-c_z)^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+c'_z & c'_x - ic'_y \\ c'_x + ic'_y & 1-c'_z \end{pmatrix}$$

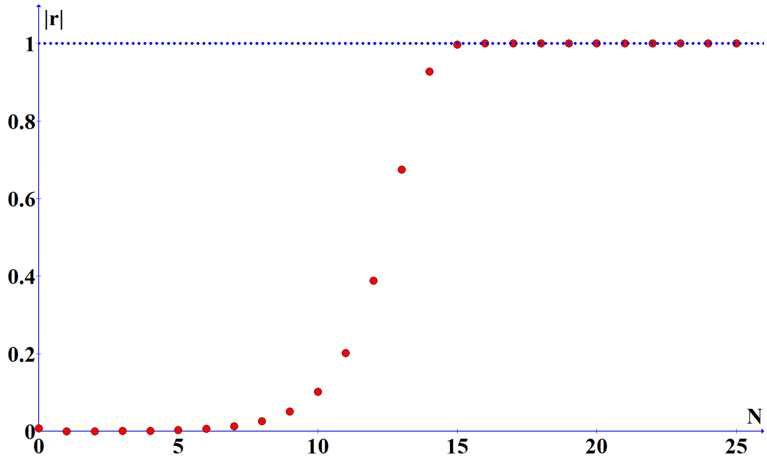
ahol (c'_x, c'_y, c'_z) az új (transzformáció utáni) Bloch-vektor koordinátái. Ezt megoldva az $\mathcal{S}$ transzformáció a Bloch-vektor koordinátáit

$$c_x \longrightarrow \frac{c_x^2 - c_y^2}{1+c_z^2} \qquad c_y \longrightarrow \frac{2c_xc_y}{1+c_z^2} \qquad c_z \longrightarrow \frac{2c_z}{1+c_z^2} \tag{37}$$

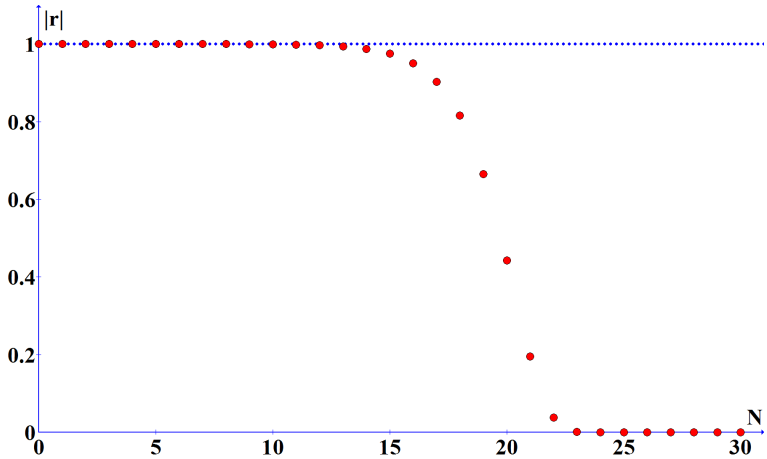
módon transzformálja. Az, hogy $\mathcal{S}$ tiszta állapotot tiszta állapotba visz át, elemi algebrával innen is könnyen ellenőrizhető (és ezzel (37) megoldása is): ha a kiinduló állapot teljesíti a $c_x^2 + c_y^2 + c_z^2 = 1$ feltételt (azaz a Bloch-gömb felszínén vagyunk), akkor a transzformált koordináták is teljesítik ezt. (37)-nek 4 fixpontja van: $(0,0,1)$; $(0,0,-1)$; $(1,0,0)$; $(0,0,0)$; az utóbbi kettő csak az (x,y) síkon stabil. Észrevehetjük azt is, hogy c_z a transzformáció során nem keveredik a többi komponenssel. Ennek az a magyarázata, hogy csak a σ_z mátrix tartalmaz diagonális elemeket. A következő táblázat összefoglalja (37) tulajdonságait, melyeket egyszerű analítikus megfontolásokból kaphatunk.

Fixpont	Stabilitás	Konvergenciaintervallum
$(0,0,1)$	stabil	$\forall c_x, c_y$; $c_z \in (0,1]$
$(0,0,-1)$	stabil	$\forall c_x, c_y$; $c_z \in [-1,0)$
$(1,0,0)$	instabil	$c_x, c_y = \pm 1$; $c_z = 0$
$(0,0,0)$	instabil	$c_x, c_y \in (-1,1)$; $c_z = 0$

Látható, hogy az állapot az (x, y) síkot kivéve mindig bekonvergál a $(0, 0, 1)$ és $(0, 0, -1)$ pontok valamelyikébe, melyek a $|0\rangle$ és $|1\rangle$ bázisállapotoknak felelnek meg. A Bloch-gömb középpontja (a tökéletesen kevert állapot) szintén fixpont, de instabil. A 9. és 10. ábrák két kezdőállapotból mutatják a Bloch-vektor hosszának változását az iteráció során.



9. ábra. A (37) transzformáció hatása a Bloch-vektor hosszára. Az x tengelyen az iterációk számát ábrázoltuk. A kezdeti állapot koordinátái: $c_x = 0,05$ $c_y = 0,05$ $c_z = 0,001$, így a kezdeti hossz $|r_0| = 0,0707$. Az állapot bekonvergál a $|1\rangle$ bázisállapotba.



10. ábra. A 9. ábrához hasonló numerikus vizsgálat. A kezdeti állapot koordinátái: $c_x = 0,799999$ $c_y = 0,6$ $c_z = 0$, így a kezdeti hossz $|r_0| = 0,999999$. Az állapot bekonvergál a tökéletesen kevert állapotba, mivel a kiinduló állapotot az (x, y) síkban vettük.

Vegyük hozzá a transzformációhoz az $U \in SU(2)$ forgatást is, (29) paraméterezéssel. Ekkor a kezdeti sűrűségoperátor transzformációja (30) és (31) szerint $\rho \xrightarrow{\mathcal{S}} \rho' \xrightarrow{\mathcal{R}} U\rho' U^\dagger$, a Bloch-vektor komponenseinek transzformációja pedig (14) összefüggést használva

$$c_x \to \Big(\left(\cos^2 x - \sin^2 x \cos 2\varphi\right)\left(c_x^2 - c_y^2\right) + 2\sin 2\varphi \sin^2(x) c_x c_y - 2\sin 2x \cos(\varphi) c_z\Big)$$

$$c_y \to \left(-\sin^2 x \sin 2\varphi \left(c_x^2 - c_y^2\right) + \left(\cos^2 x - 2\sin^2 x \cos\varphi\right) c_x c_y + 2\sin 2x \sin(\varphi) c_z\right)$$

$$c_z \to \Big(2\cos(2x)c_z + \sin(2x)\left(\cos\varphi\left(c_x^2 - c_y^2\right) - 2\sin(\varphi)c_x c_y\right)\Big)$$

Ezzel megkaptuk a (34) transzformáció kevert állapotokra történő általánosítását. Vizsgáljunk egy speciális esetet. Legyen $x = \pi/4$ és $\varphi = 0$, ez a korábban bevezetett $p = 1$-nek felel meg. Ekkor a komponensek transzformációja

$$c_x \longrightarrow -\frac{2c_z}{1+c_z^2} \qquad c_y \longrightarrow \frac{2c_x c_y}{1+c_z^2} \qquad c_z \longrightarrow -\frac{c_x^2 - c_y^2}{1+c_z^2} \tag{38}$$

alakra egyszerűsödik, ami nagyon hasonlít (37)-hoz, azonban a komponensek mindegyike keveredik egymással. Egyértelmű, hogy a kevert állapotok terében is tapasztalnunk kell azokat a dinamikai tulajdonságokat, amelyeket a tiszta állapotoknál láttunk. Ennek numerikus vizsgálatára egy lehetőség, hogy adott Bloch-sugárnál (azaz azonos mértékben kevert állapotoknál) vizsgáljuk a konvergenciatulajdonságokat. Ebben az irányban kiterjedtebb vizsgálatot a jövőben szeretnénk megvalósítani.

