Kvantti-informaation naamiointi

Pro Gradu
Turun yliopisto
Teoreettinen fysiikka
2022
LuK Markku Hahto
Tarkastajat:
Teiko Heinosaari
Juha-Pekka Pellonpää

TURUN YLIOPISTO
Fysiikan laitos

Hahto, Markku Kvantti-informaation naamionti

Pro Gradu, 59 sivua
Teoreettinen fysiikka
Elokuu 2022

Kvanttimekaniikan matemaattinen rakenne johtaa tuloksiin, joiden mukaan on olemassa sellaisia operaatioita, joita ei yleisesti ole mahdollista toteuttaa. Näitä tuloksia kutsutaan kieltolauseiksi. Tunnettuja esimerkkejä kieltolauseista ovat muun muassa kloonaamisen kieltolause ja informaation hävittämisen kieltolause. Tuorein lisäys kieltolauseiden joukkoon on kvantti-informaation naamioinnin kieltävä lause. Informaation naamiointi on operaatio, jossa jonkin tilan sisältämä informaatio hajautetaan yhdistetylle systeemille siten, että yksikään osasysteemi ei sisällä lainkaan informaatiota; kaikki alkuperäinen informaatio on siirretty osasysteemien välisiin korrelaatioihin.

Naamioinnin kieltolauseen mukaan yhdellä naamiointioperaatiolla ei ole mahdollista naamioida mielivaltaista kvanttitilaa kahdelle systeemille. Kutakin operaatiota vastaavan naamioitavien tilojen joukon rakenne ei kuitenkaan ole triviaali, ja rakenne riippuu naamiointikuvauksen ominaisuuksista.

Tutkielmassa esitellään kvantti-informaation naamiointioperaatio ja siihen liittyvä kieltolause. Naamioitavien tilojen joukon rakenteen tärkeimpiä ominaisuuksia koskevat lauseet käydään läpi todistuksineen. Lisäksi tarkastellaan kahta tapaa kiertää kieltolauseen asettamat rajat, approksimatiivista ja probabilistista naamiointia. Lopuksi naamioinnin kieltolausetta vertaillaan muutamaan muuhun merkittävään kieltolauseeseen.

Asiasanat: kvantti-informaatio, kieltolause, naamiointi

Sisältö

Johdanto

Jo kvanttimekaniikan alkuajoista lähtien on tiedetty, että klassisessa ja kvanttimaailmassa vallitsevat erilaiset säännöt. Jotkin klassisesti mahdolliset tapahtumat ovat kvanttimekaniikan lakien vastaisia, ja toisaalta on olemassa klassisesti mielipuolisilta kuulostavia ilmiöitä, jotka ovat kvanttimekaniikassa arkipäivää.

Yksi merkittävä esimerkki klassisen ja kvanttimaailman eroista on kvanttimekaniikan kieltolauseet (engl. *no-go theorems*). Nimensä mukaisesti nämä lauseet kieltävät jonkin operaation kvanttisysteemeille tai kvantti-informaatiolle, vaikka vastaava operaatio olisi klassisen fysiikan maailmassa täysin mahdollinen. Tunnetuin kieltolauseista lienee kloonauksen kieltolause, jonka mukaan mielivaltaisesta kvanttitilasta ei ole mahdollista tehdä täydellistä kopiota [1]. Klassisissa fysiikan teorioissa mikään ei periaatteessa estä rakentamasta laitetta, joka kopioisi laitteeseen syötettävän systeemin tilan täydellisesti.

Vuonna 2018 Modi *et al.* esittelivät uuden tuloksen kieltolauseiden kasvavaan joukkoon [2]. *Naamioinnin kieltolause* kieltää sellaiset operaatiot, jotka pystyvät naamioimaan mielivaltaisen tilan sisältämän kvantti-informaation. Naamiointi on kvantti-informaatioteoreettinen protokolla, jossa yhden kvanttisysteemin sisältämä kvantti-informaatio siirretään useammasta osasysteemistä koostuvaan yhdistettyyn systeemiin siten, että informaatio siirtyy yksinomaan osasysteemien välisiin korrelaatioihin eli keskinäisiin riippuvaisuuksiin, eikä yksikään osasysteemi yksinään sisällä lainkaan alkuperäistä informaatiota. Toisin sanoen naamioitu kvantti-informaatio on palautettavissa vain tarkastelemalla yhdistettyä systeemiä kokonaisuutena, ja vain yhtä osasysteemiä tutkimalla alkuperäiseen informaatioon ei ole mahdollista päästä käsiksi.

Luvussa 1 käydään lyhyesti läpi tärkeimmät tutkielmassa hyödynnettävät matemaattiset työkalut. Luvussa 2 määritellään informaation naamiointi kvanttisysteemeihin, ja luvussa 3 esitellään naamioinnin kieltolause. Sen jälkeen syvennytään tar-

kastelemaan, millaista informaatiota on mahdollista naamioida eri tilanteissa. Luku 4 esittelee kaksi mahdollista lähestymistapaa kieltolauseen kiertämiseksi, ja tarkastelee niiden toimivuutta ja tehokkuutta. Luvussa 5 tarkastellaan kvantti-informaation naamioinnin sovelluksia ja naamioinnin kieltolauseen seurauksia. Lopuksi luvussa 6 verrataan eri kieltolauseita vastaavien tilajoukkojen keskinäisiä suhteita, ja sijoitetaan naamioinnin kieltolause sitä vanhempien tulosten hierarkiaan.

1 Matemaattisia työkaluja

Tämä luku sisältää lyhyen katsauksen merkittävimpiin tutkielmassa käytettäviin matemaattisiin työkaluihin. Kvanttimekaniikan peruskäsitteet — Hilbertin avaruudet, tilat, operaattorit — oletetaan pääosin tunnetuiksi.

Lyhyenä kertauksena tutkielman merkintätapojen kiinnittämiseksi: d-ulotteisen kvanttisysteemin A tila-avaruutta merkitään $\mathcal{H}_A^d$, ja jos systeemin ulottuvuudella ei ole merkitystä, $\mathcal{H}_A$. Systeemin puhtaita tiloja vastaavat ket-vektorit, joilla esimerkiksi tila ψ systeemissä A merkitään $|\psi\rangle_A$. Yleisemmin tilojen kuvaamiseen käytetään tiheysmatriiseja ρ_A. Puhtaan tilan $|\psi\rangle_A$ tiheysmatriisi saadaan laskusta $\rho_A = |\psi\rangle_A\langle\psi|_A$. Sekoitetut tilat on mahdollista esittää vain tiheysmatriisin avulla; ne eivät vastaa mitään ket-vektoria.

Kahdesta tai useammasta osasysteemistä A, B, ... koostuvan yhdistetyn systeemin tila-avaruus muodostetaan osasysteemien tila-avaruuksien tensoritulolla, $\mathcal{H}_{AB\ldots} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots$. Yhdistetyn systeemin tiloja merkitään normaalisti $|\psi\rangle_A \otimes |\varphi\rangle_B$ tai $|\psi\rangle \otimes |\varphi\rangle$, missä $|\psi\rangle \in \mathcal{H}_A$ ja $|\varphi\rangle \in \mathcal{H}_B$. Mikäli sekaannuksen mahdollisuutta ei ole tai esitys olisi täysin merkinnöin vähemmän selkeä, käytetään lyhyempää merkintätapaa $|\psi\rangle|\varphi\rangle$, ja etenkin konkreettisia esimerkkejä käsitellessä edelleen tiiviimpää muotoa $|\psi\varphi\rangle$ — esimerkiksi kahdesta kubitista koostuvan yhdistetyn systeemin eräs tila merkitään $|00\rangle$.

1.1 Lomittuminen

Määritelmä 1. *Yhdistetyn systeemin $\mathcal{H}_A \otimes \mathcal{H}_B$ tila $|\Psi\rangle_{AB}$ on* lomittunut*, mikäli se ei ole hajoava. Hajoavat tilat ovat sellaisia tiloja $|\Phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, jotka voidaan kirjoittaa muodossa $|\psi\rangle_A \otimes |\varphi\rangle_B$, missä $|\psi\rangle \in \mathcal{H}_A$ ja $|\varphi\rangle \in \mathcal{H}_B$.*

Lomittunutta tilaa ei siis ole mahdollista erotella osasysteemien tilojen yhdistelmäksi, vaan ainoastaan yhdistetyn systeemin tila voidaan määritellä täysin: osasysteemien tilat ovat riippuvaisia toisistaan.

Tarkastellaan esimerkkinä kahdesta kubitista koostuvan yhdistetyn systeemin tiloja $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ ja $|\Phi\rangle_{AB} = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$. Jälkimmäinen tila on hajoava, sillä se voidaan kirjoittaa muodossa $|\Phi\rangle_{AB} = \frac{1}{2}(|0\rangle + |1\rangle)_A \otimes (|0\rangle + |1\rangle)_B$. Osasysteemit voidaan kirjoittaa erilleen, ja ne ovat kumpikin tilassa $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Ensimmäinen tila, $|\Psi\rangle_{AB}$, puolestaan on lomittunut, sillä siitä ei voida eritellä osasysteemien tiloja. Huomioitavaa kuitenkin on, että termit $|01\rangle$ ja $|10\rangle$ erillään ovat hajoavia tiloja, ja yleisesti mikä tahansa lomittunutkin tila voidaan lausua hajoavien tilojen lineaarikombinaationa [3].

Yllä olevasta esimerkistä voidaan nähdä myös ero osasysteemien välisissä korrelaatiooissa hajoavan ja lomittuneen tilan välillä. Jos osasysteemille A suoritetaan mittaus, kun yhdistetty systeemi on lomittuneessa tilassa $|\Psi\rangle_{AB}$, systeemi B havaitaan sen jälkeen aina vastakkaisessa tilassa: A:n mittaustuloksen ollessa $|0\rangle$ osasysteemille B tehdyn mittauksen tulos on aina $|1\rangle$. Hajoavalla tilalla tällaista yhteyttä mittaustulosten välillä ei ole: jos A:lle suoritetaan mittaus ja saadaan tulokseksi $|0\rangle$, B on edelleen tilassa $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, ja sille suoritettavan mittauksen tulosta ei voida ennustaa.

1.2 Osittainen jälki

Yhdistetyn systeemin $\mathcal{H}_A \otimes \mathcal{H}_B$ tilasta $|\Psi\rangle_{AB}$ saadaan osasysteemien tiheysmatriisit ρ_A ja ρ_B ottamalla *osittainen jälki* tilasta $|\Psi\rangle_{AB}$. Osasysteemien tiheysmatriiseja

kutsutaan myös yhdistetyn systeemin marginaalitiloiksi.

Osittainen jälki määritellään hajoavalle tilalle ρ_{AB} kuvauksena

$$\rho_B = \mathrm{Tr}_A(|\psi\rangle_A\langle\psi|_A \otimes |\varphi\rangle_B\langle\varphi|_B) = (\mathrm{Tr}|\psi\rangle_A\langle\psi|_A) \otimes |\varphi\rangle_B\langle\varphi|_B, \tag{1}$$

eli ottamalla jälki vain toisen osasysteemin yli. Lomittuneille tiloille osittainen jälki yleistyy ilmeisellä tavalla, kun sen vaaditaan olevan lineaarinen kuvaus: lomittuneet tilat voidaan esittää hajoavien tilojen lineaarikombinaationa [4].

1.3 Schmidtin hajotelma

Schmidtin hajotelma on tapa esittää yhdistyneen kvanttisysteemin puhdas tila osasysteemien Hilbertin avaruuksien ortonormaalien tilojen avulla. Hajotelma on kätevä, kun osasysteemien tiheysmatriiseja halutaan käsitellä erikseen: tiheysmatriiseilla on samat ominaisarvot.

Lause 1. *Olkoon $\mathcal{H}_A$ ja $\mathcal{H}_B$ Hilbertin avaruuksia. Jokainen yhdistetyn systeemin $\mathcal{H}_A \otimes \mathcal{H}_B$ puhdas tila $|\Psi\rangle$ voidaan esittää muodossa*

$$|\Psi\rangle = \sum_{i=1}^{d} \lambda_i |a_i\rangle|b_i\rangle, \tag{2}$$

missä $\{|a_i\rangle\}$ on joukko ortonormaaleja tiloja $\mathcal{H}_A$:ssa ja $\{|b_i\rangle\}$ joukko ortonormaaleja tiloja $\mathcal{H}_B$:ssa, ja $d = \min(d_A, d_B)$. λ_i ovat Schmidtin kertoimia*, joille pätee $\sum_i \lambda_i^2 = 1$. Esitysmuotoa* (2) *kutsutaan* Schmidtin hajotelmaksi *[4].*

Todistus. Yleisessä tapauksessa $\dim(\mathcal{H}_A) \neq \dim(\mathcal{H}_B)$, jolloin puhdas tila $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ kirjoitetaan muodossa

$$|\psi\rangle = \sum_{j=1}^{d_A} \sum_{k=1}^{d_B} a_{jk} |j\rangle|k\rangle, \tag{3}$$

missä a_{jk} ovat $d_A \times d_B$ kompleksisen kerroinmatriisin A alkiot, ja $|j\rangle$ ja $|k\rangle$ ovat osasysteemien ortonormaaleja kantavektoreita. Yleisyyttä loukkaamatta voidaan olettaa, että $d_A < d_B$.

Kerroinmatriisi A voidaan kirjoittaa singulaariarvohajotelmaksi muotoon

$$A = U\widetilde{A}V, \tag{4}$$

missä U ja V ovat $d_A \times d_A$ ja $d_B \times d_B$ unitaarimatriiseja, ja $\widetilde{A}$ on $d_A \times d_B$ diagonaalimatriisi, jolla on $\min(d_A, d_B)$ nollasta poikkeavaa alkiota. Sijoittamalla tämä hajotelma yhtälöön (3) saadaan

$$|\psi\rangle = \sum_{j=1}^{d_A}\sum_{i=1}^{d_B}\sum_{k=1}^{d_B} u_{ji}\tilde{a}_{ii}v_{ik}|j\rangle|k\rangle. \tag{5}$$

Koska $|j\rangle$ ja $|k\rangle$ ovat ortonormaaleja kantoja ja U ja V unitaarisia matriiseja, myös vektorien

$$|a_i\rangle = \sum_j u_{ji}|j\rangle \quad \text{ja} \quad |b_i\rangle = \sum_k v_{ik}|k\rangle \tag{6}$$

joukot ovat ortonormaaleja joukkoja $\mathcal{H}_A$:ssa ja $\mathcal{H}_B$:ssä. Huomioimalla, että $a_{ii} = 0$, kun $i > d_A$, voidaan $|\psi\rangle$ nyt kirjoittaa muotoon

$$|\psi\rangle = \sum_{i=1}^{d_A} \tilde{a}_{ii}|a_i\rangle|b_i\rangle, \tag{7}$$

ja kun vielä merkitään $\tilde{a}_{ii} \equiv \lambda_i$, saadaan haluttu esitysmuoto. Hajotelmasta nähdään osittaiset jäljet ottamalla, että λ_i^2 ovat osasysteemien tiheysmatriisien ominaisarvoja: $\rho_A = \sum_k \lambda_k^2|a_k\rangle\langle a_k|$ ja $\rho_B = \sum_k \lambda_k^2|b_k\rangle\langle b_k|$, ja edelleen nähdään matriisien ominaisarvojen olevan samat. □

Hajotelmassa esiintyviä vektoreita $|a_i\rangle$ ja $|b_i\rangle$ kutsutaan systeemien A ja B *Schmidtin kannoiksi*, ja nollasta poikkeavien kertoimien λ_i lukumäärä on tilan $|\Psi\rangle$ *Schmidtin luku* $\mathrm{Sch}(|\Psi\rangle)$. Yhdistetyn systeemin tilan Schmidtin luku on eräs tapa kuvata systeemin lomittumisen määrää: tulotiloilla se on aina 1, ja mitä suurempi se on, sitä useampi vektori tarvitaan kuvaamaan lomittuneiden systeemien tilaa. Yksösestä poikkeavaa Schmidtin lukua voidaankin pitää eräänä lomittuneen tilan määritelmänä. Schmidtin luku myös kuvaa tilan $|\Psi\rangle$ dimensiota: tilan määrittelemiseen tarvitaan $\mathrm{Sch}(|\Psi\rangle)$ ortogonaalista vektoria [5].

Koska Schmidtin hajotelma on tärkeä työkalu myöhemmin tutkielmassa, tarkastellaan kahta esimerkkiä hajotelman laskemisesta. Olkoon A ja B kubittisysteemejä, jolloin niiden Hilbertin avaruudet ovat $\mathcal{H}^2$, ja olkoon $|\Psi\rangle = \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$ puhdas tila yhdistetyssä systeemissä $\mathcal{H}_A \otimes \mathcal{H}_B$. Tilan $|\Psi\rangle$ kerroinmatriisi A on

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \tag{8}$$

jolle singulaariarvohajotelmaksi saadaan

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{9}$$

Summaamalla tästä ensimmäisen unitaarimatriisin rivien ja jälkimmäisen sarakkeiden yli yhtälön (6) mukaisesti saadaan Schmidtin kannan vektoreiksi $|a_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ systeemissä A ja $|b_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ systeemissä B. Koska matriisin $\widetilde{A}$ toinen diagonaalialkio on nolla, ei vektoreilla $|a_1\rangle$ ja $|b_1\rangle$ ole merkitystä. Näin saadaan tilan $|\Psi\rangle$ Schmidtin hajotelmaksi

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{10}$$

Tilan Schmidtin luku nähdään suoraan singulaariarvohajotelman diagonaalimatriisista: nollasta poikkeavia alkioita on vain yksi, joten $\mathrm{Sch}(|\Psi\rangle) = 1$. Tila on siis tulotila, eikä lainkaan lomittunut. Hajotelmasta voidaan edelleen laskea marginaalitiloiksi

$$\begin{aligned} \rho_A = \rho_B &= \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|), \end{aligned} \tag{11}$$

jotka tosin tässä tapauksessa olisi ollut helppoa laskea alkuperäisestäkin muodosta.