3.4. 2 qubites eset

Az egy qubites eset alkalmas volt arra, hogy rigorózusan, analitikus eszközökkel is bemutassuk a komplex káosz jelenlétét és tulajdonságait. Az egy tiszta qubit esetében a Riemann-gömb egy pontjával tudtuk jellemezni az állapotot, tehát a (31) transzformáció egy lépése egy $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$ leképezéssel volt megadható. A kevert qubitre a Bloch-reprezentációt használtuk, mely három valós számmal írja le az állapotot, így a transzformációt egy $\mathbb{R}^3 \to \mathbb{R}^3$ leképezés jellemezte. A továbbiakban a két qubites esettel foglalkozunk.

3.4.1. A transzformáció általánosítása 2 qubitre

Először általánosítsuk a (31) transzformációt két qubit esetére; ezek lehetnek összefondóva és kevert állapotban, azaz általánosan egy 4×4-es sűrűségmátrix írja le az állapotot. A szemléletesség kedvéért tegyük fel, hogy minden qubit párt két (különböző irányban kirepülő) részecske hordoz. Az egyik irányban kirepülő spint Alice, a másik irányban kirepülőt Bob manipulálhatja. Az $\mathcal{S}$ továbbra is - egy előírt bázisban dolgozva - a sűrűségmátrix elemeinek a négyzetre emelése lesz, melyet ebben az esetben úgy valósítunk meg, hogy a (28) operációit Alice és Bob külön-külön elvégzi a saját spinjén. Ez kompakt formában

$$(\mathbf{1}\otimes\mathbb{P}_0)_A\,(\mathbf{1}\otimes\mathbb{P}_0)_B\,\mathbb{U}_A\mathbb{U}_B(\rho^{be}\otimes\rho^{be})\mathbb{U}_B^\dagger\mathbb{U}_A^\dagger\,(\mathbf{1}\otimes\mathbb{P}_0)_B\,(\mathbf{1}\otimes\mathbb{P}_0)_A=\rho^{ki}\otimes\mathbb{P}_{00} \qquad (39)$$

írható, ahol $\mathbb{U}$ a (27)-ben bevezetett XOR kapu, az A, B alsó indexek pedig azt jelzik, hogy melyik spinre hat az adott operáció. Ez nagyon hasonló a [2]-ban már vizsgált transzformációhoz, ahol a XOR kapu helyett a

$$\mathbb{U}_A=\begin{pmatrix}-i\sigma_y & 0\\ 0 & \mathbf{1}\end{pmatrix}\quad \mathbb{U}_B=\begin{pmatrix}i\sigma_y & 0\\ 0 & \mathbf{1}\end{pmatrix} \qquad (40)$$

kapukat használták.

A lokális unitér transzformációt válasszuk $\mathcal{R}=\mathcal{R}_1\otimes\mathcal{R}_2 \qquad \mathcal{R}_1,\mathcal{R}_2\in SU(2)$ módon; a két qubitet tehát Alice és Bob bilaterálisan forgatja, továbbra is (29) szerinti paraméterezéssel:

$$U_i=\begin{pmatrix}\cos x_i & \sin x_i e^{i\varphi_i}\\ -\sin x_i e^{-i\varphi_i} & \cos x_i\end{pmatrix}\quad x_i,\varphi_i\in\mathbb{R}\quad i=\{1,2\} \qquad (41)$$

Így a transzformáció paramétertartománya már $\mathbb{R}^4$ teret feszíti ki, a bemenet pedig egy tetszőleges 4 dimenziós (az feltételeket teljesítő) sűrűségmátrix lehet.

3.4.2. Bloch-formalizmus 2 qubitre és alkalmazás állapottisztításra

Általános esetben a teljes paramétertartomány feltérképezése nehéz feladat. Ha a Bloch-formalizmust használjuk, akkor az állapotot egy $\mathbb{R}^{15}$ vektor írja le. Jelölje a vektor komponenseit $\{c_\alpha\}_{\alpha=1,\dots,15}$ (16)-nek megfelelően és fejtsük ki a két qubites sűrűségmátrixot (13) szerint. Elvégezve az $\mathcal{S}$ transzormációt, a 15 komponens

$$c_{xx}\to N(c_{xx}^2-c_{xy}^2-c_{yx}^2+c_{yy}^2)\;\; c_{xy}\to 2N(c_{xx}c_{xy}-c_{yx}c_{yy})\;\; c_{xz}\to 2N(c_{xI}c_{xz}-c_{yI}c_{yz})$$

$$c_{xI}\to N(c_{xI}^2+c_{xz}^2-c_{yI}^2-c_{yz}^2)\;\; c_{yx}\to 2N(c_{xx}c_{yx}-8c_{xy}c_{yy})\;\; c_{yy}\to 2N(c_{xy}c_{yx}+c_{xx}c_{yy})$$

$$c_{yz} \to 2N(c_{xz}c_{yI} + c_{xI}c_{yz}) \;\; c_{yI} \to 2N(c_{xI}c_{yI} + c_{xz}c_{yz}) \;\; c_{zx} \to 2N(c_{Ix}c_{zx} - c_{Iy}c_{zy})$$

$$c_{zy} \to 2N(c_{Iy}c_{zx} + c_{Ix}c_{zy}) \;\; c_{zz} \to 2N(c_{Iz}c_{zI} + c_{zz}) \;\; c_{zI} \to 2N(c_{zI} + c_{Iz}c_{zz})$$

$$c_{Ix} \to N(c_{Ix}^2 - c_{Iy}^2 + c_{zx}^2 - c_{zy}^2) \;\; c_{Iy} \to 2N(c_{Ix}c_{Iy} + c_{zx}c_{zy}) \;\; c_{Iz} \to 2N(c_{Iz} + c_{zI}c_{z}z)$$

módon transzformálódik, ahol $N = \frac{1}{4}(\sum_{i=1}^{4} \rho_{ii}^{out})^{-1} = (1 + c_{Iz}^2 + c_{zI}^2 + c_z z^2)^{-1}$ és természetesen $c_{II} = 1$. Ha ehhez még hosszávesszük a lokális unitér transzformációt (41) szerint, akkor általánosan nagyon bonyolult alakot kapunk. Ennek a részletesebb analitikus kidolgozását (speciális paraméterek esetén való számolás, más reprezentációk bevezetése) a jövőben szeretnénk megvalósítani. A Schmidt-alak alkalmasnak tűnik a 2 qubites tiszta eset dinamikájának a jellemzésére.

A továbbiakban a praktikus szempontokat fogjuk szem előtt tartani, és annak a vizsgálatára szorítkozunk, hogy hogyan alkalmazható a transzformáció állapottisztításra.

A célunk tehát, hogy ha az ún. Bell-állapotokat, melyek definíciója

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{42a}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{42b}$$

írható (a Bell-állapotok felé való tisztítás motivációjáról lásd a B függeléket) valamilyen zaj, perturbáció éri, akkor a transzformáció segítségével ezeket visszaállítsuk az eredeti, tiszta állapotba. Válasszuk a (41) paramétereit $\varphi_1 = \varphi_2 = \pi/2$ és $x_1 = x_2 = \pi/4$ értékeknek. Vizsgáljuk $|\Psi^+\rangle$ Bell-állapotot, melynek sűrűségmátrixa

$$\rho_{|\Psi^+\rangle} = |\Psi^+\rangle\langle\Psi^+| = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{43}$$

írható. Könnyen látható, hogy a φ, x paraméterekkel $|\Psi^+\rangle$ egy másodrendű ciklus része: $|\Psi^+\rangle \xrightarrow{\mathcal{F}} |\Phi^+\rangle \xrightarrow{\mathcal{F}} |\Psi^+\rangle$. Vizsgáljuk meg most a $|\Psi^+\rangle$ állapot egy perturbációját. Elsőként tekintsük a

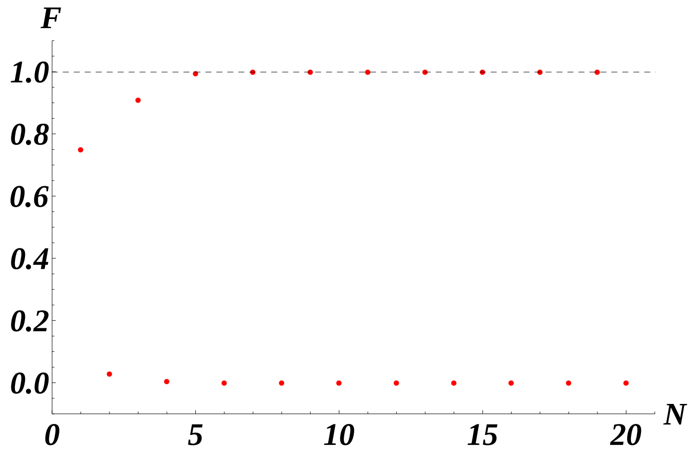
$$\rho_{pert} = \begin{pmatrix} 0.1 & 0 & 0 & 0 \\ 0 & 0.4 & 0.35 & 0 \\ 0 & 0.35 & 0.4 & 0 \\ 0 & 0 & 0 & 0.1 \end{pmatrix} \tag{44}$$

perturbált sűrűségmátrixot (a sajátértékeit ellenőrizve ez valóban egy jó sűrűségmátrix).