Edellistä esimerkkiä mielenkiintoisempi on kenties tapaus, jossa osasysteemien dimensiot ovat erit. Olkoon nyt A kubittisysteemi, ja B kolmiulotteinen systeemi, jonka kantavektorit ovat siis $|0\rangle$, $|1\rangle$ ja $|2\rangle$. Valitaan yhdistetyn systeemin tilaksi

$|\Psi'\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{2}}|02\rangle + \frac{1}{2\sqrt{3}}|11\rangle + \frac{1}{2\sqrt{3}}|12\rangle$. Tilan kerroinmatriisille saadaan singulaariarvohajotelmaksi

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} \end{pmatrix}$$
$$\approx \begin{pmatrix} 0,96 & -0,27 \\ 0,27 & 0,96 \end{pmatrix} \cdot \begin{pmatrix} 0,94 & 0 & 0 \\ 0 & 0,33 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0,59 & 0,08 & 0,80 \\ -0,47 & 0,84 & 0,26 \\ -0,65 & -0,53 & 0,53 \end{pmatrix},$$

josta Schmidtin kantavektoreiksi saadaan

$$|a_0\rangle = 0,96|0\rangle + 0,27|1\rangle \quad \text{ja} \quad |a_1\rangle = -0,27|0\rangle + 0,96|1\rangle \tag{12}$$

ja

$$|b_0\rangle = 0,59|0\rangle + 0,08|1\rangle + 0,80|2\rangle \quad \text{ja} \quad |b_1\rangle = -0,47|0\rangle + 0,84|1\rangle + 0,26|2\rangle. \tag{13}$$

Voitaisiin myös laskea $|b_2\rangle$, mutta se ei esiinny Schmidtin hajotelmassa: hajotelman termien lukumäärä määräytyy osasysteemeistä pienemmän dimension mukaan. Lukemalla vielä matriisin $\widetilde{A}$ diagonaalilta hajotelman Schmidtin kertoimet, saadaan tilan $|\Psi'\rangle$ Schmidtin hajotelmaksi

$$\begin{aligned} |\Psi'\rangle = {} & 0,94 \cdot \big(0,96|0\rangle + 0,27|1\rangle\big) \otimes \big(0,59|0\rangle + 0,08|1\rangle + 0,80|2\rangle\big) \\ & + 0,33 \cdot \big(-0,27|0\rangle + 0,96|1\rangle\big) \otimes \big(-0,47|0\rangle + 0,84|1\rangle + 0,26|2\rangle\big). \end{aligned} \tag{14}$$

Hajotelmasta nähdään tilan Schmidtin luvun olevan kaksi, eli tila on lomittunut.

1.4 Purifikaatio

Schmidtin hajotelmaa hyödyntäen saadaan suoraviivaisesti määriteltyä avaruuden $\mathcal{H}_A$ mielivaltaista tilaa ρ_A vastaava puhdas tila jossain suuremmassa Hilbertin avaruudessa $\mathcal{H}_A \otimes \mathcal{H}_S$, missä $\mathcal{H}_S$ on apusysteemin $\mathcal{S}$ Hilbertin avaruus. $\mathcal{H}_S$ on ainoastaan laskutekninen apuväline, eikä sillä tarvitse olla fysikaalista merkitystä. Tätä

tilan suurempaan Hilbertin avaruuteen upottamista kutsutaan *purifikaatioksi*, sillä tuloksena on aina puhdas tila. Purifikaatio on hyödyllinen operaatio käsitellessä sekoittuneita tiloja, sillä puhtaissa tiloissa ei ole lainkaan tilastollisia tai tietämättömyydestä johtuvia ominaisuuksia.

Mikä tahansa kvanttitila $\rho_A \in \mathcal{H}_A$ voidaan upottaa suurempaan Hilbertin avaruuteen $\mathcal{H}_A \otimes \mathcal{H}_S$ siten, että on olemassa jokin puhdas tila $|\Psi_{AS}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_S$, jolle $\rho_A = \mathrm{Tr}_S(|\Psi_{AS}\rangle\langle\Psi_{AS}|)$. Koska jokainen tiheysmatriisi voidaan kirjoittaa ortonormaalien vektoreiden $|\chi_k\rangle$ avulla muodossa

$$\rho_A = \sum_k \chi_k |\chi_k\rangle\langle\chi_k|, \tag{15}$$

voidaan edelleen määritellä lomittunut puhdas tila

$$|\Psi_{AS}\rangle = \sum_k \sqrt{\chi_k}|\chi_k\rangle|k\rangle, \tag{16}$$

missä $|k\rangle$ ovat avaruuden $\mathcal{H}_S$ kantavektoreita. Suoraan nähdään, että marginaalitila ρ_A on haluttua muotoa. Kvanttimekaniikan lineaarisuuden nojalla kaikki tilan ρ_A fysikaaliset ominaisuudet ovat laskettavissa myös tilasta Ψ_{AS} [5].

1.5 Hyperkiekoista

Olkoon $\mathcal{H}$ n-ulotteinen Hilbertin avaruus, ja $\mathcal{H}_S$ sen m-ulotteinen aliavaruus, jonka kanta on $\mathbf{B} = \{\phi_j\}_{j=0}^{m-1}$. Merkitään seuraavassa hyperkiekon määritelmässä puhtaiden tilojen $|\psi\rangle \in \mathcal{H}$ kerroinvektoria $\boldsymbol{r}_{\mathbf{B}}$ aliavaruudessa S

$$\boldsymbol{r}_{\mathbf{B}}(|\psi\rangle) = \left(|\langle\phi_0|\psi\rangle|, ..., |\langle\phi_{m-1}|\psi\rangle| \right)^{\mathrm{T}}. \tag{17}$$

Vektorin komponentit ovat siis tilan $|\psi\rangle$ sisätulo kunkin aliavaruuden kantavektorin kanssa.

Määritelmä 2. *Olkoon S joukko puhtaita tiloja $\mathcal{H}$:ssä. S on* hyperkiekko, *jos sen*

virittämällä aliavaruudella $\mathcal{V}_S = span(S)$ *on ortonormaali kanta* $\mathbf{B}$*, jolla*

$$\boldsymbol{r}_{\mathbf{B}}(|\psi\rangle) = \boldsymbol{r} \quad \forall |\psi\rangle \in S, \tag{18}$$

$$\boldsymbol{r}_{\mathbf{B}}(|\psi\rangle) \neq \boldsymbol{r} \quad \forall |\psi\rangle \notin S. \tag{19}$$

Tässä $\boldsymbol{r}$ *on hyperkiekon määrittävä vakiovektori, jonka kaikki komponentit ovat positiivisia [6].*

Yhtäpitävästi hyperkiekko voidaan myös määritellä d-ulotteisten hypertason ja hyperpallokuoren leikkauspintana, mistä saadaan samanlainen matemaattinen esitys.

Näiden vaatimusten perusteella nähdään, että kaikki puhtaat tilat $|\psi\rangle$ m- ulotteisella hyperkiekolla S voidaan kirjoittaa muodossa

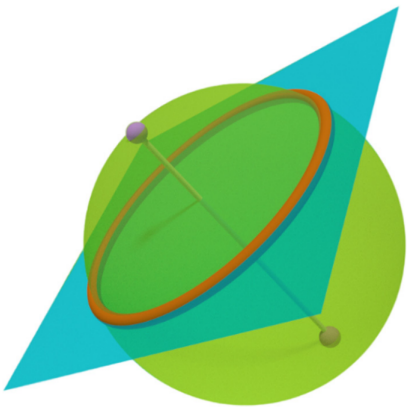
$$|\psi(\boldsymbol{\theta})\rangle = \sum_{j=1}^{m} r_j e^{i\theta_j} |\phi_j\rangle, \tag{20}$$

missä $\{|\phi_j\rangle\}$ ovat S:n ortonormaalit kantavektorit, $\theta_j \in \mathbb{R}$ ovat hyperkiekon parametrisoivan reaalivektorin $\boldsymbol{\theta}$ komponentit, ja r_j ovat hyperkiekon määrittävän vektorin $\boldsymbol{r}$ komponentit.

Esimerkkinä voidaan tarkastella tapauksia $m = 1$ ja $m = 2$. 1-ulotteinen hyperkiekko on muodossa (20) kirjoitettuna $|\psi(\theta)\rangle = re^{i\theta}|\phi\rangle$, jossa globaalilla vaiheella $e^{i\theta}$ ei ole merkitystä. Se koostuu siis vain yhdestä puhtaasta tilasta. Kun $m = 2$, hyperkiekko on tilajoukko $\{|\psi\theta\rangle = a|\phi_0\rangle + be^{i\theta}|\phi_1\rangle | a, b, \theta \in \mathbb{R}\}$, missä jälleen globaali vaihe on vähennetty termeistä. 2-ulotteinen hyperkiekko koostuu siis niistä tiloista, jotka ovat vakioetäisyydellä kantavektoreista. Kuvassa 1 on esitetty esimerkkinä kaksiulotteinen hyperkiekko tason ja Blochin pallon leikkauksena.

Tärkeä erikoistapaus hyperkiekosta on *Schmidtin hyperkiekko*. Hyperkiekko yhdistetyn systeemin Hilbertin avaruudessa $\mathcal{H}_A \otimes \mathcal{H}_B$ on Schmidtin hyperkiekko, kun

$$|\Psi(\boldsymbol{\theta})\rangle = \sum_{j=1}^{d} r_j e^{i\theta_j} |\phi_j^A \phi_j^B\rangle, \tag{21}$$



Kuva 1. Kaksiulotteisen hyperkiekon geometrinen esitys. Vihreän Blochin pallon ja turkoosin tason leikkauksena saadaan punaisella merkitty hyperkiekko. Merkityt pisteet Blochin pallon navoilla ovat hyperkiekon kantavektorit, ja nähdään, että hyperkiekolle kuuluvat ne tilat, jotka ovat vakioetäisyydellä näistä navoista. Huomionarvoista on, että navat eivät ole kiinnitettyjä tiloja, vaan kantaa vaihtamalla voidaan vaihtaa palloa leikkaavan tason orientaatiota. Kuva artikkelista [6].

missä $\boldsymbol{\theta} \in \mathbb{R}^d$, $r_j \neq 0$ ja $\{|\phi_j^A \phi_j^B\rangle\}_{j=0}^{d-1}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$:n ortonormaali kanta. Oleellisesti hyperkiekko on Schmidtin hyperkiekko vain, kun $\{|\phi_j^A \phi_j^B\rangle\}_{j=0}^{d-1}$ on Schmidtin kanta — kaikki yhdistetyn systeemin hyperkiekot eivät ole Schmidtin hyperkiekkoja. Esimerkiksi hyperkiekko $|\Psi'(\theta)\rangle = \frac{1}{\sqrt{3}}(|00\rangle + e^{i\theta}(|01\rangle + |10\rangle)) \in \mathcal{H}^2 \otimes \mathcal{H}^2$ ei ole Schmidtin hyperkiekko, sillä $|01\rangle + |10\rangle$ ei ole tulotila ja näin ollen ei kuulu yhteenkään Schmidtin kantaan. Voidaan kuitenkin nähdä, että $|\Psi'(\theta)\rangle$ kuuluu Schmidtin hyperkiekolle $|\Psi(\theta_1, \theta_2)\rangle = \frac{1}{\sqrt{3}}(|00\rangle + e^{i\theta_1}|01\rangle + e^{i\theta_2}|10\rangle)$, kun $\theta_1 = \theta_2$.

Edelleen voidaan määritellä *alihyperkiekko*: olkoon $\mathcal{S}$ hyperkiekko. Sen osajoukko $\mathcal{S}' \subseteq \mathcal{S}$ on alihyperkiekko, mikäli $\mathcal{S}'$ on myös hyperkiekko. Edellisessä esimerkissä siis $|\Psi'(\theta)\rangle$ on hyperkiekon $|\Psi(\theta_1, \theta_2)\rangle$ alihyperkiekko.

Määritellään vielä hyperkiekon *säännöllinen osajoukko*: olkoon $\mathcal{S}$ hyperkiekko. $\mathcal{C}$ on sen säännöllinen osajoukko, jos

$$\mathcal{V}_\mathcal{C} \cap \mathcal{S} = \mathcal{C}, \tag{22}$$

missä $\mathcal{V}_\mathcal{C} = \mathrm{span}(\mathcal{C})$.

Lemma 2. *Jos $\mathcal{C}$ on $\mathcal{S}$:n säännöllinen osajoukko, ehdot* $\dim(\mathcal{C}) = \dim(\mathcal{S})$ *ja* $\mathcal{C} = \mathcal{S}$ *ovat yhtäpitävät.*

Todistus. Koska $\mathcal{C}$ on $\mathcal{S}$:n osajoukko, sen virittämä avaruus $\mathcal{V}_\mathcal{S}$ on $\mathcal{S}$:n virittämän avaruuden $\mathcal{V}_\mathcal{S}$ aliavaruus. Toisaalta tällöin jos $\dim(\mathcal{C}) = \dim(\mathcal{S})$, ne virittävät saman avaruuden, $\mathcal{V}_\mathcal{S} = \mathcal{V}_\mathcal{C}$. Tästä seuraa, että $\mathcal{C} = \mathcal{V}_\mathcal{C} \cap \mathcal{S} = \mathcal{V}_\mathcal{S} \cap \mathcal{S} = \mathcal{S}$. Ehdosta $\mathcal{C} = \mathcal{S}$ seuraa triviaalisti, että avaruuksien ulottuvuudet ovat samat. □

Säännöllisillä osajoukoilla on roolinsa luvussa 3.2, kun tarkastellaan naamioitavan joukon rakennetta. Luvussa hyödynnetään myös seuraavaa lemmaa, jonka todistus sivuutetaan sen pituuden vuoksi [6].

Lemma 3. *Äärellisulotteisen hyperkiekon kaksiulotteinen säännöllinen osajoukko on joko kaksi erillistä puhdasta tilaa tai kaksiulotteinen hyperkiekko.*

2 Mitä on kvantti-informaation naamiointi?

Tässä luvussa esitellään kvantti-informaation naamiointioperaatio. Ennen varsinaisen kvantti-informaation naamioinnin määrittelemästä havainnollistetaan operaatiota vastaavalla klassisella toimituksella.

2.1 Klassinen informaation naamiointi

Klassinen informaation naamiointi voidaan ajatella tavallisena kryptografisena salaustoimituksena. Esimerkkinä voidaan tarkastella Caesar-salakirjoitus, jossa jokainen viestin kirjain korvataan kirjaimella, joka on tietyn määrän alkuperäistä kirjainta myöhempänä tai aiempana aakkostossa. Esimerkiksi neljän kirjaimen siirto eteenpäin tarkoittaa, että viestissä *a* korvataan *e*:llä, *b* korvataan *f*:llä ja niin edelleen, kunnes aakkoston lopussa siirto kierretään päädyn ympäri, ja *ö* korvataan *d*:llä. Salausavaimena toimii tieto siitä, millä kirjaimella mikäkin kirjain korvataan.

Tarkastellaan esimerkkinä klassista naamiointioperaatiota. Olkoon Aliisa ja Petri naamiointioperaation osapuolet. Aliisalla on hallussaan naamioitava viesti `INFORMAATIO`, ja Petrin hallussa on käytettävä salausavain, neljän kirjaimen siirto eteenpäin. Naamiointi tapahtuu yhdistämällä osapuolten informaatiot salaamalla Aliisan viesti Petrin salausavaimella ja hävittämällä alkuperäinen viesti. Tällöin salattu viesti on

I N F O R M A A T I O →

M R J S V Q E E X M S.

Nyt osapuolilla on hallussaan salattu viesti ja salausavain, joista kumpikaan yksinään ei teoriassa sisällä lainkaan alkuperäisen viestin informaatiota. Voidaan siis ajatella, että viesti on hajautettu osapuolten välisiin korrelaatioihin, ja vain molempia systeemejä yhdessä tutkimalla voidaan saada selville alkuperäisen viestin sisältö. Näin yksinkertaisen esimerkin kanssa tietenkin nähdään, että käytännössä on triviaalia purkaa koodaus ja selvittää salatun viestin sisältö. Modernimmilla kryptografisilla menetelmillä salausta ei ole yhtä helppo purkaa ja voidaan käytännössäkin ajatella informaation olevan hajautettu yhdistetylle systeemille.

Terminologia klassisessa tapauksessa on hieman epätarkkaa, sillä naamiointiprotokollaa on tarpeeton määritellä tuhansia vuosia tunnetun salausprosessin yhteydessä. Kvantti-informaatiolla ero naamioinnin ja muiden vastaavien prosessien välillä on kuitenkin selvä.

2.2 Kvantti-informaation naamiointi

Kvantti-informaation naamioinnille voidaan antaa kaksi hieman toisistaan poikkeavaa määritelmää. Alkuperäisessä Modin *et al.* [2] määritelmässä systeemin A sisältämä kvantti-informaatio siirretään A:n sisältävän yhdistetyn systeemin korrelaatioihin, kun taas vaihtoehtoisessa mm. Dingin *et al.* [6] käyttämässä määritelmässä tuomarisysteemin R informaatio jaetaan yhdistetylle systeemille AB. Seuraavaksi

esitellään tämä vaihtoehtoinen määritelmä, sillä se sallii monipuolisemman tarkastelun.

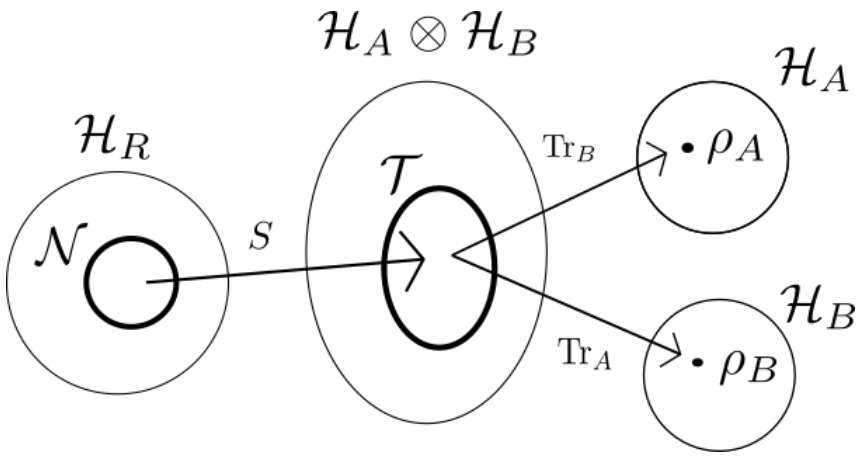
Määritelmä 3. *Olkoon R tuomarisysteemi, jonka sisältämä kvantti-informaatio naamioidaan, ja A ja B systeemejä, jotka muodostavat maalisysteeminä toimivan yhdistetyn kvanttisysteemin $\mathcal{H}_A \otimes \mathcal{H}_B$. Olkoon $\mathcal{N}$ joukko puhtaita tiloja $\mathcal{H}_R$:ssä. Joukon $\mathcal{N}$* naamiointioperaatio *on lineaarinen isometria $S : \mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B$, joka kuvaa tilajoukon $\mathcal{N}$ tilat $|\psi_k\rangle \in \mathcal{N}$ yhdistetyn systeemin puhtaiksi tiloiksi $S|\psi_k\rangle = |\Psi_k\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ siten, että tilan $|\Psi_k\rangle$ marginaalitilat ovat identtisiä kaikilla k:n arvoilla:*

$$\rho_A = Tr_B(\rho_k) \quad ja \quad \rho_B = Tr_A(\rho_k) \quad \forall k, \tag{23}$$

missä $\rho_k = |\Psi_k\rangle\langle\Psi_k|$ on yhdistetyn systeemin $\mathcal{H}_A \otimes \mathcal{H}_B$ tiheysmatriisi, ja $\rho_{A,B}$ ovat osasysteemien tiheysmatriisit. Joukkoon $\mathcal{N}$ kuulumattomat tilat $|\psi'\rangle \notin \mathcal{N}$ kuvautuvat tiloiksi, joille ehdon (23) *ei tarvitse täyttyä. Ehtoon* (23) *viitataan vastedes* naamiointiehtona. *Joukko $\mathcal{N}$ on naamiointioperaatiota S vastaava* naamioitava joukko. *Naamioitavasta joukosta saadaan määriteltyä* maalijoukko $\mathcal{T} = V(\mathcal{N}) \subset \mathcal{H}_A \otimes \mathcal{H}_B$.

Naamioinnin määritteleminen tuomarisysteemin kanssa sallii myös sen, että naamiointikone voidaan kuvata lineaarisena isometriana, kun taas alkuperäisessä määritelmässä naamiointikonetta kuvattiin unitaarioperaattorilla. Unitaarioperaattorilla $U : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$ lähtö- ja maaliavaruuksien dimensioiden tulee olla samat. Tällöin lähtöpuoli joudutaan täyttämään systeemin B aputilalla $|b\rangle$, jolla ei ole mitään merkitystä naamiointioperaation kannalta. Määrittelemällä naamiointioperaatio yleisemmin lineaarisena isometriana vähennetään siis yksi tarvittava parametri naamioinnin kuvaamisesta, ja näin määritelmä yksinkertaistuu.

Alkuperäinen määritelmä nähdään erikoistapaukseksi edellä olevasta vaihtoehtoisesta määritelmästä, kun valitaan tuomarisysteemiksi systeemi A, jolloin $R = A$. Tämä valinta on jossain määrin naamioinnin tutkimista rajoittava, sillä esimerkiksi kubitin naamiointia 3-ulotteiseen systeemiin ei ole mahdollista tarkastella. Toisinaan



Kuva 2. Naamiointikuvauksessa S systeemin R naamioitavan joukon $\mathcal{N}$ tilat kuvataan yhdistetyn systeemin $\mathcal{H}_A \otimes \mathcal{H}_B$ joukkoon $\mathcal{T}$. Joukko $\mathcal{T}$ sisältää sellaiset tilat, joille naamiointiehto (23) täyttyy: jokaisen tilan $|\Psi_k\rangle \in \mathcal{T}$ marginaalitilat ovat samat, $\mathrm{Tr}_X(|\Psi_k\rangle\langle\Psi_k|) = \rho_Y \ \forall k$. Kuva artikkelia [7] mukaillen.

kuitenkin käsitellään esimerkiksi vain kubitti-kubitti -naamiointia, jolloin määritelmän valinnalla ei ole juurikaan merkitystä.

Naamiointioperaatiota ei ole rajattu vain kahteen osasysteemiin, vaan on mahdollista määritellä edeltävää vastaava operaatio V_m, joka kuvaa systeemin R tilat $|\psi_k\rangle$ n:stä osasysteemistä koostuvan yhdistetyn systeemin $\otimes_{j=1}^{n}\mathcal{H}_{A_j}$ tiloiksi $\{|\Psi_k\rangle \in \otimes_{j=1}^{n}\mathcal{H}_{A_j}\}$. Tilojen marginaalitilat $\mathrm{Tr}_{\widehat{A_j}}(|\Psi_k\rangle\langle\Psi_k|)$, missä $\widehat{A_j} = \{A_i\}_{i\neq j}$, ovat riippumattomia k:sta jokaisella osasysteemillä A_j [8]. Luvussa 3 nähdään, että useamman kuin kahden osallistujan naamiointioperaation naamioitava joukko on koko lähtöavaruus, $\mathcal{N} = \mathcal{H}_R$.

Yksinkertaisena esimerkkinä naamioinnista voidaan tarkastella klassisen bitin naamiointia kvanttisysteemeissä [2]. Tällöin mahdolliset systeemin R alkutilat ovat $\{|0\rangle, |1\rangle\}$. Määritellään naamiointikuvaus

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Psi_0\rangle \quad \text{ja} \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Psi_1\rangle, \tag{24}$$

joka nähdään helposti lineaariseksi isometriaksi: kantavektorit kuvautuvat lineaari-

sesti riippumattomiksi maaliavaruuden vektoreiksi, ja

$$|| \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) || = \frac{1}{2}(|| \, |00\rangle \, || + || \, -|11\rangle \, ||) = \frac{1}{2}(1+1) = 1,$$

missä Hilbertin avaruuden sisätulon indusoiman metriikan mukaisesti $|| \, |ii\rangle \, || = |\langle ii|ii\rangle| = |\langle i|i\rangle\langle i|i\rangle| = 1$.

Nyt tiheysmatriisit $\rho_k = |\Psi_k\rangle\langle\Psi_k|$ yhdistetylle systeemille ovat

$$\rho_0 = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \tag{25}$$

ja

$$\rho_1 = \frac{1}{2}(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|). \tag{26}$$

Laskemalla tiheysmatriiseista marginaalitilat osasysteemeille nähdään suoraan ristitermien katoavan, jolloin saadaan kummallekin systeemille

$$\rho_X = \mathrm{Tr}_Y(\rho_0) = \mathrm{Tr}_Y(\rho_1) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|), \tag{27}$$

missä $X = A, B$ ja vastaavasti $Y = B, A$. Lopputilan marginaalitilat eivät siis riipu alkuperäisestä naamioitavan bitin arvosta, mutta yhdistetyn systeemin tilasta ero alkutiloissa on havaittavissa. Luvussa 3 tarkastellaan, mitä tapahtuu, kun bitti korvataan kubitilla, jonka mahdolliset alkutilat kuuluvat vektorien $\{|0\rangle, |1\rangle\}$ virittämään Hilbertin avaruuteen.

3 Milloin naamiointi on mahdollista?

Naamiointi kuuluu joukkoon kvantti-informaatioteorian operaatioita, joihin liittyy vastaava kieltolause (engl. *no-go theorem*). Kieltolauseet määrittelevät, missä tila-avaruuden osassa operaatio on mahdollinen — tai kenties ennemmin missä osassa mahdoton. Kvantti-informaation naamiointi esiteltiin ensimmäistä kertaa juurikin siihen liittyvän kieltolauseen yhteydessä [2]. Artikkelissa osoitettiin, että yksikään naamiointioperaatio ei pysty naamioimaan kaikkia alkutiloja.

3.1 Naamioinnin kieltolause

Tässä alaluvussa esittelen kieltolauseen todistuksen d-ulotteiselle kvanttisysteemille Modia *et al.* [2] ja Zhua [9] mukaillen. Koska naamiointi on kohtalaisen uusi operaatio kvantti-informaation saralla, kieltolauseelle on esitetty joitain erilaisia todistuksia. Pääosin kuitenkin todistuksen rakenne on kaikissa muotoiluissaan samanlainen.

Lause 4. *Yhdellä naamiointikoneella S ei ole mahdollista naamioida mielivaltaista kvanttitilaa.*

Todistus. Todistetaan lause ristiriidan kautta. Olkoon naamioinnin osapuolina lähtösysteemi R ja maalisysteemi AB, joiden Hilbertin avaruudet ovat $\mathcal{H}_R$ ja $\mathcal{H}_A \otimes \mathcal{H}_B$. Olkoon S naamiointikone, joka pystyy naamioimaan mielivaltaisen tilan. Valitaan kaksi tilaa, $|s_0\rangle$ ja $|s_1\rangle \in \mathcal{H}_R$, joille määritellään kuvaukseksi $|s_0\rangle \to |\Psi_0\rangle$ ja $|s_1\rangle \to |\Psi_1\rangle$, missä $|\Psi_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.

Naamioinnin määritelmän mukaisesti $\rho_A = \mathrm{Tr}_B(|\Psi_i\rangle\langle\Psi_i|)$, $i = 0, 1$. Tällöin puhtaat tilat $|\Psi_i\rangle$ voidaan tulkita tilan ρ_A purifikaatioiksi $\mathcal{H}_A \otimes \mathcal{H}_B$:ssä. Kun $\rho_A = \sum_k \lambda_k |a_k\rangle\langle a_k|$, missä $|a_k\rangle$ ovat ortonormaaleja tiloja, voidaan tilat $|\Psi_i\rangle$ kirjoittaa Schmidtin hajotelmina muotoon

$$|\Psi_i\rangle = \sum_k \sqrt{\lambda_k} |a_k\rangle |b_k^{(i)}\rangle, \tag{28}$$

missä $|b_k^{(i)}\rangle$ ovat ortonormaaleja tiloja $\mathcal{H}_B$:ssä kullakin i:llä. Vastaavasti tietenkin naamiointiehdon mukaan systeemin B tiloille pätee

$$\mathrm{Tr}_A(|\Psi_i\rangle\langle\Psi_i|) = \sum_k \lambda_k |b_k^{(i)}\rangle\langle b_k^{(i)}| = \rho_B \quad \forall i.$$

Tarkastelu voitaisiin suorittaa symmetrisesti tulkitsemalla tilat $|\Psi_i\rangle$ tilojen ρ_B purifikaatioiksi, mutta riittää tarkastella vain naamiointiehdon toista puolta, sillä naamioitavalle joukolle saadaan asetettua rajoituksia näinkin.

Lähtöoletuksen mukaan naamiointikone pystyy naamioimaan myös mielivaltaisen superpositiotilan $\mu|s_0\rangle + \nu|s_1\rangle \to |\Psi\rangle$, missä $|\mu|^2 + |\nu|^2 = 1$. Tällöin naamioin-

tiehdon mukaan

$$\mathrm{Tr}_A(|\Psi_i\rangle\langle\Psi_i|) = \mathrm{Tr}_A(|\Psi\rangle\langle\Psi|) = \rho_B, \tag{29}$$

johon sijoittamalla superpositiotila $|\Psi\rangle$ saadaan

$$\begin{aligned}
\rho_B &= \mathrm{Tr}_A(|\Psi\rangle\langle\Psi|) && (30)\\
&= |\mu|^2\mathrm{Tr}_A\left(|\Psi_0\rangle\langle\Psi_0|\right) + |\nu|^2\mathrm{Tr}_A\left(|\Psi_1\rangle\langle\Psi_1|\right) && (31)\\
&\quad + \mu\nu^*\mathrm{Tr}_A\left(|\Psi_0\rangle\langle\Psi_1|\right) + \mu^*\nu\mathrm{Tr}_A\left(|\Psi_1\rangle\langle\Psi_0|\right)\\
&= (|\mu|^2 + |\nu|^2)\rho_B + \mu\nu^*\mathrm{Tr}_A\left(|\Psi_0\rangle\langle\Psi_1|\right) + \mu^*\nu\mathrm{Tr}_A\left(|\Psi_1\rangle\langle\Psi_0|\right) && (32)\\
&= \rho_B + \mu\nu^*\mathrm{Tr}_A\left(|\Psi_0\rangle\langle\Psi_1|\right) + \mu^*\nu\mathrm{Tr}_A\left(|\Psi_1\rangle\langle\Psi_0|\right). && (33)
\end{aligned}$$

Naamiointiehto täyttyy superpositiotilalla, kun edellisen yhtälön ristitermit katoavat:

$$\mu\nu^*\mathrm{Tr}_A\left(|\Psi_0\rangle\langle\Psi_1|\right) + \mu^*\nu\mathrm{Tr}_A\left(|\Psi_1\rangle\langle\Psi_0|\right) = 0. \tag{34}$$

Sijoittamalla tähän yhtälöön tilojen $|\Psi_i\rangle$ Schmidtin hajotelmat (28) saadaan se edelleen muotoon

$$\mu\nu^*\mathrm{Tr}_A\left(\sum_k \lambda_k|a_k\rangle|b_k^{(0)}\rangle\langle b_k^{(1)}|\langle a_k|\right) + \mu^*\nu\mathrm{Tr}_A\left(\sum_k \lambda_k|a_k\rangle|b_k^{(1)}\rangle\langle b_k^{(0)}|\langle a_k|\right) = 0,$$

josta osittaiset jäljet auki laskemalla saadaan

$$\mu\nu^*\sum_k \lambda_k|b_k^{(0)}\rangle\langle b_k^{(1)}| + \mu^*\nu\sum_k \lambda_k|b_k^{(1)}\rangle\langle b_k^{(0)}| = 0. \tag{35}$$

Ottamalla edellisestä odotusarvo tilan $|b_j^{(0)}\rangle$ suhteen saadaan

$$\lambda_j\left(\mu\nu^*\langle b_j^{(0)}|b_j^{(1)}\rangle + \mu^*\nu\langle b_j^{(1)}|b_j^{(0)}\rangle\right) = 0. \tag{36}$$

$\lambda_j = 0$ ei kelpaa ratkaisuksi, sillä silloin $\rho_A = \sum_j \lambda_j|a_j\rangle\langle a_j| = 0$. Ratkaistavaksi jää siis yhtälö

$$\mu\nu^*\langle b_j^{(0)}|b_j^{(1)}\rangle + \mu^*\nu\langle b_j^{(1)}|b_j^{(0)}\rangle = 0, \tag{37}$$

joka toteutuu, kun $\langle b_j^{(1)}|b_j^{(0)}\rangle = 0$, $\mu = 0$, $\nu = 0$ tai $\mu\nu^*\langle b_j^{(1)}|b_j^{(0)}\rangle = -\overline{\mu\nu^*\langle b_j^{(1)}|b_j^{(0)}\rangle}$, eli $\mu\nu^*\langle b_j^{(1)}|b_j^{(0)}\rangle$ on puhtaasti imaginaarinen.

Ratkaisu $\langle b_j^{(1)}|b_j^{(0)}\rangle = 0$ vastaa tilannetta, jossa $|\Psi_0\rangle$ ja $|\Psi_1\rangle$ ovat ortogonaalisia. Koska naamiointikone oletuksen mukaan pystyy naamioimaan mielivaltaisen tilan ja naamiointikuvaus on lineaarinen isometria, voidaan aina valita sellaiset lähtötilat $|s_0\rangle$ ja $|s_1\rangle$, että $|\Psi_0\rangle$ ja $|\Psi_1\rangle$ eivät ole ortogonaalisia, ja näin ollen $\langle b_j^{(1)}|b_j^{(0)}\rangle = 0$ ei kelpaa yleiseksi ratkaisuksi. Muissa ratkaisuissa kertoimet μ ja ν eivät ole vapaasti valittavissa, ja näin ollen naamiointikoneella S ei ole mahdollista naamioida mielivaltaista superpositiotilaa $|\Psi\rangle$. □

Esimerkkinä kieltolauseen seurauksista voidaan tarkastella aiemmin määriteltyä bittien naamiointikuvausta (24), mutta käyttämällä alkutiloina bittien sijaan kubitteja. Tällöin siis mahdolliset alkutilat ovat muotoa $\mu|0\rangle + \nu|1\rangle$. Suoraviivaisesti sijoittamalla kuvauksen mukaisesti määritellyt tilat $|\Psi_0\rangle$ ja $|\Psi_1\rangle$ ylläolevaan todistukseen saadaan yhtälö (34) muotoon

$$\frac{\mu\nu^*}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|) + \frac{\mu^*\nu}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|) = 0 \tag{38}$$

$$(\frac{\mu\nu^*}{2} + \frac{\mu^*\nu}{2})(|0\rangle\langle 0| - |1\rangle\langle 1|) = 0, \tag{39}$$

$$\tag{40}$$

missä

$$\mathrm{Tr}_A(|\Psi_0\rangle\langle\Psi_1|) = \mathrm{Tr}_A(|\Psi_1\rangle\langle\Psi_0|) = \frac{1}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|). \tag{41}$$

Koska $(|0\rangle\langle 0| - |1\rangle\langle 1|) \neq 0$, on edessä olevan kertoimen oltava 0, eli

$$\frac{\mu\nu^*}{2} + \frac{\mu^*\nu}{2} = 0 \tag{42}$$

$$\mu\nu^* = -\mu^*\nu = -(\mu\nu^*)^*. \tag{43}$$

Kuten kieltolauseen todistuksessa, tämä ehto toteutuu vain, kun $\mu = 0$, $\nu = 0$ tai $\mu\nu^*$ on puhtaasti imaginaarinen. Näin ollen naamiointikuvaus (24) ei pysty naamioimaan mielivaltaista kubittitilaa.