Ennek a $|\Psi^+\rangle$ célállapottal vett, 2.3. fejezetben bevezetett átmeneti valószínűsége $F = Tr(\rho_{|\Psi^+\rangle} \cdot \rho_{pert}) = 0,75$. Iterálva $\mathcal{F}$-et a az átmeneti valószínűségre az alábbi sorozatot kapjuk:

$$\{0,75; 0,02941; 0,90996; 0,00522; 0,99412; 0.00003; 0,99999; 0; 1; 0; 1...\}$$

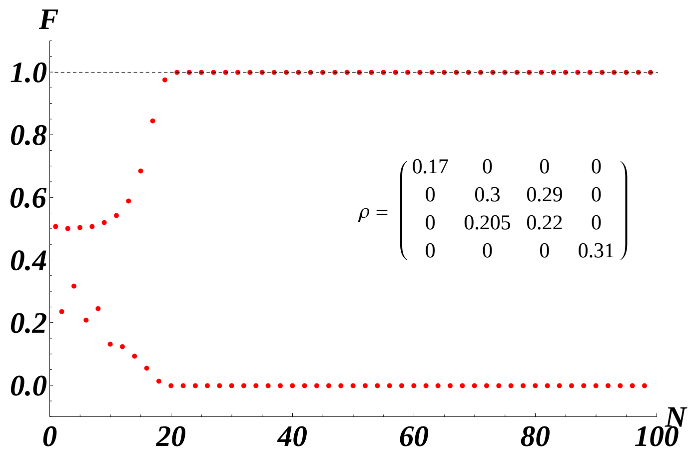
A 11. ábra az átmeneti valószínűséget mutatja az iterációk számának a függvényében. Látható, hogy a (44) állapot már a 6. iteráció után számolási pontosságon belül bekonvergált a $\{|\Psi^+\rangle, |\Phi^+\rangle\}$ ciklusba. Ez tekinthető egy tisztulási folyamatnak.



11. ábra. A (44) állapot $|\Psi^+\rangle$ -val vett átmeneti valószínűsége az iterációk számának függvényében. Az állapot minden páros számú lépésben egyre közelebb kerül a $|\Psi^+\rangle$ állapothoz; néhány iteráció után már számolási pontosságon belül $F = 1$. Ez azt jelenti, hogy az állapot kitisztult és nincs összefonódva a környezettel vagy egy esetleges lehallgatóval.

A numerikus számolások azt mutatják, hogy bármilyen kezdeti állapotot veszünk, amelyre $F_0 > 0,5$, az iteráció bekonvergál a stabil ciklusba. Vannak esetek, amikor az első néhány lépés során távolodik az állapot, majd megfordul a tendencia és bekövetkezik a tisztulás (például 12. ábra), azaz az átmeneti valószínűség az iterációk számának nem feltétlen monoton függvénye.

Eddig azzal az ideális esetettel foglalkoztunk, amikor Alice és Bob tökéletesen el tudja végezni a szükséges lokális forgatást. Vizsgáljuk meg mi történik, ha a forgatások paramétereit változtatjuk; ez lehet egy modellezése annak, hogy a kvantumkapuk fizikai realizációja sosem tökéletes. Továbbra is legyen $\varphi_1 = \varphi_2 = \pi/2$ és $x_1 = x_2 = x$, ez utóbbit fogjuk változtatni (hasonló jellegű eredmények jönnek ki, ha a $\varphi_{1,2}$-t, illetve ha

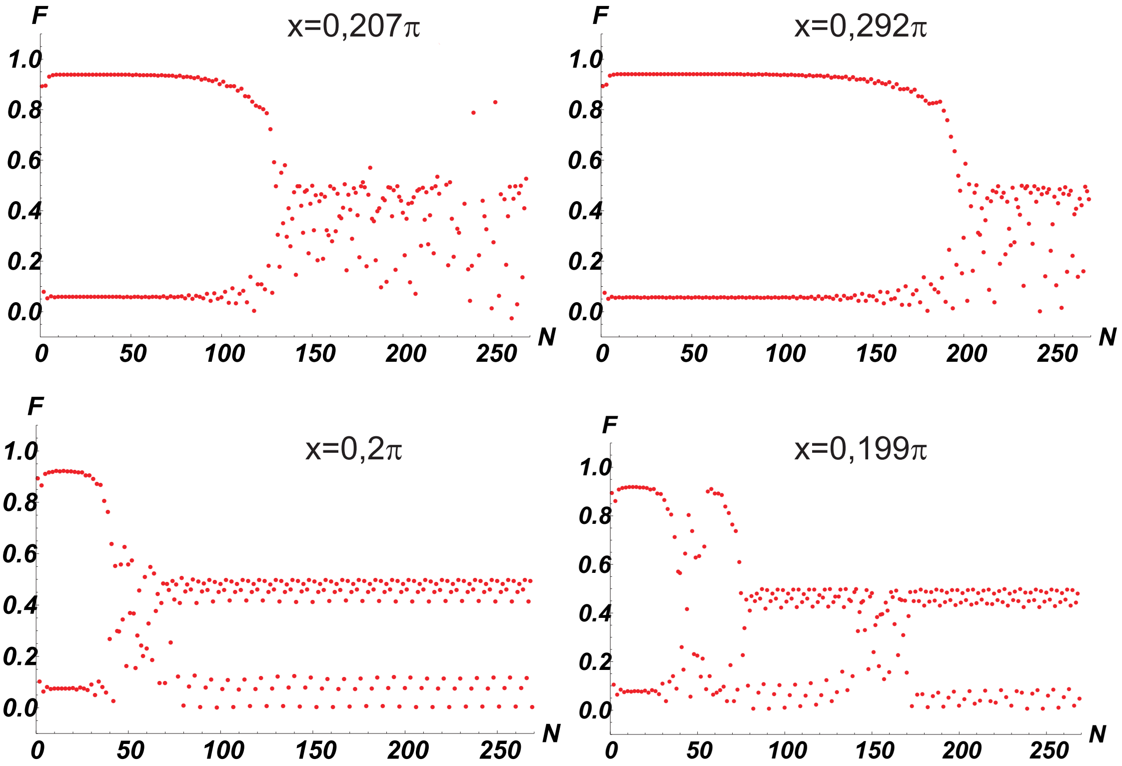


12. ábra. Az állapot tisztításának numerikus vizsgálata $F_0 = 0,5075$ kezdeti átmeneti valószínűség mellett (a kiinduló állapot sűrűségmátrixát is feltüntettük az ábrán). A második lépésben $F_2 = 0,50183$, tehát távolodtunk a célállapottól; ez után azonban megfordul a tendencia és bekövetkezik a tisztulás.