3.2 Naamioitavan joukon rakenne

Modi *et al.*[2] osoittivat, että vaikka yhdellä naamiointioperaatiolla ei ole mahdollista naamioida mielivaltaista tilaa, naamioitavien tilojen joukko on tila-avaruudessa jatkuva ja ylinumeroituvan ääretön. Toisaalta kaikkien tilojen joukossa naamioitavien tilojen osajoukko on nollamittainen: jos valitaan kaikkien tilojen joukosta satunnainen tila, todennäköisyys osua johonkin naamioitavan joukon tilaan on 0. Artikkelissa esitettiin konjektuuri, jonka mukaan kaikki naamioitavat joukot sijaitsevat jollakin hyperkiekolla. Konjektuuri on sittemmin todistettu oikeaksi kubittisysteemeille muun muassa artikkelissa [10], mutta toisaalta osoitettu epätäydelliseksi useampiulotteisille systeemeille [6]. Todistus naamioitavan joukon ylinumeroituvuudelle on melko suoraviivainen ja esittelee hyperkiekkokonjektuurin idean.

Lause 5. *On olemassa ylinumeroituva joukko tiloja, jotka on mahdollista naamioida yhdellä naamiontikoneella [2].*

Todistus. Olkoon $\{|k\rangle\}_{k=1}^{d}$ ortonormaali kanta avaruudelle $\mathcal{H}_R$. Määritellään naamiointikone $S^\sharp : \mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B$ seuraavasti:

$$S^\sharp : |k\rangle \to |k\rangle|k\rangle. \tag{44}$$

Osoitetaan, että $S^\sharp$ voi naamioida kaikki tilat, jotka kuuluvat hyperkiekolle $|a(\boldsymbol{\theta})\rangle = d^{-1/2}\sum_k e^{i\theta_k}|k\rangle$. Tilojen sisältämä kvantti-informaatio on koodattu jatkuviin parametreihin $\{\theta_k \in [-\pi, \pi]\}$. Operoimalla $S^\sharp$:lla tällaiseen tilaan saadaan

$$S^\sharp|a\rangle = S^\sharp\left(\frac{1}{\sqrt{d}}\sum_k e^{i\theta_k}|k\rangle\right) = \frac{1}{\sqrt{d}}\sum_k e^{i\theta_k}|k\rangle|k\rangle \equiv |\Psi\rangle. \tag{45}$$

Tilan $|\Psi\rangle$ marginaalitilat ovat

$$\begin{aligned}
\mathrm{Tr}_A|\Psi\rangle\langle\Psi| &= \mathrm{Tr}_A\left(\frac{1}{\sqrt{d}}\sum_k e^{i\theta_k}e^{-i\theta_k}|k\rangle\langle k| \otimes |k\rangle\langle k|\right) \\
&= \frac{1}{\sqrt{d}}\sum_{h,k} e^{i\theta_k - i\theta_k}\langle h|k\rangle\langle k|h\rangle \otimes |k\rangle\langle k| \\
&= \frac{1}{\sqrt{d}}\sum_k \mathbf{I}_A \otimes |k\rangle\langle k|,
\end{aligned}$$

missä $\{|k\rangle\}$ ovat $\mathcal{H}_B$ kantavektoreita, ja vastaavasti

$$\mathrm{Tr}_B|\Psi\rangle\langle\Psi| = \frac{1}{\sqrt{d}}\sum_n |n\rangle\langle n| \otimes \mathbf{I}_B,$$

missä $\{|n\rangle\}$ ovat avaruuden $\mathcal{H}_A$ kantavektoreita. Marginaalitilat eivät selvästi riipu parametreistä θ_k, joten ne eivät sisällä lainkaan alkuperäistä informaatiota. Hyperkiekko sisältyy siis naamiointikoneen $S^\sharp$ naamioitavaan joukkoon. Koska parametrit θ_k ovat jatkuvia, naamioitava joukko on ylinumeroituvasti ääretön. □

Toisaalta vaikka naamioitava joukko voi olla ylinumeroituvasti ääretön, kaikkien tilojen joukossa se on nollamittainen. Tämä on intuitiivisesti nähtävissä edelliselle esimerkkikuvaukselle kubittien tapauksessa kuvasta 1: Blochin pallolla hyperkiekko on vain ympyrä pallon pinnalla, ja yksiulotteisen objektin kaksiulotteinen mitta on nolla. Intuitiivisen selityksen lisäksi artikkelissa [11] esitettiin seuraava lause, joka vastaa kysymykseen, onko mahdollista kehitellä naamiointioperaatio, jolla pystyttäisiin naamioimaan ei-nollamittainen joukko.

Lause 6. *Ei ole olemassa lineaarista isometriaa, joka pystyisi naamioimaan ei-nollamittaisen joukon puhtaita tiloja.*

Lauseen todistus on pitkä ja vaatii paneutumista mittateoriaan, joten se sivuutetaan tässä.

3.3 Yleinen naamioitavan joukon rakenne

Jatkuvan naamioitavan joukon todistuksessa osoitettiin, että määritelmän (44) mukainen naamiointikone pystyy naamioimaan jonkin hyperkiekon kaikki tilat. Modi *et al.* [2] esittivätkin tämän pohjalta konjektuurin, jonka mukaan jokaista naamiointikonetta vastaava naamioitava joukko sijaitsee kokonaisuudessaan jollakin hyperkiekolla. Konjektuurissa ei otettu kantaa siihen, voisiko joukon rakenne riippua lähtöavaruuden dimensiosta d, ja sittemmin muun muassa Liang *et al.* [10] ovat esittäneet todistuksen konjektuurille, kun $d = 2$.

Useampiulotteisessa tapauksessa joukon rakenne voi kuitenkin olla monipuolisempi. Seuraava tarkastelu mukailee artikkelia [6], jossa joukon rakennetta tutkittiin tarkemmin. Naamioitavan joukon rakenteen tarkastelua helpottaa, kun huomataan, että maalijoukko $\mathcal{T}$ on isomorfinen naamioitavan joukon kanssa $\mathcal{R}$: naamiointikuvaus lineaarisena isometriana säilyttää kuvattavan joukon rakenteen. Havainto on tarkastelun kannalta edullinen, sillä naamiointiehto on rajoitus nimenomaan maalijoukon tiloille. Voidaan siis tarkastella, millaisen rakenteen naamiointiehto asettaa maalijoukolle, ja sivutuotteena saadaan naamioitavan joukon rakenne.

Määritellään vielä yksi apujoukko tarkastelua varten: olkoon joukko $\mathcal{L}$ *lailliset tilat*, ne tilat $\mathcal{H}_A \otimes \mathcal{H}_B$:ssä, joille naamiointiehto täyttyy. Näiden tilojen ei välttämättä tarvitse kuulua naamioitavan joukon kuvajoukkoon naamiointikuvauksessa. Yhdistämällä laillisten tilojen joukko $\mathcal{L}$ ja niiden tilojen joukko, jotka saadaan $\mathcal{H}_R$:stä lineaarisella isometrialla, $\mathrm{span}(\mathcal{T}) \equiv \mathcal{V}_\mathcal{T}$, voidaan maalijoukko $\mathcal{T}$ kirjoittaa muodossa

$$\mathcal{T} = \mathcal{V}_\mathcal{T} \cap \mathcal{L}. \tag{46}$$

Tästä voidaan havaita yhteys säännöllisiin osajoukkoihin ja niitä koskevaan lemmaan 3, ja lemmaa tullaankin hyödyntämään tarkastellessa kubittisysteemien naamiointia.

Yleisyyttä loukkaamatta voidaan asettaa $\mathcal{H}_R = \mathrm{span}(\mathcal{R})$, sillä naamioitavaan joukkoon kuulumattomat tilat eivät vaikuta tarkasteluun mitenkään. Merkitään tässä luvussa $\dim(\mathcal{H}_R) = \dim(\mathrm{span}(\mathcal{T})) = n$ ja $\dim(\mathrm{span}\mathcal{L}) = d$. Lailliset tilat $\mathcal{L}$ ovat sellaisia lomittuneita tiloja, joiden tiheysmatriisit ovat d-ulotteisia, eli niiden Schmidtin luku on d. Asetetaan myös maalisysteemin osasysteemien dimensioiksi $\mathcal{H}_{A,B} = d$, koska laillisten tilojen joukkoon kuulumattomat tilat eivät vaikuta tarkasteluun.

Marginaalitilojen $\rho_{A,B}$ degeneraatiosta — tiheysmatriisien yksikäsitteisten ominaisarvojen määrästä — riippuen naamioitavalle joukolle saadaan useampi erilainen

hyperkiekkojen yhdisteistä koostuva rakenne. Tarkastellaan ensin yleisellä tasolla naamioitavan joukon rakennetta erilaisten degeneraatioiden tapauksissa, jonka jälkeen tutkitaan esimerkkitapauksina kubittien naamioimista ja 3-ulotteisten systeemien naamioimista. Kubiteille saadaan hyperkiekkokonjektuurin vahvistava tulos, mutta 3-ulotteisessa tapauksessa konjektuuri ei päde: kaikki naamioitavat tilat eivät sijaitse samalla hyperkiekolla.

Degeneroitumaton tapaus

Degeneroitumattomassa tapauksessa marginaalitilat ovat muotoa

$$\rho_A = \sum_{j=1}^{d} \lambda_j |a_j\rangle\langle a_j| \quad \text{ja} \quad \rho_B = \sum_{j=1}^{d} \lambda_j |b_j\rangle\langle b_j|, \tag{47}$$

missä $\lambda_j \neq \lambda_k$, kun $j \neq k$. Helposti nähdään, että lailliset tilat ovat muotoa

$$|\Psi(\boldsymbol{\theta})\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j} e^{i\theta_j} |a_j b_j\rangle, \tag{48}$$

joka tunnistetaan d-ulotteiseksi Schmidtin hyperkiekoksi. Yhtälöstä (46) nähdään, että maalijoukko on korkeintaan d-ulotteinen. Lemman 2 mukaan nähdään, että jos $n = d$, jos tuomarisysteemin ja osanottajasysteemien dimensiot ovat samat, maalijoukko ja siis myös naamioitava joukko on d-ulotteinen hyperkiekko.

Voidaan myös tarkastella tilannetta, jossa $n < d$, eli tuomarisysteemin informaatio naamioidaan suurempidimensioisiin osanottajasysteemeihin. Tällöin maalijoukko voi koostua useammista hyperkiekoista, jotka eivät välttämättä ole kaikki yhden hyperkiekon alihyperkiekkoja. Esimerkki tällaisesta joukosta löytyy artikkelin [6] luvusta IIIA. Joukon esittely on melko pitkä eikä kovin mielenkiintoinen, joten se sivuutetaan.

Täysin degeneroitunut tapaus

Marginaalitilat ovat täysin degeneroituneita, kun kaikki tiheysmatriisien ominaisarvot ovat samat, eli

$$\rho_{A,B} = \mathbf{I}/d = \frac{1}{d}\sum_{j=1}^{d}|j\rangle\langle j|. \tag{49}$$

Tämän tilanteen määritelmän mukaisesti toteuttavat maksimaalisesti lomittuneet tilat, jotka ovat muotoa

$$|\Psi(U)\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d} U\otimes\mathbb{I}|j\rangle|j\rangle = U\otimes\mathbb{I}|\Phi_{\mathbb{I}}\rangle, \tag{50}$$

missä U on d-ulotteinen unitaarioperaattori toiselle osasysteemille ja

$$|\Phi_{\mathbb{I}}\rangle = \sum_{j=1}^{d}|j\rangle|j\rangle. \tag{51}$$

Laskemalla auki $\mathrm{Tr}_X|\Psi\rangle\langle\Psi|$, missä $X = A, B$ saadaan

$$\begin{aligned}\mathrm{Tr}_X|\Psi\rangle\langle\Psi| &= \mathrm{Tr}_X\frac{1}{d}\big(\sum_{j,k} U\otimes\mathbb{I}|j\rangle|j\rangle)(U\otimes\mathbb{I}\langle j|\langle j|\big)\\ &= \frac{1}{d}\mathrm{Tr}_X\big(\sum_{j,k} U|j\rangle\langle k|U^\dagger\otimes|j\rangle\langle k|\big)\\ &= \frac{1}{d}\mathrm{Tr}_X\big(\sum_{j} UU^\dagger|j\rangle\langle j|\otimes|j\rangle\langle j| + \sum_{j\neq k} U|j\rangle\langle k|U^\dagger\otimes|j\rangle\langle k|\big).\end{aligned}$$

Tästä jälki otettaessa jälkimmäinen termi häviää ja jäljelle jää

$$\frac{1}{d}\mathrm{Tr}_X|\Psi\rangle\langle\Psi| = \frac{1}{d}\mathrm{Tr}_X(\sum_{j=1}^{d}|j\rangle|j\rangle\langle j|\langle j|) = \frac{1}{d}\sum_{j=1}^{d}|j\rangle\langle j|,$$

missä ollaan saatu halutun muotoiset marginaalitilat.

On olemassa sellainen joukko unitaarioperaattoreita $\{U^i\}_{i\in\mathcal{I}}$, että tilat $|\Psi(U^i)\rangle$ muodostavat avaruuden $\mathcal{H}_{AB}$ kannan. Esimerkiksi yleistetyt Paulin operaattorit $Z = \sum_n \exp(2n\pi i/d)|n\rangle\langle n|$ ja $X = \sum_n|(n+1) \mod d\rangle\langle n|$ yhdistettynä muodoksi $|\Psi(U^{jk})\rangle = X^jZ^k\otimes\mathbb{I}|\Phi_{\mathbb{I}}\rangle$ muodostavat tällaisen joukon. Laillisten tilojen virittämä avaruus $\mathrm{span}(\mathcal{L})$ on siis koko $\mathcal{H}_{AB}$, ja maalijoukon $\mathcal{T}$ dimensioiden lukumäärän rajana on $n \leq d^2$.

Koska $\mathcal{L}$ ei nyt ole hyperkiekko, ei $\mathcal{T}$ ole välttämättä minkään hyperkiekon osajoukko. Onkin mahdollista konstruoida esimerkiksi tilanne, jossa maalijoukko koostuu äärettömän monesta erillisestä hyperkiekosta. Esimerkki tästä löytyy artikkelin [6] luvusta IIIB. Koska joukon esittely on pitkähkö eikä erityisen merkittävä, se sivuutetaan.

Osittain degeneroitunut tapaus

Yleisessä tapauksessa osasysteemien tiheysmatriisit ovat osittain degeneroituneita. Tällöin kutakin eri ominaisarvoa vastaa yksi tai useampi ominaisvektori, jotka virittävät ominaisarvoa vastaavan ominaisavaruuden. Merkitään j:nnettä ominaisarvoa λ_j vastaavaa ominaisavaruutta $\mathcal{H}_X^{(j)}$, j:n degeneraatiota eli sitä vastaavien ominaisvektorien lukumäärää $g(j)$ ja ominaisvektoreita $|j,k\rangle$. Näillä merkinnöillä lailliset tilat voidaan kirjoittaa muotoon

$$|\Psi(U)\rangle = \sum_{j=1}^{t} \sqrt{\lambda_j} \sum_{k=1}^{g(j)} U^{(j)} \otimes \mathbb{I} |j,k\rangle |j,k\rangle, \tag{52}$$

missä t on eriävien ominaisarvojen lukumäärä ja $U^{(j)}$ on ominaisavaruuteen $\mathcal{H}_A^{(j)}$ operoiva unitaarioperaattori. Edellinen voidaan kirjoittaa myös lyhyempään muotoon yhdistämällä unitaarioperaattorit yhdeksi blokkidiagonaaliseksi unitaarioperaattoriksi

$$U = \oplus_{j=0}^{t-1} U^{(j)}, \tag{53}$$

ja yhdistämällä muut termit ilmeisellä tavalla, $|\Psi_{\mathbb{I}}\rangle = \sum_{j=1}^{t} \sqrt{\lambda_j} \sum_{k=1}^{g(j)} |j,k\rangle |j,k\rangle$, jolloin tila (52) saadaan muotoon

$$|\Psi\rangle = U \otimes \mathbb{I} |\Psi_{\mathbb{I}}\rangle. \tag{54}$$

Muodosta (54) on helppo hyödyntää seuraavaa lemmaa, jonka merkitys selviää tarkastellessa, ovatko lailliset tilat ja siis myös maalijoukon tilat jollakin hyperkiekolla. Lemman todistus sivuutetaan, sillä se on pitkähkö lemman merkittävyyteen nähden [6].

Lemma 7. *Tilajoukko* $\{|\Psi(U)\rangle\}$, $U \in \mathcal{U}$, *missä* $|\Psi\rangle$ *on muotoa* (54), *sijaitsee Schmidtin hyperkiekolla jos ja vain jos on olemassa muotoa* (53) *oleva blokkidiagonaalinen unitaarimatriisi* U_T, *jolle* $[UU_T, U'U_T] = 0$ *kaikilla unitaarimatriiseilla* $U, U' \in \mathcal{U}$.

Degeneroitumattomien ja täysin degeneroituneiden marginaalitilojen tapaukset saadaan tietenkin osittain degeneroituneista tiloista erikoistapauksina. Kun $t = d$, eriäviä ominaisarvoja on yhtä monta kuin ominaisvektoreita, eli palataan degeneroitumattomaan tapaukseen. Tutkimalla nyt yhtälöä (53) voidaan nähdä, miksei degeneroitumattomassa tilanteessa laillisiin tiloihin (48) sisällytetä unitaarioperaattoria: kuhunkin ominaisavaruuteen operoiva unitaarioperaattori $U^{(j)}$ on yksiulotteinen unitaarioperaattori, ja unitaarioperaattorien määritelmän mukaisesti on olemassa vain yksi tällainen operaattori, 1×1 identiteettikuvaus. Siispä degeneroitumattomassa tapauksessa $U = \mathbb{I}$.

Vastaavasti täysin degeneroituneessa tapauksessa $t = 1$, eli marginaalitiloilla on vain yksi yksikäsitteinen ominaisarvo. Jokaista ominaisvektoria riittää siis kuvaamaan yksi luku, jolloin yhtälöstä (52) voidaan vaihtaa merkintää $|j, k\rangle \equiv |k\rangle$. Koska myös yhtälöstä (53) saadaan nyt, että U on d-ulotteinen unitaarioperaattori, voidaan yhtälön (52) jälkimmäinen summaus pudottaa pois, ja yhtälö palautuu suoraan aiemmin esiteltyyn täysin degeneroituneen tapauksen laillisten tilojen määritelmään (50).

Esimerkkitapaus: $n = 2$**,** $d \geq 2$

Käytännön kvanttimekaniikan kannalta merkittävin tapaus on kubittisysteemin sisältämän informaation naamiointi. Tarkastellaan tilannetta, jossa tuomarisysteemi on kubittisysteemi, $\mathcal{H}_R = \mathcal{H}^2$, ja vastaanottajasysteemien $\mathcal{H}_{A,B}$ dimensio on vähintään kaksi. Tällöin edellä sovituin käytännöin $\dim(\mathcal{T}) = 2$. Maalijoukon rakenteeseen päästään käsiksi tutkimalla yhtälön (46) osia, $\mathcal{V}_\mathcal{T}$ ja $\mathcal{L}$. Tarkastellaan suoraan

osittain degeneroituneiden tiheysmatriisien tapausta.

Koska maalijoukon dimensio on 2, siihen kuuluu ainakin kaksi tilaa, $|\Psi_0\rangle$ ja $|\Psi_1\rangle$. Tällöin

$$|\Psi\rangle = a|\Psi_0\rangle + b|\Psi_1\rangle \quad \forall |\Psi\rangle \in \mathcal{V}_\mathcal{T}, \tag{55}$$

missä $a, b \in \mathbb{C}$ siten, että tila $|\Psi\rangle$ on normalisoitu. Toisaalta kaikki lailliset tilat voidaan kirjoittaa muodossa (54)

$$|\Psi\rangle = U \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle, \tag{56}$$

missä $|\Psi_\mathbb{I}\rangle$ on yhtälön (51) mukainen lomittunut tila. Koska $|\Psi_i\rangle$ kuuluvat maalijoukkoon, ne kuuluvat myös laillisten tilojen joukkoon. Tällöin ne voidaan siis kirjoittaa muotoon

$$|\Psi_0\rangle = U_0 \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle \quad \text{ja} \quad |\Psi_1\rangle = U_1 \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle. \tag{57}$$

Yhdistämällä maalijoukon tilojen virittämään avaruuteen kuulumisen ehto (55) ja laillisten tilojen joukkoon kuulumisen ehto (57) saadaan yleinen muoto maalijoukon tiloille:

$$\begin{aligned} |\Psi\rangle &= aU_0 \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle + bU_1 \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle \\ &= U(a,b) \otimes \mathbb{I}|\Psi_\mathbb{I}\rangle, \end{aligned} \tag{58}$$

missä tilassa esiintyvää unitaarioperaattoria merkitään $U(a,b) = aU_0 + bU_1$. Lemmaa 7 voidaan nyt hyödyntää, kun löydetään unitaarioperaattori U_T, jolle lemmassa tarvittava operaattorien kommutaatioehto $[U(a,b)U_T, U(a',b')U_T] = 0$ täyttyy (tässä $U' = U(a',b')$, sillä a ja b määräävät operaattorin täysin). Sopivaksi operaattoriksi voidaan valita esimerkiksi $U_T = U_0^\dagger$:

$$U(a,b)U_T = (aU_0 + bU_1)U_0^\dagger = a + bU_1U_0^\dagger \tag{59}$$

$$U(a',b')U_T = (a'U_0 + b'U_1)U_0^\dagger = a' + b'U_1U_0^\dagger, \tag{60}$$

joiden nähdään kommutoivan suoraviivaisella laskulla.

Nyt siis lemman 7 mukaan yhtälön (58) mukaiset tilat kuuluvat Schmidtin hyperkiekolle $S^{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. Maalijoukko kokonaisuudessaan sijaitsee siis yhdellä hyperkiekolla, joka on laillisten tilojen joukon osajoukko. Tämä tieto voidaan edelleen sijoittaa yhtälöön (46) laillisten tilojen joukon paikalle, jolloin $\mathcal{T} = \mathcal{V}_{\mathcal{T}} \cap S^{AB}$. Lemman 3 mukaisesti maalijoukko on nyt hyperkiekon S^{AB} kaksiulotteinen säännöllinen osajoukko, joten sen mahdolliset rakenteet ovat joko kaksiulotteinen hyperkiekko tai kaksi erillistä puhdasta tilaa. Koska yksittäinen puhdas tila on yksiulotteinen hyperkiekko, voidaan jälkimmäinen rakenne tulkita kahden erillisen hyperkiekon yhdisteeksi, mutta nämä ovat saman hyperkiekon alihyperkiekkoja.

Degeneroitumattomassa tapauksessa laillisten tilojen joukko itsessään on d -ulotteinen Schmidtin hyperkiekko, jolloin voidaan suoraan hyödyntää lemmaa 3. Lisäksi nähdään, että kun $d = 2$, laillisten tilojen joukko ja maalijoukko ovat sama joukko.

Koska maalijoukko ja naamioitava joukko ovat keskenään isomorfiset, on näin tullut selvitetyksi naamioitavan joukon mahdolliset rakenteet naamioitaessa kubittisysteemin informaatiota. Nähdään siis hyperkiekkokonjektuurin pätevän kubiteilla.

Esimerkkitapaus: $n = 3$**,** $d = 3$

Edellisessä esimerkissä nähtiin hyperkiekkokonjektuurin pätevän kubittisysteemeille. Kun tarkastellaan 3-ulotteisia kvanttisysteemejä, nähdään, että konjektuuri ei enää pidä: naamioitava joukko voi koostua useammasta osasta, jotka sijaitsevat erillisillä hyperkiekoilla. Artikkelissa [6] esitettiin seuraava lause naamioitavan joukon mahdollisista rakenteista tilanteessa, jossa $n = 3$ ja $d = 3$. Lauseen todistus käsittelee itse asiassa maalijoukon rakennetta, mutta jälleen koska naamiointikuvaus on isomorfismi naamioitavan joukon ja maalijoukon välillä, kertoo lauseen tulos suoraan

naamioitavankin joukon rakenteen.

Lause 8. *Kun $n = d = 3$, ja naamioitava joukko $\mathcal{T}$ sisältää vähintään yhden jonkin Schmidtin hyperkiekon 2-ulotteisen alihyperkiekon, joukon $\mathcal{T}$ rakenne on riippuen marginaalitilojen degeneraatiosta riippuen jokin seuraavista kolmesta mahdollisuudesta:*

1) $\mathcal{T}$ on 3-ulotteinen Schmidtin hyperkiekko,

2) $\mathcal{T}$ koostuu kahdesta 2-ulotteisesta hyperkiekosta, jotka eivät ole saman 3-ulotteisen Schmidtin hyperkiekon osajoukkoja, tai

3) $\mathcal{T}$ koostuu jonkin Schmidtin hyperkiekon 2-ulotteisesta alihyperkiekosta, ja yhdestä jollakin toisella Schmidtin hyperkiekolla sijaitsevasta yksittäisestä tilasta.

Jos $\mathcal{T}$ ei sisällä yhdenkään Schmidtin hyperkiekon 2-ulotteista alihyperkiekkoa, joukolla ei ole yleisesti määriteltävää rakennetta, eikä se välttämättä sisällä yhtäkään hyperkiekkoa tai sisälly yhteenkään hyperkiekkoon.

Artikkelissa [6] esitetty todistus lauseelle on pitkähkö ja kohtalaisen suoraviivasta erilaisten tapausten tarkastelua, joten sen tarkempi läpikäynti sivuutetaan. Sen sijaan lauseen seurauksena saadaan seuraavat melko selkeät matemaattiset muotoilut eri rakenteita vastaaville tilajoukoille:

1) 3-ulotteiselle Schmidtin hyperkiekolle kuuluvat määritelmän mukaisesti tilat, jotka ovat muotoa

$$|\Psi(\boldsymbol{\theta})\rangle = \sqrt{\lambda_0}e^{i\theta_0}|00\rangle + \sqrt{\lambda_1}e^{i\theta_1}|11\rangle + \sqrt{\lambda_2}e^{i\theta_2}|22\rangle, \tag{61}$$

missä $\theta_i \in [0, 2\pi)$, $i = 0, 1, 2$, ja $\{|00\rangle, |11\rangle, |22\rangle\}$ on Schmidtin kanta. Vähentämällä vielä globaali vaihe riittää tilojen parametrisointiin kaksi parametria. Tällöin siis maalijoukko voidaan kirjoittaa muotoon

$$\mathcal{T}_1 = \{|\Psi(\theta_1, \theta_2\rangle)|\theta_1, \theta_2 \in [0, 2\pi)\}. \tag{62}$$

2) Maalijoukon muodostavat 2-ulotteiset erilliset hyperkiekot $\{|\Psi_0(\alpha)\rangle\}$ ja

$\{|\Psi_1(\beta)\rangle\}$, missä $\alpha, \beta \in [0, 2\pi)$. Hyperkiekot ovat muotoa

$$|\Psi_0(\alpha)\rangle = \sqrt{\lambda_1}|00\rangle + e^{i\alpha}(\sqrt{\lambda_1}|11\rangle + \sqrt{\lambda_2}|22\rangle) \tag{63}$$

$$|\Psi_1(\beta)\rangle = \sqrt{\lambda_1}(|\phi_{01}^-\psi_{01}^-\rangle + |\phi_{01}^+\psi_{01}^+\rangle) + \sqrt{\lambda_2}|22\rangle, \tag{64}$$

missä $\{|\phi_{01}^-\rangle, |\phi_{01}^+\rangle\} \in \mathcal{H}_A$ ja $\{|\psi_{01}^-\rangle, |\psi_{01}^+\rangle\} \in \mathcal{H}_B$ ovat avaruuden span$\{|0\rangle, |1\rangle\}$ ortonormaaleja kantoja, joille pätee $0 < |\langle 0|\phi_{01}^+\rangle| = |\langle 0|\psi_{01}^+\rangle| < 1$. Toisin sanoen ne eivät ole sama kanta kuin $\{|0\rangle, |1\rangle\}$. Maalijoukko voidaan kirjoittaa muodossa

$$\mathcal{T}_2 = \{|\Psi_0(\alpha)\rangle|\alpha \in [0, 2\pi)\} \cup \{|\Psi_1(\beta)\rangle|\beta \in [0, 2\pi)\}. \tag{65}$$

3) Maalijoukko koostuu hyperkiekosta $\{|\Psi_0(\alpha)\rangle\}$ ja erillisestä tilasta $|\Psi'\rangle$, missä $\alpha \in [0, 2\pi)$. Hyperkiekon ollessa muotoa

$$|\Psi_0(\alpha)\rangle = |00\rangle + e^{i\alpha}(|11\rangle + |22\rangle) \tag{66}$$

voidaan erillinen tila kirjoittaa muodossa

$$|\Psi'\rangle = \cos\frac{\theta}{2}|00\rangle + \sin\frac{\theta}{2}\left(e^{i\varphi_0}|10\rangle + e^{i\varphi_1}|0\psi_{12}^+\rangle\right) + e^{i(\varphi_0+\varphi_1)}\left(e^{i\eta}|2\psi_{12}^-\rangle - \cos\frac{\theta}{2}|1\psi_{12}^+\rangle\right), \tag{67}$$

missä $\theta \in [0, \pi)$ ja η, φ_0 ja $\varphi_1 \in [0, 2\pi)$ ovat vakioita, ja $\{|\psi_{12}^-\rangle, |\psi_{12}^+\rangle\}$ on ortonormaali kanta avaruudelle span$\{|1\rangle, |2\rangle\}$, jolle pätee $|\langle 1|\psi^+\rangle| \neq 1$. Hyperkiekolla ja erillisellä tilalla ei siis ole mitään suoraa keskinäistä matemaattista yhteyttä, vaan tilan vakiot ovat vapaasti naamiointikoneesta riippuvia. Näillä merkinnöillä maalijoukko on muotoa

$$\mathcal{T}_3 = \{|\Psi_0(\alpha)\rangle|\alpha \in [0, 2\pi)\} \cup \{|\Psi'\rangle\}. \tag{68}$$

Marginaalitilojen degeneraatiosta riippuu, mitkä edellä olevista rakenteista ovat mahdollisia naamioitavan joukon rakenteita. Koska $n = d$, lemman 2 mukaan degeneroitumattomassa tapauksessa ainoastaan $\mathcal{T}_1$ — 3-ulotteinen Schmidtin hyperkiekko — on mahdollinen. Osittain degeneroituneessa tapauksessa mahdollisia rakenteita ovat $\mathcal{T}_1$ ja $\mathcal{T}_2$, ja täysin degeneroituneessa puolestaan kaikki kolme rakennetta ovat mahdollisia.

3.4 Useamman osasysteemin naamiointioperaatio

Kuten luvussa 2 mainittiin, naamiointioperaatio voidaan kahden osallistujan sijaan määritellä myös useamman osasysteemin kanssa. Kahden osallistujan tapauksesta poiketen osoittautuu kuitenkin, että useamman osallistujan kanssa mielivaltaisen tilan naamiointi on mahdollista.

Modi *et al.* mainitsivat alkuperäisessä artikkelissaan [2] kvanttivirheenkorjauskoodit esimerkkinä operaatiosta, joka naamioi informaatiota usean osasysteemin välisiin korrelaatioihin. Esimerkkinä voidaan tarkastella Shorin virheenkorjauskoodia, jossa yhden kubitin tila kuvataan yhdeksän kubitin yhdistetylle systeemille seuraavasti:

$$|0\rangle \to \frac{1}{2\sqrt{2}}\big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big) \equiv |\Psi_0\rangle, \tag{69}$$

$$|1\rangle \to \frac{1}{2\sqrt{2}}\big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big) \equiv |\Psi_1\rangle. \tag{70}$$

Tässä $|000\rangle \pm |111\rangle$ on kolmen kubitin superpositiotila. Helposti nähdään, että kunkin yksittäisen kubitin tiheysmatriisiksi tulee $\mathbb{I}/2$. Tilat $|0\rangle$ ja $|1\rangle$ on siis mahdollista naamioida tällä virheenkorjauskoodilla. Suoraviivaisesti voidaan edelleen laskea, että superpositiotila $\alpha|0\rangle + \beta|1\rangle$ joka kuvautuu tilaksi $\alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$ täyttää myös naamiointiehdon. Näin ollen Shorin virheenkorjauskoodi pystyy naamioimaan kaikki kubittitilat.

Edellisessä esimerkissä yhden mielivaltaisen kubitin naamioimiseen tarvitaan yhdeksän kubittia. Tästä loogisesti seuraava kysymys on, että montako osallistujaa minimissään vaaditaan mielivaltaisen tilan naamioinnin mahdollistamiseen. Li ja Wang selvittivät artikkelissaan [8] vastausta tähän kysymykseen. Artikkelissa esitettiin seuraavat kaksi lausetta, joista toinen antaa ylärajan osallistujien minimimäärälle, ja toisessa esitetään kolmen osallistujan riittävän, mikäli sopivat ehdot täyttyvät.

Lause 9. *Olkoon $\mathcal{H}_R$ d-ulotteinen kvanttisysteemi, eli $\mathcal{H}_R = \mathbb{C}^d$, $d \geq 2$. Mielivaltai-*

nen systeemin $\mathcal{H}_R$ tila on mahdollista naamioida, kun osallistujia on $2d$, ja jokaisen osallistujan Hilbertin avaruus on myös $\mathbb{C}^d$. Toisin sanoen, on olemassa kuvaus

$$\mathcal{H}_R \to \otimes_{j=1}^{2d} \mathcal{H}_j \tag{71}$$

missä $\mathcal{H}_R = \mathcal{H}_j = \mathbb{C}^d$, joka pystyy naamioimaan kaikki avaruuden $\mathcal{H}_R$ tilat.