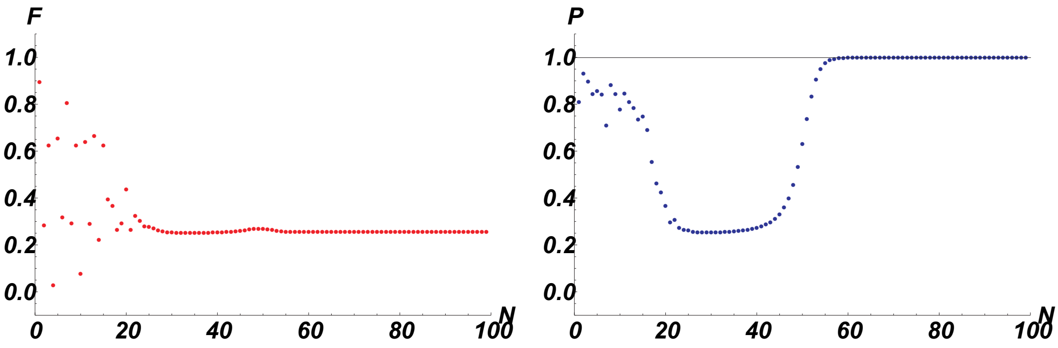
mind a négy paramétert külön-külön változtatjuk).

Legyen például $x = 0,23\pi$. Ekkor a transzformáció stabil ciklusa már nem a tiszta $|\Psi^+\rangle$ és $|\Phi^+\rangle$ Bell-állapotokból, hanem a $\{\rho_1, \rho_2\}$ sűrűségmátrixszal jellemzett állapotokból áll, ahol $F(|\Phi^+\rangle, \rho_1) = F(|\Psi^+\rangle, \rho_2) \approx 0,985$ és egy megfelelő kezdőállapotból elindítva az iteráció ebbe a ciklusba konvergál. Ez az elvárásoknak megfelelő; ha azonban tovább csökkentjük x értékét, érdekes instabilitásokra bukkanhatunk. A 13. ábra áttekintést ad a numerikus eredményekről. Ha az ideális $x = \pi/4$-től megfelelően eltávolodunk, akkor metastabil tartományokra bukkanhatunk: egy kezdeti tisztulás után bizonyos iterációszám után kaotikus lesz a leképezés. Még tovább távolodva különböző hosszúságú stabil ciklusok alakulnak ki.

Az eredmények az egy qubites esettel (7., 8. ábrák) összevetve érthetőek. Az x változtatása az ott bevezetett p paramétert változtatja és így a stabil ciklussal rendelkező illetve nem rendelkező tartományok között váltunk. Az érdekesség az, hogy több esetben egy viszonylag hosszú stabil tisztulás után következik be a káosz.



13. ábra. A (44) állapot $|\Psi^+\rangle$ -val vett átmeneti valószínűsége az iterációk számának függvényében, különböző x forgatási paraméterek mellett.



14. ábra. $F_0 = 0,895$ kezdeti átmeneti valószínűség, $x = 16/25\pi$. A jobb oldali ábrán az állapot tisztasága ($P = Tr\left(\rho^2\right)$) látható az iterációk számának a függvényében. Egy kezdeti keveredés után az állapot kitisztul és bekonvergál egy 1 elemű stabil ciklusba, melyre $F = 0,2566$.

4. A transzformáció általánosítási lehetőségei

4.1. Az általánosított XOR

A következőkben a 3.1. fejezetben bevezetett $\mathcal{S}$ transzformációt, a sűrűségmátrix elemeinek a négyzetre emelését általánosítjuk. A dolgozatban tárgyalt transzformáció alapvető eleme volt a (26) szabályokkal megadott, két qubittel operáló XOR kapu. Az általánosítást így ennek a kapunak a részletesebb vizsgálatával és kiterjesztésével kezdjük. Ez a kapu a kvantuminformatikában több szempontból is központi jelentőségű. Egyrészt, mert két másik egyszerű 1 qubites kapuval, nevezetesen a

$$H : |0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad T : |0\rangle \longrightarrow |0\rangle \quad |1\rangle \longrightarrow e^{i\frac{\pi}{4}}|1\rangle \tag{45}$$

kapukkal (ahol H-t Hadamard-kapunak, T-t pedig fázistoló kapunak is hívják) egy univerzális rendszerhez jutunk. Ez azt jelenti, hogy véges számú ilyen kapu segítségével bármely U unitér operáció tetszőleges pontossággal implementálható. Továbbá számos egyéb művelet elvégezhető a XOR kapuval, például állapotcsere (*quantum state swapping*), állapotok összefonása, Bell-féle méréseket megvalósító protokollok.

Felmerül tehát az igény a XOR kapu általánosítására (melyet GXOR-nak fogunk hívni), amely nem csak qubiteken, hanem quditeken (D állapotú rendszereken) is értelmezve van. Az általánosítást [1] alapján ismertetjük. Ehhez először írjuk át a már megismert XOR-t más, egyszerűbb formalizmusba:

$$XOR_{12}|i\rangle_1|j\rangle_2 = |i\rangle_1|i \oplus j\rangle_2 \quad i \in \{0, 1\} \tag{46}$$

ahol $\oplus$ az összeadás moduló 2-t jelöli. A XOR tulajdonságai:

(i) unitér (tehát reverzibilis)

(ii) hermitikus

(iii) $i \oplus j = 0$ akkor és csak akkor, ha $i = j$

Szeretnénk, ha ezek a tulajdonságok az általánosítás során megmaradnának. A D-dimenziós állapotok bázisait jelölje $\{|i\rangle\} \quad i = 0, 1, ..., D-1$ (precízebben a Z_D gyűrű elemei, amelyek között a szokásos módon definiáljuk a moduló D-t). Ha (46) definíciót nem változtatjuk meg, csak bevezetjük az előbbi jelöléseket, az több szempontból sem kényelmes. Ekkor $D > 2$-re az operáció nem lenne hermitikus, azaz az inverze sem lenne önmaga (az inverzet ekkor iterációval tudnánk megkapni: $GXOR_{12}^{-1} = GXOR_{12}^{D-1} = GXOR_{12}^{\dagger} \neq GXOR_{12}$). Ehelyett általánosított XOR-t definiáljuk

$$GXOR_{12}|i\rangle_1|j\rangle_2 = |i\rangle_1|i \ominus j\rangle_2 \quad i \in \{0, 1, ..., D-1\} \tag{47}$$

módon, ahol $\ominus$ a különbség moduló D-t jelöli. Ez $D = 2$ esetben visszaadja (46)-t, hiszen ekkor $i \ominus j \equiv i \oplus j$. Ez már kielégíti a (46) tulajdonságait tetszőleges D-re, azaz unitér, hermitikus és $i \ominus j = 0$ akkor és csak akkor, ha $i = j$. Megjegyezzük, hogy ez a definíció természetesen kiterjeszthető folytonos változókra is (azaz ha a kontroll és célállapotok is folytonos spektrummal rendelkeznek). Ebben az esetben csak annyi a dolgunk, hogy $\{|i\rangle\}$ helyébe beírjuk $\{|x\rangle\} \quad x \in \mathbb{R}$ folytonos változót, ahol a $\langle x|y\rangle = \delta(x-y)$ ortogonalitási feltételt kikötjük. Ahogy D tart végtelenhez, a kivonás moduló helyettesíthető normál kivonással, így

$$GXOR_{12}|x\rangle_1|x\rangle_2 = |x\rangle_1|x-y\rangle_2 \tag{48}$$

alakra jutunk.