Todistus. Olkoon $\{|l\rangle\}_{l=0}^{d}$ avaruuden $\mathcal{H}_R$ ortonormaali kanta. Määritellään naamiointikuvaus

$$|l\rangle \to |\Psi_l\rangle = \otimes_{k=1}^{d} |\psi_l\rangle, \tag{72}$$

missä $|\psi_l\rangle$ ovat d kappaletta maksimaalisen lomittuneita d-ulotteisia kahden systeemin tiloja, *yleistettyjä Bellin tiloja*

$$|\psi_l\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} \omega^{kl} |kk\rangle, \tag{73}$$

missä $\omega = e^{2\pi i/d}$. Tilat $|\psi_l\rangle$ ovat keskenään ortogonaalisia, eli $\langle \psi_l | \psi_m \rangle = \delta_{lm}$.

Naamioinnin lineaarisuuden nojalla superpositiotila $|\boldsymbol{a}\rangle = \sum_{j=1}^{d} a_j |j\rangle$ kuvautuu tilaksi

$$|\Psi_{\boldsymbol{a}}\rangle = \sum_{l=1}^{d} a_l |\Psi_l\rangle = \sum_{l=1}^{d} a_l (\otimes_{k=1}^{d} |\psi_l\rangle). \tag{74}$$

Tilasta $|\Psi_{\boldsymbol{a}}\rangle$ voidaan nyt ottaa osittainen jälki kaikkien paitsi kahden ensimmäisen osasysteemin yli. Suoraviivaisesti nähdään tilojen $|\psi_l\rangle$ ortonormaaliuden nojalla, että osittainen jälki kahden osasysteemin yli kerrallaan on

$$\begin{aligned} \mathrm{Tr}_{A_d, A_{d-1}} (|\Psi_{\boldsymbol{a}}\rangle\langle\Psi_{\boldsymbol{a}}|) &= \sum_{j=1}^{d} \langle \psi_j | \left(\sum_{l=1}^{d} |a_l|^2 (\otimes_{k=1}^{d} |\psi_l\rangle\langle\psi_l|) \right) |\psi_j\rangle \\ &= \sum_{l=1}^{d} |a_l|^2 (\otimes_{k=1}^{d-2} |\psi_l\rangle\langle\psi_l|). \end{aligned}$$

Iteroimalla toimitusta, kunnes jäljellä on vain kaksi ensimmäistä osasysteemiä, saadaan systeemin $A_1 A_2$ tiheysmatriisiksi

$$\rho_{A_1 A_2} = \sum_{l=1}^{d} |a_l|^2 |\psi_l\rangle\langle\psi_l|. \tag{75}$$

Määritelmän mukaisesti maksimaalisen lomittuneille tiloille $|\psi_l\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ pätee $\mathrm{Tr}_{A_2}|\psi_l\rangle\langle\psi_l| = \mathbb{I}/d$, ja kertoimien a_l normalisaation nojalla

$$\begin{aligned}\rho_{A_1} = \mathrm{Tr}_{A_2}\rho_{A_1A_2} &= \sum_{l=1}^{d} |a_l|^2 \mathrm{Tr}_{A_2}(|\psi_l\rangle\langle\psi_l|) \\ &= \sum_{l=1}^{d} |a_l|^2 \mathbb{I}/d \\ &= \mathbb{I}/d.\end{aligned}$$

Tilojen symmetrisyyden nojalla sama tiheysmatriisi saadaan jokaiselle osasysteemille, ja näin ollen kuvaus (72) pystyy naamioimaan mielivaltaisen tilan $\mathcal{H}_R$:stä $2d$:n osallistujan yhdistetylle systeemille. □

Esimerkkinä lauseessa määritellystä naamiointikuvauksesta voidaan tarkastella kubittien tapausta, jolloin yleistettyjen Bellin tilojen sijaan käytetään tavallisia Bellin tiloja. Määritellään naamiointikuvaus

$$\begin{aligned}|0\rangle \to |\Psi_0\rangle &= \frac{1}{2}(|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle) \\ |1\rangle \to |\Psi_1\rangle &= \frac{1}{2}(|00\rangle - |11\rangle) \otimes (|00\rangle - |11\rangle).\end{aligned} \tag{76}$$

Tilat $|\Psi_i\rangle$ voidaan kirjoittaa auki muotoon

$$\begin{aligned}|\Psi_0\rangle &= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle) \\ |\Psi_1\rangle &= \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle),\end{aligned}$$

mikä selkeyttää niiden yhdistämistä seuraavassa vaiheessa. Kubitin superpositiotila $|a\rangle = a|0\rangle + b|1\rangle$ kuvautuu nyt tilaksi $|a\rangle \to |\Psi_a\rangle = a|\Psi_0\rangle + b|\Psi_1\rangle$, johon sijoittamalla ylläolevat muodot $|\Psi_i\rangle$:lle saadaan

$$|\Psi_a\rangle = \frac{a+b}{2}(|0000\rangle + |1111\rangle) + \frac{a-b}{2}(|0011\rangle + |1100\rangle).$$

Suoraviivaisesti saadaan nyt otettua osittaiset jäljet kolmen ensimmäisen systeemin

yli, jolloin saadaan neljännen osasysteemin tiheysmatriisiksi

$$\begin{aligned}\rho_{A_4} &= \mathrm{Tr}_{\hat{A}_4}|\Psi_a\rangle\langle\Psi_a| = \frac{1}{4}(a+b)^2(|0\rangle\langle 0| + |1\rangle\langle 1|) + \frac{1}{4}(a-b)^2(|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \frac{1}{4}((a+b)^2 + (a-b)^2)(|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \frac{1}{4}(2|a|^2 + 2|b|^2)\mathbb{I} \\ &= \mathbb{I}/2,\end{aligned}$$

missä hyödynnettiin suunnikassääntöä ja kertoimien a ja b normalisointia. Kuvauksen symmetrisyyden nojalla jokaisen osasysteemin tiheysmatriisi on samaa muotoa, joten kuvaus (76) pystyy naamioimaan kubitin mielivaltaisen tilan siten, että jokainen marginaalitila on $\mathbb{I}/2$.

Seuraava lause kertoo itseasiassa, että $2d$ osallistujan sijaan kolme osallistujaa riittää mahdollistamaan mielivaltaisen kvanttitilan naamioimisen. Lauseen todistus tosin kattaa vain tapaukset $d \geq 3$, $d \neq 6$, joten edellisen lauseen tulos ei ole täysin hyödytön. Ennen seuraavaa lausetta määritellään todistuksessa tarvittava työkalu, *keskenään kohtisuorat latinalaiset neliöt*. Latinalainen neliö on $d \times d$-matriisi, jossa esiintyy d erilaista arvoa siten, että jokaisella rivillä ja jokaisessa sarakkeessa kukin arvo esiintyy tasan kerran. Yleisyyttä loukkaamatta voidaan merkitä eri arvoja kokonaisluvuilla väliltä $[1, d]$. Kaksi latinalaista neliötä $V = (v_{ij})$ ja $W = (w_{ij})$ ovat keskenään kohtisuoria, mikäli

$$\{(v_{ij}, w_{ij}) | 1 \leq i, j \leq d\} = \{(i, j) | 1 \leq i, j \leq d\}. \tag{77}$$

Toisin sanoen, kun neliöt V ja W laitetaan päällekkäin ja tarkastellaan järjestettyjä pareja (v_{ij}, w_{ij}), jokainen mahdollinen järjestetty pari (i, j) esiintyy tasan kerran. Esimerkiksi

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{ja} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \tag{78}$$

ovat keskenään kohtisuorat latinalaiset neliöt: asettamalla ne päällekkäin saadaan

$$\begin{pmatrix} 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \end{pmatrix}, \tag{79}$$

jossa jokainen järjestetty pari esiintyy tasan kerran.

Lause 10. *Olkoon $\mathcal{H}_R = \mathcal{H}^d$ d-ulotteinen kvanttisysteemi, $d \geq 3$. Olkoon $V, W \in M_d(\mathbb{C})$ keskenään kohtisuoria $d \times d$ latinalaisia neliöitä, joille merkitään $V = (v_{ij})$ ja $W = (w_{ij})$, ja olkoon $U = (u_{ij}) = (k)$ $d \times d$ matriisi, jonka jokainen alkio on sen rivin numero. Tällöin naamiointikuvaus $\mathcal{H}_R \to \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{A_3}$*

$$|j\rangle \to |\psi_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |u_{jk}\rangle|v_{jk}\rangle|w_{jk}\rangle, \tag{80}$$

missä $\mathcal{H}_{A_i} = \mathcal{H}^d$, pystyy naamioimaan mielivaltaisen avaruuden $\mathcal{H}_R$ tilan.

Todistus. Mielivaltainen superpositiotila $|\boldsymbol{a}\rangle = \sum_{j=1}^{d} a_j|j\rangle$ kuvautuu tilaksi

$$|\Psi_{\boldsymbol{a}}\rangle = \sum_{j=1}^{d} \sum_{k=1}^{d} \frac{a_j}{\sqrt{d}} |u_{jk}\rangle|v_{jk}\rangle|w_{jk}\rangle. \tag{81}$$

U ei ole latinalainen neliö, mutta on määritelmän (77) mukaisesti kohtisuora V:n ja W:n kanssa. Näin ollen joukko $\{|u_{jk}\rangle \otimes |v_{jk}\rangle\}$ sisältää kaikki mahdolliset parit $|j\rangle \otimes |k\rangle$. Se muodostaa siis ortogonaalisen kannan avaruudelle $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Nyt voidaan suoraviivaisesti ottaa jälki systeemien A_1 ja A_2 yli, jolloin saadaan

$$\rho_{A_3} = Tr_{(A_1,A_2)} |\Psi_{\boldsymbol{a}}\rangle\langle\Psi_{\boldsymbol{a}}| = \sum_{j=1}^{d} \sum_{k=1}^{d} \frac{|a_j|^2}{d} |w_{jk}\rangle\langle w_{jk}|. \tag{82}$$

Koska jokainen W:n rivi sisältää jokaisen mahdollisen arvon väliltä $[0, d-1]$, summaamalla k:n yli saadaan $\sum_{k=1}^{d} |w_{jk}\rangle\langle w_{jk}| = \mathbb{I}$, ja huomioimalla kertoimien a_j normalisointiehto saadaan tiheysmatriisiksi

$$\rho_{A_3} \sum_{j=1}^{d} \frac{|a_j|^2}{d} \mathbb{I} = \frac{\mathbb{I}}{d}. \tag{83}$$

Kaikki argumentit toimivat symmetrisesti myös marginaalitilojen ρ_{A_1} ja ρ_{A_2} laskemiseksi, joten kunkin osasysteemin tiheysmatriisi on $\rho_{A_i} = \mathbb{I}/d$. Näin ollen kuvaus (80) pystyy naamioimaan systeemin $\mathcal{H}_R$ mielivaltaisen tilan. □

Edellisen lauseen todistus perustuu kohtisuorien $d \times d$ latinalaisten neliöiden olemassaoloon, joten on helppo nähdä, miksi todistus ei päde, kun $d = 2$: ainoat 2×2 latinalaiset neliöt ovat $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ ja $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, jotka selvästi eivät täytä ehtoa (77). Suurempia d:n arvoja on tutkittu 1700-luvulta lähtien, ja onkin todistettu, että jokaiselle $d \geq 3$, $d \neq 6$ on olemassa ainakin yksi pari kohtisuoria latinalaisia neliöitä [12].

Näiden artikkelissa [8] esitettyjen lauseiden perusteella pienin määrä osasysteemejä, jolle mielivaltaisen kvanttitilan informaatio on mahdollista naamioida, on kolme alkuperäisen systeemin kanssa samanulotteista osasysteemiä, kun $d \geq 3$, $d \neq 6$, ja kun $d = 2, 6$, yläraja pienimmälle määrälle on 4 tai 12 samanulotteista systeemiä. Lauseet eivät kuitenkaan ota kantaa, onko 2- ja 6-ulotteisten systeemien yläraja myös alaraja.

Artikkelissa [13] tutkittiin tarkemmin tapausta $d = 2$, eli naamiointikuvausta $\mathcal{H}^2 \to \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2$. Muutaman aputuloksen avulla artikkelissa yhdistettiin mielivaltaisen tilan naamiointiin kykenevän koneen olemassaolo vastaavan kvanttivirheenkorjauskoodin olemassaoloon, ja virheenkorjauskoodeja koskevien aiempien tulosten nojalla esitettiin seuraava lause.

Lause 11. *Ei ole mahdollista naamioida avaruuden $\mathcal{H}^2$ mielivaltaista tilaa kolmelle osanottajalle, joiden tila-avaruudet ovat $\mathcal{H}^2$.*

Todistus. Artikkelin [13] lauseen 3.2 mukaan on olemassa naamiointikuvaus $S : \mathcal{H}^d \to \otimes_{i=0}^{n-1} \mathcal{H}^d$, joka pystyy naamioimaan mielivaltaisen tilan $\mathcal{H}^d$:ssä jos ja vain jos on olemassa virheenkorjauskoodi $V : \mathcal{H}^d \to \otimes_{i=0}^{n-1} \mathcal{H}^d$, joka pystyy korjaamaan yhden osasysteemin virheen. Toisaalta artikkelissa [14] esitettiin lause, jonka mukaan ei ole

olemassa virheenkorjauskoodia, joka kuvaisi kubittisysteemin tilan kolmelle kubitille. Näin ollen ei ole olemassa naamiointikuvausta $S' : \mathcal{H}^2 \to \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \mathcal{H}^2$, joka pystyisi naamioimaan mielivaltaisen tilan. Todistuksen yksityiskohtaisempi tarkastelu sivuutetaan. □

Edellisessä lauseessa hyödynnettyjen tulosten perusteella voidaan tarkastella myös aiemmin esiteltyjen lauseiden avoimeksi kysymykseksi jättämää tapausta $d = 6$: jos on olemassa virheenkorjauskoodi $\mathcal{H}^6 \to \mathcal{H}^6 \otimes \mathcal{H}^6 \otimes \mathcal{H}^6$, vastaava naamiointioperaatio on myös olemassa. Tällainen virheenkorjauskoodi konstruoitiin sivutuotteena artikkelissa [15], jossa tarkasteltiin 6×6 latinalaisten kvanttineliöiden olemassaoloa. Latinalaisten neliöiden kvanttiversiossa kokonaislukujen sijaan alkiot ovat Hilbertin avaruuden vektoreita siten, että kukin rivi ja sarake muodostaa avaruuden kannan. Virheenkorjauskoodin olemassaolon seurauksena siis myös 6-ulotteinen kvanttisysteemi on mahdollista naamioida kolmelle osasysteemille. Näin ollen kubittisysteemien tapaus on ainoa, jossa kolmelle systeemille naamioiminen ei ole mahdollista.

Tässä luvussa esitetyissä useamman osasysteemin naamiointikuvauksissa kaikki marginaalitilat olivat aina identiteettimatriisiin verrannollisia, $\mathbb{I}/d$. Artikkeli [8] jätti avoimeksi kysymykseksi, onko mahdollista luoda sellainen kuvaus, jossa marginaalitilat eivät ole $\mathbb{I}/d$. Artikkelissa [16] johdettiin kielteinen vastaus tähän kysymykseen vastaavia kvanttivirheenkorjauskoodeja koskevan tuloksen seurauksena.

4 Epätäydelliset operaatiot

Tähän asti on käsitelty vain tilannetta, jossa naamiointioperaatio naamioi tilan täydellisesti joka kerta. Vaatimuksista täydellisyydestä ja joka kerta onnistumisesta voidaan kuitenkin luopua ja selvittää, onko mahdollista kehitellä sellainen naamiointikone, joka pystyy naamioimaan mielivaltaisen tilan jollakin täydellisestä poikkeavalla tarkkuudella. Esimerkiksi kvanttikloonauksen tapauksessa osoittautuu, että vaik-

ka täydellisen kloonin tuottaminen on kieltolauseenmukaan mahdotonta, sopivalla järjestelyllä pystytään tuottamaan melko tarkkoja approksimaatioita. Kieltolauseen vaikutukset pystytään siis osittain kiertämään [17].

Samaan sarjaan approksimatiivisen operaation kanssa kuuluu probabilistinen toteutus, jossa kone tuottaa täydellisiä kopioita, mutta toimii satunnaisesti vain osan ajasta. Tällöin konetta kuvaava matemaattinen operaattori on eri muotoa kuin täydellä varmuudella toimivan koneen operaattori, ja kieltolauseen matemaattinen todistus ei välttämättä päde.

Luvun sisältö perustuu lähinnä artikkelissa [18] esitettyihin määritelmiin ja tuloksiin.

4.1 Approksimatiivinen naamiointi

Täydellisessä naamiointioperaatiossa jokaisen maalijoukon tilan $|\Psi_k\rangle$ marginaalitilat ρ_A ovat identtiset. Ehtoa voidaan lieventää niin, että marginaalitilat eivät ole identtisiä, mutta mahdollisimman samankaltaisia. Tilojen samankaltaisuuden mittana käytetään uskollisuutta (engl. *fidelity*), joka kuvaa tilojen ρ_1 ja ρ_2 samankaltaisuutta yhtälön

$$F(\rho_1, \rho_2) = \sqrt{(\rho_1)^{1/2}\rho_2(\rho_1)^{1/2}} \tag{84}$$

mukaisesti. Uskollisuus saa arvoja väliltä $0 \leq F \leq 1$. Kun $F = 0$, tilat ovat täysin erilaiset ja on mahdollista kehittää järjestely, joka pystyy erottamaan tilat täydellä varmuudella. Kun puolestaan $F = 1$, tilat ovat täysin samanlaiset, eikä niitä ole mahdollista erottaa toisistaan. Toisin sanoen ρ_1 ja ρ_2 ovat tällöin sama tila.

Määritelmä 4. *Lineaarinen isometria S_ϵ on approksimatiivinen naamiointioperaatio, kun se kuvaa tilat $|\psi_k\rangle \in \mathcal{H}_R$ tiloiksi $|\Psi_{AB_k}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ siten, että maalijoukon kaikkien tilojen marginaalitilat ovat likimääräisesti samat. Marginaalitilat ovat liki-*

määräisesti samat, kun kaikilla k ja k' pätee

$$F(\rho_{A|k}, \rho_{A|k'}) \geq 1 - \epsilon \quad ja \quad F(\rho_{B|k}, \rho_{B|k'}) \geq 1 - \epsilon, \tag{85}$$

missä $\rho_{X|k}$ on tilaa $|\Psi_k\rangle$ vastaava osasysteemin X tiheysmatriisi. $\epsilon \geq 0$ on parametri, joka mittaa, kuinka hyvä approksimaatio on täydelliseen naamiontioperaatioon verrattuna.

Seuraava lause 12 antaa rajan sille, kuinka tarkka approksimatiivinen naamionti voi olla. Lauseen todistusta varten määritellään johdetaan ensin tarpeellinen epäyhtälö. Uskollisuuden ja jälkietäisyyden välille saadaan epäyhtälö

$$F(\rho_1, \rho_2) \leq \sqrt{1 - \frac{1}{4}||\rho_1 - \rho_2||_1^2}, \tag{86}$$

missä $\frac{1}{2}||\rho_1 - \rho_2||_1$ on tilojen ρ_1 ja ρ_2 välinen jälkietäisyys,

$$||\rho_1 - \rho_2||_1 =: \mathrm{Tr}(\sqrt{(\rho_1 - \rho_2)^\dagger(\rho_1 - \rho_2)}). \tag{87}$$

Kun sijoitetaan tähän approksimatiivisen naamioinnin määritelmän epäyhtälö (85), saadaan

$$\begin{aligned} 1 - \epsilon &\leq \sqrt{1 - \frac{1}{4}||\rho_{X|k} - \rho_{X|k'}||_1^2} \\ 1 - 2\epsilon + \underbrace{\epsilon^2}_{\approx 0} &\leq 1 - \frac{1}{4}||\rho_{X|k} - \rho_{X|k'}||_1^2 \\ \frac{1}{4}||\rho_{X|k} - \rho_{X|k'}||_1^2 &\leq 2\epsilon \\ ||\rho_{X|k} - \rho_{X|k'}||_1 &\leq 2\sqrt{2\epsilon}. \end{aligned} \tag{88}$$

Lause 12. *Approksimatiivinen naamiointikone $S_\epsilon : \mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B$ voi naamioida kaikki puhtaat tilat $\mathcal{H}_R$:ssä, kun $\epsilon \geq \frac{1}{1296}(1 - \sqrt{1 + \frac{36}{t}} + \frac{18}{t})$, missä $t = \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$.* [1]

[1] Artikkelissa [18] esitettiin hieman erilainen raja ϵ:lle todistuksen alkupuolella tehdyn pienen virheen vuoksi. Virhe ei kuitenkaan vaikuta lauseen lopputulokseen kuin lukuarvollisesti.

Todistus. Olkoon $\{|j\rangle_A\}$ ja $\{|k\rangle_B\}$ avaruuksien $\mathcal{H}_A$ ja $\mathcal{H}_B$ ortonormaalit kannat. Olkoon $|s_1\rangle$ ja $|s_2\rangle$ kaksi lineaarisesti riippumatonta tilaa $\mathcal{H}_R$:ssä. Naamiointikuvaus S_ϵ kuvaa ne tiloiksi

$$|s_1\rangle \to |\Psi_1\rangle \quad \text{ja} \quad |s_2\rangle \to |\Psi_2\rangle. \tag{89}$$

Merkitään tilojen $|\Psi_1\rangle$ ja $|\Psi_2\rangle$ kerroinmatriiseja $M = (m_{jk})$ ja $N = (n_{jk})$, eli $|\Psi_1\rangle = \sum_{j=1}^{d_A}\sum_{k=1}^{d_B} m_{jk}|j\rangle|k\rangle$ ja $|\Psi_2\rangle = \sum_{j=1}^{d_A}\sum_{k=1}^{d_B} n_{jk}|j\rangle|k\rangle$. Tällöin marginaalitilojen kerroinmatriiseiksi saadaan

$$\begin{aligned} \mathrm{Tr}_A(|\Psi_1\rangle\langle\Psi_1|) \equiv M^\dagger M, \quad \mathrm{Tr}_A(|\Psi_2\rangle\langle\Psi_2|) \equiv N^\dagger N \\ \mathrm{Tr}_B(|\Psi_1\rangle\langle\Psi_1|) \equiv MM^\dagger, \quad \mathrm{Tr}_B(|\Psi_2\rangle\langle\Psi_2|) \equiv NN^\dagger, \end{aligned} \tag{90}$$

missä merkintöjen selkeyttämisen vuoksi vektorit on jätetty merkitsemättä. Tilojen $|s_1\rangle$ ja $|s_2\rangle$ mielivaltaiselle superpositiolle $|\Psi'\rangle = \mu|s_1\rangle + \nu|s_2\rangle$ saadaan operaation S_ϵ lineaarisuuden nojalla kerroinmatriisiksi $\mu M + \nu N$, ja marginaalitiloiksi $\mathrm{Tr}_X|\Psi'\rangle\langle\Psi'| = (\mu M + \nu N)(\mu M + \nu N)^\dagger$, $X = A, B$.

Tavoitteena on saada ylä- ja alarajat suureelle $|\mathrm{Tr}(MN^\dagger NM^\dagger)|$ parametrin ϵ suhteen. Tässä otetaan tavallinen matriisin jälki eikä osittaista jälkeä, koska käsitellään kerroinmatriiseja eikä marginaalitiloja. Koska M ja N ovat $d_A \times d_B$ matriiseja, $MN^\dagger NM^\dagger$ on $d_A \times d_A$ neliömatriisi.

Sijoittamalla tiloille $|\Psi_1\rangle$ ja $|\Psi'\rangle$ saadut marginaalitilat yhtälöön (88) saadaan

$$||\mathrm{Tr}_B(|\Psi'\rangle\langle\Psi'|) - \mathrm{Tr}_B(|\Psi_1\rangle\langle\Psi_1|)||_1 \leq 2\sqrt{2\epsilon}, \tag{91}$$

johon kerroinmatriisit yhtälöstä (90) sijoittamalla saadaan

$$\begin{aligned} ||\,|\mu|^2 MM^\dagger + \mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger + |\nu|^2(NN^\dagger - MM^\dagger)||_1 \leq 2\sqrt{2\epsilon} \\ ||(|\mu|^2 - 1)MM^\dagger + \mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger + |\nu|^2 NN^\dagger||_1 \leq 2\sqrt{2\epsilon} \\ ||\,|\nu|^2(NN^\dagger - MM^\dagger) + (\mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger)||_1 \leq 2\sqrt{2\epsilon}, \end{aligned} \tag{92}$$

missä on hyödynnetty kertoimien μ ja ν normalisointia: $|\mu|^2 + |\nu|^2 = 1 \Leftrightarrow |\mu|^2 - 1 = -|\nu|^2$. Merkitään hetkeksi epäyhtälön vasemman puolen termejä A ja B, eli

$v.p. = ||A + B||_1$. Koska A ja B ovat vektoreita, ne muodostavat kolmion vektorin $A+B$ kanssa. Kolmioille pätee epäyhtälö $||B||_1 \leq ||A||_1 + ||A+B||_1$, jolloin saadaan

$$\begin{aligned} ||\mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger||_1 \leq & |\nu|^2 ||(NN^\dagger - MM^\dagger)||_1 \\ & + ||\,|\nu|^2(NN^\dagger - MM^\dagger) + (\mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger)||_1, \end{aligned} \tag{93}$$

josta jälkimmäinen termi tunnistetaan epäyhtälöstä (92), ja ensimmäinen termi löydetään yhtälöstä (88) sijoittamalla siihen marginaalitilat $\mathrm{Tr}_B(|\Psi_2\rangle\langle\Psi_2|)$ ja $\mathrm{Tr}_B(|\Psi_1\rangle\langle\Psi_1|)$. Näillä havainnoilla ylläolevasta epäyhtälöstä (93) saadaan

$$||\mu\nu^* MN^\dagger + \mu^*\nu NM^\dagger||_1 \leq |\nu|^2 2\sqrt{2}\epsilon + 2\sqrt{2}\epsilon = 2\sqrt{2\epsilon}(1 + |\nu|^2). \tag{94}$$

Koska tämä epäyhtälö oletuksen mukaan pätee kaikilla tiloilla $|\Psi'\rangle$, tutkitaan kahta eri tilaa, joiden kertoimet (μ, ν) ovat $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ ja $(\frac{i}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ Tällöin epäyhtälöstä (94) saadaan kaksi epäyhtälöä (tässä $\pm$)

$$||\tfrac{1}{2} MN^\dagger \pm \tfrac{1}{2} NM^\dagger||_1 \leq 2\sqrt{2\epsilon}(1 + \frac{1}{2}) = 3\sqrt{2\epsilon}. \tag{95}$$

Merkitään taas selkeyden vuoksi vasenta puolta $||A \pm B||_1$. Kolmioepäyhtälöä hyödyntäen saadaan $||(A+B) + (A-B)||_1 \leq ||A+B||_1 + ||A-B||_1$, ja toisaalta $||(A+B) + (A-B)||_1 = ||2A||_1$. Sijoittamalla tähän takaisin todelliset arvot, saadaan

$$\begin{aligned} 2||\tfrac{1}{2} MN^\dagger||_1 &\leq 2 \cdot 3\sqrt{2\epsilon} \\ ||MN^\dagger||_1 &\leq 6\sqrt{2\epsilon}, \end{aligned}$$

ja vastaavalla tarkastelulla myös $||NM^\dagger||_1 \leq 6\sqrt{2\epsilon}$. Näitä hyödyntämällä saadaan suureelle $|\mathrm{Tr}(MN^\dagger NM^\dagger)|$ yläraja:

$$|\mathrm{Tr}(MN^\dagger NM^\dagger)| \leq ||MN^\dagger NM^\dagger||_1 \leq ||MN^\dagger||_1 ||NM^\dagger||_1 \leq (6\sqrt{2\epsilon})^2 = 72\epsilon. \tag{96}$$

Alaraja suureelle $|\mathrm{Tr}(MN^\dagger NM^\dagger)|$ saadaan hyödyntämällä jäljen syklisyyttä ja tarkastelemalla ekvivalenttia suuretta $|\mathrm{Tr}(M^\dagger MN^\dagger N)|$. Merkitään $L := N^\dagger N -$

$M^\dagger M$, ja sijoitetaan edellä olevaan jälkeen $N^\dagger N = M^\dagger M + L$:

$$\begin{aligned} |\mathrm{Tr}(M^\dagger M N^\dagger N)| &= |\mathrm{Tr}((M^\dagger M)^2) + \mathrm{Tr}(M^\dagger M L)| \\ &\geq |\mathrm{Tr}((M^\dagger M)^2)| - |\mathrm{Tr}(M^\dagger M L)| \end{aligned} \tag{97}$$

Tarkastellaan ensin ensimmäistä termiä $|\mathrm{Tr}((M^\dagger M)^2)|$. Koska M on $d_A \times d_B$ matriisi, matriisin $M^\dagger M$ aste on korkeintaan $t := \min\{d_A, d_B\}$. $M^\dagger M$ voidaan diagonalisoida jollakin $d_B \times d_B$ unitaarimatriisilla U, jolloin $U^\dagger M^\dagger M U$ on muotoa $diag(x_1, ..., x_{d_B})$, missä on korkeintaan $k \leq t$ nollasta poikkeavaa alkiota. Yleisyyttä loukkaamatta voidaan olettaa näiden olevan k ensimmäistä diagonaalialkiota. Tällöin saadaan

$$\begin{aligned} \big(\mathrm{Tr}(U^\dagger M^\dagger M U)\big)^2 &= \left(\sum_{i=1}^{k} x_i\right)^2 \leq \left(\sum_{i=1}^{k} 1^2\right)\left(\sum_{i=1}^{k} x_i^2\right) \\ &= k|\mathrm{Tr}((M^\dagger M)^2)| \leq t|\mathrm{Tr}((M^\dagger M)^2)| \end{aligned} \tag{98}$$

missä ensimmäisen epäyhtäsuuruuden kohdalla on hyödynnetty Cauchy-Schwarzin epäyhtälöä $|a \cdot b|^2 \leq |a \cdot a||b \cdot b|$. Edelleen saadaan $\frac{1}{t}\left(\mathrm{Tr}(M^\dagger M)\right)^2 \leq |\mathrm{Tr}((M^\dagger M)^2)|$, mikä epäyhtälöön (97) sijoittamalla saadaan

$$|\mathrm{Tr}(M^\dagger M N^\dagger N)| \geq \frac{1}{t}(\mathrm{Tr}(M^\dagger M))^2 - |\mathrm{Tr}(M^\dagger M L)| \tag{99}$$

Ensimmäisestä termistä saadaan suoraan $\frac{1}{t}$, sillä koska M on tilan $|\Psi_1\rangle$ kerroinmatriisi, $\mathrm{Tr}(M^\dagger M) = 1$.

Tarkastellaan erikseen jälkimmäistä termiä $|\mathrm{Tr}(M^\dagger M L)|$. Käytetään taas matriisin $M^\dagger M$ diagonalisoitua muotoa $U M^\dagger M U^\dagger$. Merkitään sen diagonaalialkioita $(x_1, x_2, ...)$. Merkitään myös matriisin $ULU^\dagger$ diagonaalialkioita $(y_1, y_2, ...)$. Nyt

$$|\mathrm{Tr}(M^\dagger M L)| = |\mathrm{Tr}(M^\dagger M U^\dagger U L U^\dagger U)| = |\mathrm{Tr}(U M^\dagger M U^\dagger U L U^\dagger)|.$$

Huomioimalla matriisin $U M^\dagger M U^\dagger$ diagonaalisuus saadaan edelleen jälki auki laskemalla

$$|\mathrm{Tr}(U M^\dagger M U^\dagger U L U^\dagger)| \leq \sum_j x_j |y_j| \leq \sum_j x_j ||L||_2.$$

Jälkimmäisessä epäyhtäsuuruudessa hyödynnetään tietoa, että kukin $|y_j|$ on korkeintaan $||ULU^\dagger||_2$, ja edelleen unitaarimatriisien isometrisyydestä seuraa $||ULU^\dagger||_2 = ||L||_2$. Toisaalta epäyhtälön (91) mukaan $||L||_1 \leq 2\sqrt{2\epsilon}$, ja $||L||_2 \leq ||L||_1$. Huomataan myös, että $\sum_j x_j = 1$, jolloin

$$|\mathrm{Tr}(UM^\dagger MU^\dagger ULU^\dagger)| \leq \sum_j x_j ||L||_2 = ||L||_2 \leq 2\sqrt{2\epsilon}.$$

Sijoittamalla saadut tulokset kaavaan (99) saadaan

$$|\mathrm{Tr}(M^\dagger MN^\dagger N)| \leq \frac{1}{t} - 2\sqrt{2\epsilon},$$

joka kaavan (96) kanssa antaa

$$\frac{1}{t} - 2\sqrt{2\epsilon} \leq |\mathrm{Tr}(M^\dagger MN^\dagger N)| \leq 72\epsilon. \tag{100}$$

Ratkaisemalla tämä epäyhtälö saadaan tulokseksi

$$\epsilon \geq \frac{1}{1296}(1 - \sqrt{1 + \frac{36}{t}} + \frac{18}{t}) \tag{101}$$

□

Todistuksessa johdettu alaraja ϵ:lle ei ole tiukka, ja monet tehdyistä arvioista ovat vain likimääräisiä. On siis mahdollista, että toisenlaisella tarkastelulla rajaa saataisiin vielä alemmas. Käytännössä kuitenkin tämäkin alaraja on erittäin hyvä tulos: tarkastellaan esimerkkinä kubittisysteemin informaation naamiointia kahdelle kubittisysteemille. Tällöin $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}^2$, eli $t = 2$. Sijoittamalla tämä lauseen tulokseen saadaan $\epsilon \geq \frac{1}{1296}(1 - \sqrt{1 + \frac{36}{2}} + \frac{18}{2}) \approx 0,0044$, eli marginaalitilojen $\rho_{X|k}$ välinen uskollisuus on $F(\rho_{X|k}, \rho_{X|k'}) \geq 1 - 0,00435 = 0,9956$. Tämä tarkoittaa, että kun verrataan kahta eri marginaalitilaa $\rho_{X|k}$ ja $\rho_{X|k'}$, 99,5 % todennäköisyydellä niitä ei pystytä erottamaan. Koska ϵ on kääntäen verrannollinen t:hen, suurempidimensioisiin kvanttisysteemeihin informaatiota naamioitaessa uskollisuus kasvaa. Näin määritelty approksimatiivinen naamiointikuvaus on siis hyvin tehokas, ja käytännössä mittalaitteiden tarkkuuden rajoissa kuvaus saattaa käydä täydellisestä.