Vegyük észre, hogy a 3.1. fejezetben ismertetett transzformációban, melynek kompakt alakját (28) írja le, ki van tüntetve a $\mathbb{P}_0$ projekció, azaz a szűrési eljárásnál a cél állapotot mindig a $|0\rangle$-ba projektáltuk. Természetesen minden további nélkül megendgedhetünk általános projektor operátort. Preparáljuk kezdetben a kontroll és cél állapotot ρ^c illetve ρ^t sűrűségmátrixokkal jellemzett állapotokba (ez is egy általánosítás, hiszen a korábbiakban azt tettük fel, hogy ugyanazon qubitállapotnak vesszük két másolatát). Két qudit esetére a transzformációt

$$T(\rho^c, \rho^t) = \frac{A(\rho^c \otimes \rho^t)A^{\dagger}}{Tr\left(A(\rho^c \otimes \rho^t)A^{\dagger}\right)} \tag{49}$$

alakban írhatjuk általánosan, ahol

$$A = (\mathbf{1}_c \otimes \mathbb{P})GXOR_{c,t} \tag{50}$$

Itt $\mathbf{1}_c$ jelöli a kontroll bit Hilbert-terén ható egységoperátort, $\mathbb{P} = |p\rangle_t\, {}_t\langle p|$ pedig a cél bit terén ható projekciót. Írjuk ki a két sűrűségmátrix dekompozícióját:

$$\rho^c = \sum_{i,j}^{D-1} \rho^c_{ij} |i\rangle_{c\ c}\langle j| \tag{51a}$$

$$\rho^t = \sum_{i,j}^{D-1} \rho^t_{ij} |i\rangle_{t\ t}\langle j| \tag{51b}$$

Ezzel a transzformáció expliciten kiírva a

$$T(\rho^c, \rho^t) = \frac{\sum\limits_{i,j,k,l}^{D-1} \rho^c_{ij}\rho^t_{kl} |i\rangle_{c\ c}\langle j| \otimes \mathbb{P}|i \ominus k\rangle_{t\ t}\langle j \ominus l|\mathbb{P}}{\sum\limits_{i,k,l}^{D-i} \rho^c_{ii}\rho^t_{kl} \langle p|i \ominus j\rangle_{t\ t}\langle i \ominus l|p\rangle} \tag{52}$$

alakot ölti, ahol a (51a) és (51b) alakokat beírtuk (49)-be és elvégeztük az A transzformációt (50) szerint, kihasználva a GXOR definícióját. Ebből az általános alakból vezessük most vissza a korábbi esetet. Tegyük fel, hogy $\rho^c = \rho^t$. Ekkor

$$T(\rho^c, \rho^t = \rho^c) = \frac{\sum\limits_{i,j,k,l}^{D-1} \rho^c_{ij}\rho^c_{kl} |i\rangle_{c\ c}\langle j| \otimes \mathbb{P}|i \ominus k\rangle_{c\ c}\langle j \ominus l|\mathbb{P}}{\sum\limits_{i,k,l}^{D-i} \rho^c_{ii}\rho^c_{kl} \langle p|i \ominus j\rangle_{c\ c}\langle i \ominus l|p\rangle} = \rho^c_{ki} \otimes \mathbb{P} \tag{53}$$

ahol

$$\rho^c_{ki} = \frac{\sum\limits_{i,j}^{D-1} \rho^c_{ij}\rho^c_{i-p,j-p} |i\rangle_{c\ c}\langle j|}{\sum\limits_{i}^{D-i} \rho^c_{ii}\rho^c_{i-p,i-p}} \tag{54}$$

a kontroll bit kimeneti (transzformáció utáni) sűrűségmátrixa. A korábbi esetben qubitekkel foglalkoztunk, így $D = 2$ és a projektort $\mathbb{P} = |00\rangle_{t\ t}\langle 00|$-nak választottuk. Ha ezeket behelyettesítjük (54) kifejezésbe, akkor a normálási faktortól eltekintve a

$$\rho_{ki}^c = \begin{pmatrix} (\rho_{00}^c)^2 & (\rho_{01}^c)^2 & (\rho_{02}^c)^2 & (\rho_{03}^c)^2 \\ (\rho_{10}^c)^2 & (\rho_{11}^c)^2 & (\rho_{12}^c)^2 & (\rho_{13}^c)^2 \\ (\rho_{20}^c)^2 & (\rho_{21}^c)^2 & (\rho_{22}^c)^2 & (\rho_{23}^c)^2 \\ (\rho_{30}^c)^2 & (\rho_{31}^c)^2 & (\rho_{32}^c)^2 & (\rho_{33}^c)^2 \end{pmatrix} \tag{55}$$

kimeneti mátrixot kapjuk, ami valóban az elemek négyzetre emelése. Más projekciók választásával elérhető, hogy a mátrixelemek egymással bonyolultabb módon keveredjenek. Legyen például $\mathbb{P} = |11\rangle_t\, {}_t\langle 11|$, ekkor a végeredmény a

$$\rho_{ki}^c = \begin{pmatrix} \rho_{00}^c \cdot \rho_{33}^c & \rho_{01}^c \cdot \rho_{32}^c & \rho_{02}^c \cdot \rho_{31}^c & \rho_{03}^c \cdot \rho_{30}^c \\ \rho_{10}^c \cdot \rho_{23}^c & \rho_{11}^c \cdot \rho_{22}^c & \rho_{12}^c \cdot \rho_{21}^c & \rho_{13}^c \cdot \rho_{20}^c \\ \rho_{20}^c \cdot \rho_{13}^c & \rho_{21}^c \cdot \rho_{12}^c & \rho_{22}^c \cdot \rho_{11}^c & \rho_{23}^c \cdot \rho_{10}^c \\ \rho_{30}^c \cdot \rho_{03}^c & \rho_{31}^c \cdot \rho_{02}^c & \rho_{32}^c \cdot \rho_{01}^c & \rho_{33}^c \cdot \rho_{00}^c \end{pmatrix} \tag{56}$$

kimeneti sűrűségmátrix lesz.

További általánosításhoz jutunk, ha megengedjük, hogy több célállapot legyen (például N darab), és a kontroll és célállapotok is M darab quditból álló összetett rendszerek legyenek. Ekkor a kontroll állapot egy általános M-qudit állapot, tehát sűrűségmátrixa

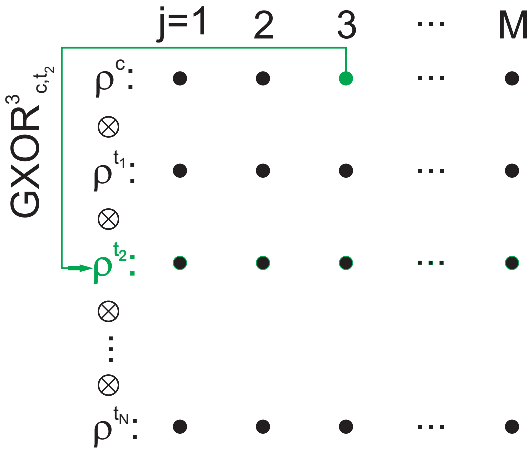
$$\rho^c = \sum_{\mathbf{i},\mathbf{j}} \rho_{\mathbf{ij}}^c |\mathbf{i}\rangle_c\, {}_c\langle \mathbf{j}| \quad \mathbf{i} = \{i_1, i_2, ..., i_M\} \quad \mathbf{j} = \{j_1, j_2, ..., j_M\} \tag{57}$$

alakban írható. Az A operátor definícióját is általánosabb alakra kell írnunk:

$$A = (\mathbf{1}_c \otimes \mathbb{P}) \prod_{j=1}^{M} \prod_{i=1}^{N} GXOR_{c,t_i}^j \qquad \mathbb{P} = \prod_{i=1}^{N} \otimes \mathbb{P}_{t_i} \qquad \mathbb{P}_{t_i} = |p_i\rangle_{t_i}\, {}_{t_i}\langle p_i| \tag{58}$$

Itt a $\mathbb{P}_{t_i}$ projektor az i. célállapotot (amely egy M quditból álló összetett rendszer) vetíti a $|p_i\rangle_{t_i}$ állapotba (mivel N darab célállapotunk van, $i = \{1, 2, ..., N\}$), $GXOR_{c,t_i}^j$ pedig a kontroll rendszer j. quditjén és az i. célállapoton hat. Ez a transzformáció legáltalánosabb alakja. A 15 ábra a $GXOR_{c,t_i}^j$ hatását szemlélteti.

Ezt a formalizmust az általánosságra való törekvés és a matematikai érdekesség kedvéért mutattuk be, a továbbiakban egyszerűbb esetekkel foglalkozunk. Előtte azonban foglaljuk össze (49) tulajdonságait:



15. ábra. Az általános $GXOR^j_{c,t_i}$ hatásának sematikus szemléltetése. Adott egy kontrollállapot és N darab célállapot; ezek mindegyike M darab quditből áll (az ábrán a quditeket pontokkal reprezentáltuk). Formálisan $GXOR^j_{c,t_i}$ hatása $GXOR^j_{c,t_i}|\mathbf{k}\rangle_c|\mathbf{l}\rangle_{t_i} = |\mathbf{k}\rangle_c|\tilde{\mathbf{l}}\rangle_{t_i}$ írható, ahol $|\tilde{\mathbf{l}}\rangle_{t_i} = |l_1, l_2, ..., l_{j-1}, (k_j - l_j)\ mod\ D, l_{j+1}, ..., l_M\rangle$

(i) sűrűségmátrixokat sűrűségmátrixokba visz át

(ii) nem injektív

(iii) nemlineáris

(iv) léteznek invariáns állapotai

4.2. Lokális transzformáció hozzáadása, szeparálható tiszta 2 qubites eset

A továbbiakban vizsgáljuk speciálisan a két qubites esetet, azaz $M = 2$ és $D = 2$ és dolgozzunk fix projekciókkal: $\mathbb{P}_{t_i} \equiv \mathbb{P} = |p_i\rangle_{t_i}\ {}_{t_i}\langle p_i| \quad \forall i$. Az esetet már vizsgálták [32]-ban. A (54) transzformációhoz vegyük hozzá a forgatást is, melyet a már megszokott módon $U = U_1 \otimes U_2 \quad U_{1,2} \in SU(2)$ választunk, (41) paraméterezéssel. A bemeneti állapotunk legyen szeparálható tiszta két qubites állapot, azaz sűrűségmátrixa $\rho = \rho_1 \otimes \rho_2$ írható, ahol $\rho_{1,2} = |\psi\rangle_{1,2}\ {}_{1,2}\langle\psi|$. Az egyes tiszta állapotokat írjuk Riemann-féle paraméterezésben, a paramétereket pedig hívjuk $z_{1,2}$-nek. A 3.2. fejezetben tárgyaltaknak megfelelően vezessük be a $p_{1,2} = \tan x_{1,2} \cdot e^{i\varphi_{1,2}}$ paramétert.

Négy lehetséges projekciót használhatunk, és ezek az állapotokat

$$\mathbb{P} = |00\rangle\langle 00| : \qquad z_{1,2} \longrightarrow \frac{z_{1,2}^{N+1} + p_{1,2}}{1 - p_{1,2}^* \cdot z_{1,2}^{N+1}}$$

$$\mathbb{P} = |01\rangle\langle 01| : \qquad z_1 \longrightarrow \frac{z_1^{N+1} + p_1}{1 - p_1^* \cdot z_1^{N+1}} \quad z_2 \longrightarrow \frac{1 + p_2 z_2^{N-1}}{z_2^{N-1} - p_2^*}$$

$$\mathbb{P} = |10\rangle\langle 10| : \qquad z_1 \longrightarrow \frac{1 + p_1 z_1^{N-1}}{z_1^{N-1} - p_1^*} \quad z_2 \longrightarrow \frac{z_2^{N+1} + p_2}{1 - p_2^* \cdot z_2^{N+1}}$$

$$\mathbb{P} = |11\rangle\langle 11| : \qquad z_{1,2} \longrightarrow \frac{z_{1,2}^{N+1} + p_{1,2}}{1 - p_{1,2}^* \cdot z_{1,2}^{N+1}}$$

szerint transzformálják. Vegyük észre, hogy $\mathbb{P} = |00\rangle\langle 00|$ projekcióval és $N = 1$ esetén (azaz 1 cél állapottal) pontosan visszakaptuk a (34) alakot. Legyen továbbá $p = 0$, ekkor a $z_{1,2} \longrightarrow z^{N+1}$ leképezéshez jutunk. A Julia-halmaz továbbra is az egységkör és $N + 2$ darab fixpontunk van: $\{0, e^{(2i\pi k)/(N+1)}\}$, ahol $k \in \{0, ..., N\}$.

Számoljuk ki a dinamikát egy olyan esetre is, ahol a lokális unitér transzformáció nem forgatás. Vegyük például az ún. Hadamard-kaput (ezen a transzformáción alapul például a [1]-ban vizsgált purifikációs protokoll):

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{59}$$

A qubitek dinamikája ebben az esetben, amikor a lokális unitér transzformációt $U = U_H \otimes U_H$-nak választjuk, a qubitek állapotát a következők szerint transzformálja:

$$\mathbb{P} = |00\rangle\langle 00| : \qquad z_{1,2} \longrightarrow \frac{z_{1,2}^{N+1}+1}{z_{1,2}^{N+1}-1}$$

$$\mathbb{P} = |01\rangle\langle 01| : \qquad z_1 \longrightarrow \frac{z_1^{N+1}+1}{z_1^{N+1}-1} \quad z_2 \longrightarrow \frac{z_2^{N-1}+1}{1-z_2^{N-1}}$$

$$\mathbb{P} = |10\rangle\langle 10| : \qquad z_1 \longrightarrow \frac{z_1^{N-1}+1}{1-z_1^{N-1}} \quad z_2 \longrightarrow \frac{z_2^{N+1}+1}{z_2^{N+1}-1}$$

$$\mathbb{P} = |11\rangle\langle 11| : \qquad z_{1,2} \longrightarrow \frac{z_{1,2}^{N-1}+1}{1-z_{1,2}^{N-1}}$$

Ha $N \geq 3$, akkor bármely projekció választása esetén a Julia-halmaz nemüres [16], tehát kaotikus tartományok vannak.

5. Összefoglalás és kitekintés

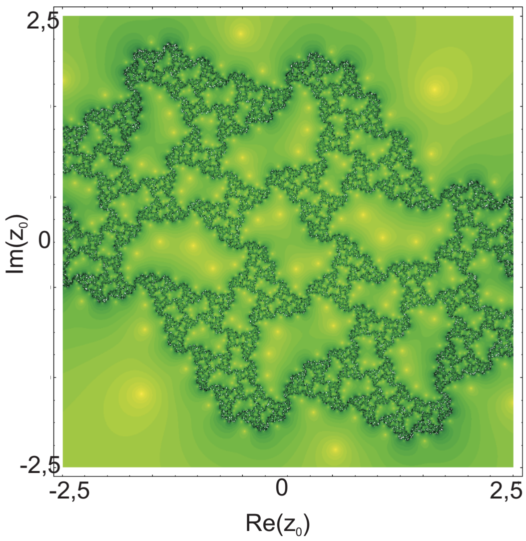
A dolgozatban egy speciális, a mai eszközökkel már realizálható, qubiteken értelmezett transzformációt vizsgáltunk. Az egy qubites tiszta esetben a dinamikát egy $\mathbb{C} \to \mathbb{C}$ nemlineáris leképezés jellemezte; nem ismerünk más olyan fizikai rendszert, amely direkt módon ilyen típusú dinamikát valósítana meg. Ezek a leképezések a matematikában már régóta ismertek, így ezen eszköztár segítségével analítikusan tudtuk vizsgálni a problémát és megmutattuk, hogy a transzformáció iteratív alkalmazása során a dinamika kaotikussá válhat. A kaotikus jelleg több irányból is megjelent: egyrészt a kezdőállapotra való érzékenységben, másrészt a transzformáció egy belső paraméterére vett érzékenységben. Az analítikus megfontolásokat numerikus szimulációval tettük szemléletessé. A kevert állapotokat a Bloch-formalizmus segítségével analítikusan közelítettük meg; ez utóbbi az irodalomban még nem vizsgált eset. Két qubitnél a paramétertartomány már az egy qubites esetnél jóval nagyobb; itt bemutattuk, hogy a transzformáció hogyan alkalmazható állapottisztításra, melynek kvantuminformatikai felhasználásban lehet jelentősége. Numerikusan vizsgáltuk az így megvalósított tisztító protokoll stabilitását a transzformáció belső paraméterére és kaotikus tartományokra bukkantunk. Végül bemutattuk a transzformáció egy lehetséges általánosítását, melyet az irodalomban már tárgyaltak. Itt a legáltalánosabb formalizmus bevezetése után visszatértünk a két qubit esetéhez és az általánosságból bizonyos elemeket meghagyva újra levezettük a dinamikát.

A dolgozat több lezáratlan témakört, kérdést tartalmaz, melyek további kutatási témát képeznek. Szeretnénk elvégezni az egy qubites kevert állapot numerikus vizsgálatát. A két qubit dinamikáját további reprezentációkban lehetne vizsgálni; erre alkalmas lehet például a Schmidt-bázis, melynek elméletét a dolgozat elején kifejtettük. Vizsgálhatjuk továbbá a transzformáció általánosítási lehetőségeit. A téma kapcsán egy fundamentálisabb kérdés is felmerül, mégpedig hogy a kvantummechanika által megengedett nemlineáris transzformációk mikor, milyen feltételek mellett vezethetnek káoszhoz.

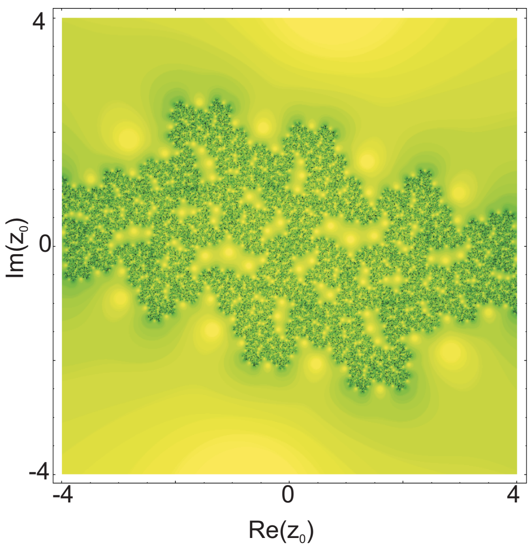
Köszönetnyilvánítás

Szeretném megköszönni Kiss Tamásnak a téma felvetését és az igényes, időt és fáradtságot nem kímélő témavezetést. A téma feldolgozása, mely közben komoly tapasztalatokat szereztem és amely érzésem szerint jelentős előrehaladást hozott a szakmai fejlődésemben, értékes tanácsai és ötletei nélkül nem sikerült volna.

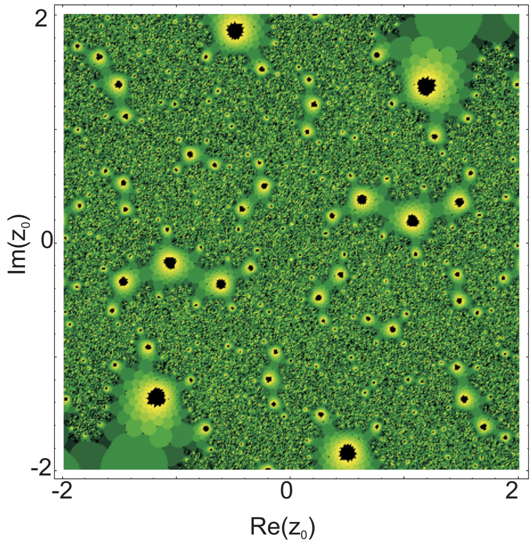
A. Néhány további kép az 1 qubites esethez



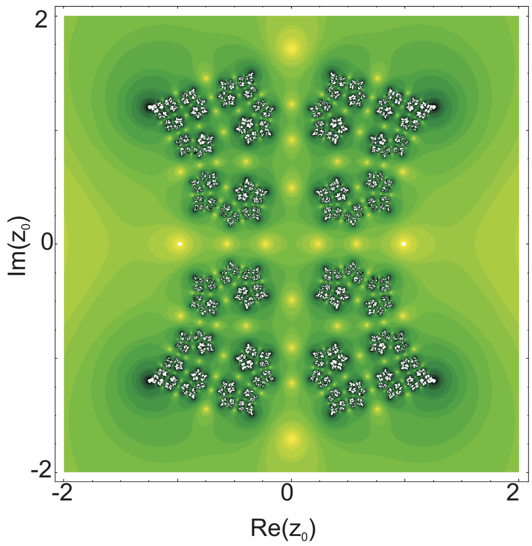
16. ábra. Julia-halmaz $p = 1 + 0,4i$ esetre. A Julia-halmaz összekötött; megfigyelhető a torzulás a 4. ábrához képest. Egy stabil ciklus van, melynek hossza 2: $z_1 \approx -0,8340 - 0,2976i \quad z_2 \approx 0,8340 + 5,6976i$



17. ábra. Julia-halmaz $p = 1 + 0,6i$ esetre. A Julia-halmaz továbbra is összekötött és egy stabil ciklus van, melynek hossza 2: $z_1 \approx -0,7183 - 0,3536i \quad z_2 \approx 0,7183 + 4,2870i$



18. ábra. $p = 1 + 0,8i$. Elértük a kaotikus tartomány szélét (vö. 5. ábra)



19. ábra. Julia-halmaz $p = 0,5$ esetre. A fehér szigetek nem konvergálnak (a szigetek területe valójában nulla, hiszen a Julia-halmaznak vagy nincs belső pontja, vagy maga az egész $\hat{\mathbb{C}}$; a numerikus pontatlanság miatt látjuk mégis kiterjedtnek). A Julia-halmaz teljesen szétesett. Egy stabil ciklus van, melynek hossza 1: $z_1 \approx -2,8312$

B. Kvantuminformatikai protokollok: az összefonódás, mint erőforrás

B.1. Szupersűrű kódolás

A kvantuminformatika, melynek alapjait körülbelül 20 évvel ezelőtt kezdték el lerakni és azóta rendkívül nagy fejlődésen ment keresztül, elméletben a hagyományos informatikát meghaladó hatékonysággal kezel több fontos információelméleti kérdést. A qubitek segítségével, szofisztikált protokollok alkalmazásával és a kvantummechanika törvényeinek kiaknázásával olyan titkosítási vagy kommunikációs sémák dolgozhatók ki, melyek teljesítménye jóval a klasszikus teljesítmény fölött lehet. A 3. fejezet (és ezen belül is főként a 3.4. fejezet) praktikus hasznát illusztrálandó, bemutatunk két egyszerű protokollt, mely a tiszta, tökéletesen összefonódott állapotot (Bell-állapotot), mint erőforrást használja. Ezek a sémák az LOCC (*Local Operations and Classical Communication*) családba tartoznak, mert megvalósításukhoz szükséges egy klasszikus információs csatorna és helyi operációk elvégzése.

Az első ilyen protokoll az ún. szupersűrű kódolás. Tegyük fel, hogy Alice szeretne 2 klasszikus bit információt elküldeni Bobnak (hogy a nevekkel hűek maradjunk a szakirodalomhoz). Ehhez először is szükség van arra, hogy Alice és Bob előzetesen megosszanak egy Bell-állapotot, melyeket

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{60a}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{60b}$$

módon definiáljuk. Tegyük fel, hogy Alice és Bob a $|\Phi^+\rangle$ állapotot osztották meg előzetesen; Alice az első bitet, Bob a második bitet kapta. A második lépésben Alice a saját qubitjén elvégez egy adott transzformációt, attól függően, hogy milyen információt szeretne küldeni, az alábbi szabály szerint:

Küldeni kívánt bitpár	Elvégzendő transzformáció	Hatása $|\Phi^+\rangle$-ra
00	$\hat{I} \otimes \hat{I}$	$|\Phi^+\rangle$
01	$\hat{\sigma_x} \otimes \hat{I}$	$|\Psi^+\rangle$
10	$\hat{\sigma_z} \otimes \hat{I}$	$|\Phi^-\rangle$
11	$\hat{\sigma_x} \cdot \hat{\sigma_x} \otimes \hat{I}$	$|\Psi^-\rangle$

Ezt röviden úgy is jelölhetjük, hogy ha Alice ab bitpárt akarja elküldeni, akkor egy $U_{ab} = \hat{\sigma_z}^a \cdot \hat{\sigma_x}^b$ lokális unitér transzformációt végez el a saját qubitjén. A harmadik lépésben Alice elküldi a qubitjét Bobnak, aki ezzel valamelyik Bell-állapot birtokában van. Nincs más dolga, mint elvégezni egy mérést a Bell-bázisban (ez fizikailag implementálható); a mérési eredmény után bizonyossággal tudja Alice két bites üzenetét. Alice tehát egy fizikai qubit küldésével két klasszikus bit információt tudott küldeni Bobnak, feltéve persze, hogy sikeresen megosztottak egy - általuk ismert - Bell-párt.

B.2. Kvantumteleportáció

Ezzel analóg probléma az ún. kvantumteleportáció, mely során Alice egy qubit állapotát szeretné elküldeni Bobnak. Ennek során tegyük fel, hogy Alice és Bob rendelkezésére áll egy őket összekötő klasszikus kommunikációs csatorna (pl. telefon). Intuíciónk azt mondja, hogy Alice nem tehet mást: vagy elküldi magát a qubitet (ezt egy klasszikus csatornán nyilván nem teheti meg) vagy a qubitet jellemző paramétereket - reprezentációtól függően pl. a két komplex amplitudót - küldi el végtelen pontossággal (ez utóbbit pedig azért nem teheti meg, mert ezeket az információkat ő sem tudja). Kiderül azonban, hogy ez az intuíció hibás, és egy előzetesen megosztott Bell-állapottal és két klasszikus bit információval Alice elteleportálhatja a kérdéses qubitet. A protokoll semmiféle ellentmondásban nincs a kvantummechanika alapjaival, pl. a no-cloning tétellel (azaz hogy a kvantumállapotok nem klónozhatók): Alice a teleportáció után a kérdéses qubitről nem tud semmit.

Tegyük fel, hogy - akárcsak a szupersűrű kódoló protokollnál - Alice és Bob megosztanak egy $|\Phi^+_{AB}\rangle$ párt. Alice elteleportálandó qubitjét írjuk $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ alakban. Kezdetben tehát a 3 qubit együttes állapota

$$|\psi_A\rangle|\Phi^+_{AB}\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{61}$$

ahol az egyszerűség kedvéért alsó indexben feltüntettük, hogy melyik bit kinél található. Végezzük el a szorzást:

$$|\psi_A\rangle|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(\alpha|0_A 0_A 0_B\rangle + \alpha|0_A 1_A 1_B\rangle + \beta|1_A 0_A 0_B\rangle + \beta|1_A 1_A 1_B\rangle) \tag{62}$$

Ezt írjuk át, hogy Alice része a Bell-bázisban legyen felírva.

$$
\begin{aligned}
|\psi_A\rangle|\Phi^+_{AB}\rangle &= \frac{1}{2}\Big(|\Phi^+_{AA}\rangle(\alpha|0_B\rangle + \beta|1_B\rangle) + |\Phi^-_{AA}\rangle(\alpha|0_B\rangle - \beta|1_B\rangle) + \\
&\quad + |\Psi^+_{AA}\rangle(\alpha|1_B\rangle + \beta|0_B\rangle) + |\Psi^-_{AA}\rangle(\alpha|1_B\rangle - \beta|0_B\rangle)\Big)
\end{aligned}
$$

Ezek eddig matematikailag ekvivalens átalakítások voltak, fizikailag nem történt semmi. A következő lépésben Alice elvégez egy mérést a Bell-bázisban, és az eredményt elküldi Bobnak telefonon (ez két biten megtehető). Bob ezzel megtudja, hogy a $(\alpha|0\rangle \pm \beta|1\rangle), (\beta|0\rangle \pm \alpha|1\rangle)$ állapotok közül melyik van nála, és ettől függően elvégez egy lokális unitér transzformációt az eredeti $|\psi\rangle$ állapot elöllítására, az alábbi szabályok szerint:

Alice mérése	Bob állapota	Bob transzformációja
$\|\Phi^+\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$\hat{I}$
$\|\Phi^-\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\hat{\sigma_z}$
$\|\Psi^+\rangle$	$\beta\|0\rangle + \alpha\|1\rangle)$	$\hat{\sigma_x}$
$\|\Psi^-\rangle$	$\beta\|0\rangle - \alpha\|1\rangle)$	$\hat{\sigma_x} \cdot \hat{\sigma_z}$

Alice tehát két klasszikus bit és egy megosztott Bell-pár segítségével elteleportálhat egy qubitet Bobnak. A fenti két protokoll mutatja, hogy az összefonódás, amellett, hogy mai fizika egyik fundamentális kérdéskörét képezi, praktikus szempontból is érdekes lehet és nem véletlen, hogy ezzel kapcsolatban a fizika az elmúlt két évtizedben egy szemléletváltáson ment keresztül.

Hivatkozások

[1] G. Alber, A. Delgado, N. Gisin, and I. Jex. Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces. *J. Phys. A: Math. Gen*, 34, 2001.

[2] H. Bechmann-Pasquinucci, B. Huttner, and N. Gisin. Non-linear quantum state transformation of spin-1/2. *Phys. Lett. A*, 242, 1999.

[3] G. Benenti and G. Strini. Simple representation of quantum process tomography. *Phys. Rev. A*, 80(2), 2009.

[4] M. S. Byrd and N. Khaneja. Characterization of the positivity of the density matrix in terms of the coherence vector representation. *Phys. Rev. A*, 68, 2003.

[5] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* Wiley, 2006.

[6] P. Cvitanovic, Artuso R., Tanner G., and Vattay G. *Chaos: Classical and Quantum.* http://www.chaosbook.org/, 2009.

[7] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77(13), 1996.

[8] P. Fatou. *C. R. Hebd. Seances Acad. Sci.*, 143(546), 1906.

[9] S. Habib, T. Bhattacharya, B. Greenbaum, K. Jacobs, K. Shizume, and B. Sundaram. Chaos and quantum mechanics. *arXiv:quant-ph/0505085v1*, 2005.

[10] S. Habib, K. Jacobs, and K. Shizume. *Phys. Rev. Lett.*, 96(010403), 2006.

[11] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[12] T. Kiss, I. Jex, G. Alber, and E. Kollar. Properties of complex chaos in conditional qubit dynamics. *International Journal of Quantum Information*, 6, 2008.

[13] T. Kiss, I. Jex, G. Alber, and S. Vymetal. Complex chaos in the conditional dynamics of qubits. *Phys. Rev. A*, 74, 2006.

[14] S. Lloyd and J.-J. Slotine. *Phys. Rev. A.*, 62(012307), 2000.

[15] C. Macchiavello. *Phys. Rev. A*, 246(385), 1998.

[16] J. Milnor. *Dynamics in One Complex Variable.* Stony Brook IMS Preprint, 1990.

[17] J. Milnor. Geometry and dynamics of quadratic rational maps. *Experimental Mathematics*, 2(1), 1993.

[18] J. A. Miszczak, Z. Puchala, P. Horodecki, A. Uhlmann, and K. Zyczkowski. Sub- and super-fidelity as bounds for quantum fidelity. *Quantum Information and Computation*, 9(1–2):103–130, 2009.

[19] S. Morosawa, Y. Nishimura, M. Taninguchi, and T. Ueda. *Holomorphic Dynamics.* Cambridge University Press, 2000.

[20] M. Mosca, P. Kaye, and P. Laflamme. *An Introduction to Quantum Computing.* Oxford University Press, 2007.

[21] R. Mosseri and R. Dandoloff. Geometry of entangled states, Bloch spheres and Hopf fibrations. *J. Phys. A: Math. Gen.*, 34(47), 2001.

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

[23] M. Ozols and L. Mancinska. Generalized Bloch vector and the eigenvalues of a density matrix (unpublished). 2007.

[24] H. Poincaré. *Les Méthodes Noivelles de la Méchanique Céleste.* Gauthier-Villars, Paris, 1892.

[25] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738–2747, 1995.

[26] M. Shishikura. On the quasiconformal surgery of the rational functions. *Ann. scient. Ec. Norm. Sup.*, 4, 1987.

[27] E. Sjöqvist. Geometric phase for entangled spin pairs. *Phys. Rev. A*, 62, 2000.

[28] D. R. Terno. Nonlinear operations in quantum-information theory. *Phys. Rev. A*, 62(5), 1999.

[29] A. Uhlmann. *Rep. Math. Phys.*, 9:273, 1976.

[30] H. Urbantke. *Am. J. Phys.*, 59(503), 1991.

[31] V. Vedral. *Introduction to Quantum Information Science.* Oxford University Press, 2006.

[32] S. Vymetal. Dynamics of two qubits purification protocol (unpublished).