Lauseesta voidaan myös havaita, että koska ϵ on verrannollinen osasysteemien dimensioihin, $\epsilon = 0$ vaatisi, että $\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\} = 0$. Tämä tarkoittaa siis, että approksimatiivinen naamiointioperaatio, jolla marginaalitilojen välillä ei ole eroa, ei ole mahdollinen. Toisaalta tällainen naamiointioperaatio ei ole lainkaan approksimatiivinen vaan täysin eksakti, joten näin ollen yleiselle naamioinnin kieltolauseelle on saatu vaihtoehtoinen todistus.

4.2 Probabilistinen naamiointi

Probabilistisessa naamioinnissa tehdään vaatimuksille myönnytys, että naamiointioperaation tarvitsee onnistua vain jollakin todennäköisyydellä p. Naamioinnin epäonnistuessa saadulle tilalle ei ole muita vaatimuksia kuin että se ei ole $|\Psi_k\rangle$. Epäonnistuneet tilat hävitetään.

Määritelmä 5. *Kuvaus S_p on probabilistinen naamiointioperaatio, kun se kuvaa tilat $|\psi_k\rangle \in \mathcal{H}_R$ tiloiksi $|\Psi_k\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ todennäköisyydellä p_k, missä tilat $|\Psi_k\rangle$ toteuttavat naamiointiehdon* (23)*. Kuvauksen mahdollisten tulosten todennäköisyydet ovat siis*

$$P(|\psi_k\rangle \to |\Psi_k\rangle) = p_k \tag{102}$$

$$P(|\psi_k\rangle \to |\Phi\rangle) = 1 - p_k, \quad |\Phi\rangle \neq |\Psi_k\rangle, \tag{103}$$

joista vain edellinen Lineaarisen isometrian sijaan S_p on lineaarinen tilan jälkeä pienentävä kuvaus, $Tr(|\psi_k\rangle) \geq Tr(p_k|\Psi_k\rangle) = p_k Tr(|\Psi_k\rangle)(= p_k Tr(|\psi_k\rangle))$. Lisäksi oletetaan, että kuvaus on bijektio, jotta kaksi eri tilaa eivät tuota samaa lopputilaa.

Lause 13. *Yksikään probabilistinen naamiointioperaatio ei pysty naamioimaan kaikkia tiloja $\mathcal{H}_R$:ssä.*

Todistus. Selkeyden vuoksi tarkastellaan vain tilannetta, jossa $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. Oletetaan vastaoletuksena, että on olemassa probabilistinen naamiointioperaatio

S_p, joka pystyy naamioimaan kaikki tilat $\mathcal{H}_R$:ssä. Olkoon tämä kuvaus

$$S_p(|\psi_0\rangle) = p_0|\Psi_0\rangle \quad \text{ja} \quad S_p(|\psi_1\rangle) = p_1|\Psi_1\rangle, \tag{104}$$

missä $|\psi_i\rangle$ ovat lineaarisesti riippumattomia tiloja $\mathcal{H}_R$:ssä, ja $|\Psi_i\rangle$ kuvauksen lineaarisuuden nojalla myös lineaarisesti riippumattomia tiloja $\mathcal{H}_A \otimes \mathcal{H}_B$:ssä. Kuten naamioinnin kieltolauseen todistuksessa, tulkitaan tilat $|\Psi_i\rangle$ marginaalitilan ρ_A purifikaatioina, jolloin niiden Schmidtin hajotelmat ovat

$$|\Psi_0\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j}|j\rangle|b_j^{(0)}\rangle \quad \text{ja} \quad |\Psi_1\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j}|j\rangle|b_j^{(1)}\rangle. \tag{105}$$

Mielivaltainen superpositiotila $\mu|\psi_0\rangle + \nu|\psi_1\rangle$ kuvautuu tilaksi

$$S_p(\mu|\psi_0\rangle + \nu|\psi_1\rangle) = \mu p_0|\Psi_0\rangle + \nu p_1|\Psi_1\rangle \equiv |\Psi'\rangle. \tag{106}$$

Tila $|\Psi'\rangle$ ei ole normalisoitu todennäköisyyksien p_i vuoksi. Olkoon N tilan normalisaatiokerroin, eli normalisoituna tila on $\frac{1}{N}(\mu p_0|\Psi_0\rangle + \nu p_1|\Psi_1\rangle)$. Naamiointiehdon nojalla myös tämä tila on marginaalitilan ρ_A purifikaatio, ja sen Schmidtin hajotelma on

$$|\Psi'\rangle = \sum_{j=1}^{d} \frac{\sqrt{\lambda_j}}{N}|j\rangle(\mu p_0|b_j^{(0)}\rangle + \nu p_1|b_j^{(1)}\rangle). \tag{107}$$

Näin ollen $\left\{\frac{1}{N}(\mu p_0|b_j^{(0)}\rangle + \nu p_1|b_j^{(1)}\rangle)\right\}$ on ortonormaali joukko tiloja. Kahden joukon tilan sisätulo on siis

$$\frac{1}{N}(\mu p_0\langle b_j^{(0)}| + \nu p_1\langle b_j^{(1)}|)\frac{1}{N}(\mu p_0|b_k^{(0)}\rangle + \nu p_1|b_k^{(1)}\rangle) = 0 \tag{108}$$

$$\mu^*\nu p_0 p_1\langle b_j^{(0)}|b_k^{(1)}\rangle + \nu^*\mu p_0 p_1\langle b_j^{(1)}|b_k^{(0)}\rangle = 0 \tag{109}$$

$$\mu^*\nu\langle b_j^{(0)}|b_k^{(1)}\rangle + \nu^*\mu\langle b_j^{(1)}|b_k^{(0)}\rangle = 0, \tag{110}$$

missä on hyödynnetty myös tilojen $|b_j^{(i)}\rangle$ ortogonaalisuutta. Yhtälö tunnistetaan kieltolauseen todistuksessa esiintyväksi yhtälöksi (37). Oletuksen mukaan yhtälö pätee kaikille μ ν, joten jäljelle jää ratkaisu $\langle b_j^{(1)}|b_k^{(0)}\rangle = 0$, kun $j \neq k$.

Naamiointiehto pätee myös osasysteemille B, joten tilat (105) ovat myös marginaalitilan ρ_B purifikaatioita. Tällöin ρ_B voidaan kirjoittaa kahdella tavalla:

$$\rho_B = \sum_{j=1}^{d} \lambda_j |b_j^{(0)}\rangle\langle b_j^{(0)}| = \sum_{j=1}^{d} \lambda_j |b_j^{(1)}\rangle\langle b_j^{(1)}|. \tag{111}$$

Vektoreiden $|b_l^{(0)}\rangle$ ja $|b_l^{(1)}\rangle$ saadaan yhteys laskemalla $\mathrm{Tr}(\rho_B |b_l^{(0)}\rangle\langle b_l^{(0)}|)$ kummallakin ylläolevista ρ_B:n muodoista. Ensimmäisellä muodolla selvästi

$$\mathrm{Tr}(\sum_{j=1}^{d} \lambda_j |b_j^{(0)}\rangle\langle b_j^{(0)}||b_l^{(0)}\rangle\langle b_l^{(0)}|) = \mathrm{Tr}(\lambda_l \langle b_l^{(0)}|b_l^{(0)}\rangle\langle b_l^{(0)}|b_l^{(0)}\rangle) = \lambda_l, \tag{112}$$

ja toisen muodon kanssa lasketun jäljen ollessa yhtä suuri tämän kanssa saadaan

$$\mathrm{Tr}(\sum_{j=1}^{d} \lambda_j |b_j^{(1)}\rangle\langle b_j^{(1)}||b_l^{(0)}\rangle\langle b_l^{(0)}|) = \lambda_l \tag{113}$$

$$\lambda_l |\langle b_l^{(1)}|b_l^{(0)}\rangle|^2 = \lambda_l \tag{114}$$

kaikilla λ_l. Kun $\lambda_l \neq 0$, saadaan $|\langle b_l^{(1)}|b_l^{(0)}\rangle|^2 = 1$, mikä täyttyy, kun $|b_l^{(1)}\rangle = e^{i\theta_l}|b_l^{(0)}\rangle$, missä $\theta_l \in [0, 2\pi)$. Tätä käyttämällä tilasta $|\Psi'\rangle$ saadaan

$$|\Psi'\rangle = \sum_{j=1}^{d} \frac{\sqrt{\lambda_j}}{N} |j\rangle(\mu p_0 + \nu p_1 e^{i\theta_j})|b_j^{(0)}\rangle. \tag{115}$$

Laskemalla tästä muodosta jälleen marginaalitila ρ_B saadaan

$$\rho_B = \sum_{j=1}^{d} \frac{|(\mu p_0 + \nu p_1 e^{i\theta_j})|^2}{N} |b_j^{(0)}\rangle\langle b_j^{(0)}|, \tag{116}$$

jota yhtälöön (111) vertaamalla nähdään, että $|(\mu p_0 + \nu p_1 e^{i\theta_j})|^2 = N$ kaikilla j. Tällöin saadaan

$$|(\mu p_0 + \nu p_1 e^{i\theta_j})|^2 = |(\mu p_0 + \nu p_1 e^{i\theta_k})|^2 \tag{117}$$

$$\mu p_0 (\nu p_1 e^{i\theta_j})^* + (\mu p_0)^* \nu p_1 e^{i\theta_j} = \mu p_0 (\nu p_1 e^{i\theta_k})^* + (\mu p_0)^* \nu p_1 e^{i\theta_k} \tag{118}$$

$$\mu\nu^*(e^{-i\theta_j} - e^{-i\theta_k}) + \mu^*\nu(e^{i\theta_j} - e^{i\theta_k}) = 0. \tag{119}$$

Toisaalta koska yhtälön on toteuduttava kaikilla μ, ν, ratkaisuksi kelpaa vain $e^{i\theta_j} - e^{i\theta_k} = e^{-i\theta_j} - e^{-i\theta_k} = 0$ kaikilla j, k. Tämä tarkoittaa, että θ_l on j:stä riippumaton

vakiokerroin tilassa $|b_j^{(1)}\rangle = e^{i\theta_l}|b_j^{(0)}\rangle$, eli

$$|\Psi_1\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j}|j\rangle|b_j^{(1)}\rangle = e^{i\theta_l} \sum_{j=1}^{d} \sqrt{\lambda_j}|b_j^{(0)}\rangle = e^{i\theta_l}|\Psi_0\rangle. \tag{120}$$

Tulos on ristiriidassa sen oletuksen, että $|\Psi_0\rangle$ ja $|\Psi_1\rangle$ ovat lineaarisesti riippumattomia. Näin ollen probabilistinen naamiointioperaatio ei pysty naamioimaan mielivaltaista tilaa $\mathcal{H}_R$:ssä. □

Tässä todistuksessa on huomattavan paljon samoja piirteitä kuin naamioinnin kieltolauseen todistuksessa. Merkittävänä erona kuitenkin on, että kertoimien μ ja ν mielivaltaisuudesta pidettiin tiukemmin kiinni, mikä lopulta johti ristiriitaan.

Yritys kiertää kieltolauseen vaikutus operaation probabilistisella versiolla on ottanut inspiraatiota probabilistisesta kloonaamisesta [19]. Ensimmäinen lähestymistapa, jolla probabilistista naamiointia tutkittiin, olikin hyvin samankaltainen probabilistisen kloonauksen määrittelyn kanssa. Operaatiossa alkutilat ensin kuvataan maalitiloiksi, ja mittauksen jälkeen valitaan vain ne tilat, jotka täyttävät vaatimukset. Seuraavassa esittelen lyhyesti tämän vaihtoehtoisen probabilistisen kuvauksen ja sille artikkelissa [20] johdetun tuloksen.

Olkoon alkutiloina joukko tiloja $\{|\psi_k\rangle\} \in \mathcal{H}_R$, jotka naamioidaan probabilistisesti tiloiksi $|\Phi_k\rangle = \sqrt{p_k}|\Psi_k\rangle|P_k\rangle + \sqrt{1-p_k}|\Phi_k'\rangle$. Tässä $|\Psi_k\rangle$ on tuttuun tapaan naamiointiehdon täyttävä tila $\mathcal{H}_{AB}$:ssä, $\{|P_k\rangle\}$ on joukko mittalaitteen tiloja, ja $|\Phi_k'\rangle \in \mathcal{H}_{ABP}$ on tila yhdistetyssä systeemissä ABP.

Valitaan tilat siten, että tilat $|\Phi_k'\rangle$ ovat ortogonaalisia joukon $\{|P_k\rangle\}$ virittämän avaruuden kanssa. Tällöin $\langle P_k|\Phi_l'\rangle = 0$ kaikilla k, l. Näin voidaan suorittaa mittaus P:llä, joka valikoi vain ne tilat AB:ssä, jotka täyttävät naamiontiehdon. Näin määritellylle kuvaukselle pätee seuraava lause, jonka todistus sivuutetaan.

Lause 14. *Olkoon $\mathcal{H}_R$, $\mathcal{H}_A$ ja $\mathcal{H}_B$ d-ulotteisia kvanttisysteemejä, ja probabilistinen naamiointikuvaus määritelty kuten edellä. Tilajoukko $\{|\psi_k\rangle\} \in \mathcal{H}_R$ on mahdollista*

naamioida probabilistisesti, kun tilojen lukumäärä on $n \leq d$, ja tilat ovat keskenään lineaarisesti riippumattomia.

Lauseen tulos ei ole mitenkään mullistava, sillä luvussa 3.3 nähtiin esimerkiksi kubiteille, että myös ei-probabilistinen naamiointikuvaus pystyy naamioimaan kaksi keskenään lineaarisesti riippumatonta tilaa, ja toisaalta yleisessä tapauksessakin naamioitavien tilojen joukko on ääretön. Voidaankin siis todeta, että probabilistinen naamiointioperaatio ei ole ei-probabilistista operaatiota tehokkaampi.

5 Seuraukset ja sovellukset

Uudenlaisen kvantti-informaatioteoreettisen operaation keksimisen myötä herää aina kysymys, miten tätä uutta tietoa voidaan hyödyntää? Kvantti-informaation naamioinnin mahdollisten sovellusten lisäksi naamioinnin kieltolause tarjoaa mielenkiintoisen kohteen tutkittavaksi: millaisia seurauksia kieltolauseella on? Ratkaiseeko kieltolause aiemmin esitettyjä avoimia kysymyksiä? Mihin kvantti-informaation naamiointi sijoittuu jo tunnettujen operaatioiden kartalla?

Tässä luvussa esitellään ensin naamiointioperaatiota vastaava aiemmin tunnettu tulos. Lisäksi esitellään kieltolauseesta seurauksena saatava kubittiin sitoutumisprotokollan mahdottomuus, ja lopuksi yksi mielenkiintoinen havainto kvanttiinformaation ja klassisen informaation erosta naamioitavan joukon rakenteen kautta.

5.1 Kvanttisalaisuuksien jakaminen

Kvanttisalaisuuksien jakaminen on järjestely, jossa kvanttitilan sisältämä informaatio jaetaan n:lle osasysteemille siten, että tarvitaan vähintään k osasysteemiä informaation selvittämiseen, ja mikään osasysteemien joukko, jossa on alle k jäsentä, ei sisällä lainkaan informaatiota. Tällaista järjestelyä kutsutaan salaisuuden

(k, n)-jakamiseksi [21]. Jo tästä määritelmästä on suoraviivaista nähdä, että kvanttiinformaation naamiointi kahdelle osasysteemille on vain erikoistapaus salaisuuksien jakamisesta, kun (k, n) on $(2, 2)$. Naamioinnin kieltolausekin saadaan seurauksena jo vuonna 1999 julkaistussa artikkelissa [21] esitetystä salaisuuksien jakamista koskevasta lauseesta. Itse lause ja sen todistus menevät syvemmälle kvanttivirheenkorjauskoodien teoriaan, mutta lauseen seurauksena saatava tulos on ymmärrettävissä tämän kirjoitelman tiedoin.

Salaisuuksien jakaminen voidaan jakaa puhtaiden tilojen ja sekoitettujen tilojen versioiksi, riippuen siitä, onko jaettu tila puhdas vai sekoitettu. Tähän mennessä tarkastelluissa naamiointioperaatioissa on siis ollut kyse puhtaalle tilalle kvanttisalaisuuden jakamisesta. Seuraava lause, jonka todistus sivuutetaan, kattaa kvanttiinformaation naamioinnin.

Lause 15. *Jokaiselle puhtaalle tilalle mielivaltaisen kvanttisalaisuuden jakavalle* (k, n)*-järjestelylle pätee* $n = 2k - 1$.

Koska kvantti-informaation naamiointioperaatio on puhdas kvanttisalaisuuden $(2, 2)$-jakamisjärjestely ja $2 \neq 3$, edellisestä lauseesta seuraa suoraan naamioinnin kieltolause. Naamiointia koskevat tulokset eivät kuitenkaan ole pelkkää pyörän uudelleen keksimistä, sillä salaisuuksien jakamisen tarkastelu artikkelissa [21] keskittyi tuloksiin, jotka koskevat mielivaltaisia tiloja. Rajatun joukon kattavat salaisuuden jakamisen järjestelyt mainittiin artikkelissa vain ohimennen, ja niiden tarkastelu sivuutettiin vähemmän hyödyllisenä. Toisaalta Modin *et al.* avoimeksi jättämään kysymykseen informaation naamioimisesta sekoitetuille tiloille löytyy vastaus salaisuuksien jakamisesta: artikkelissa [21] osoitettiin, että sekoitetuille tiloille mahdollisia (k, n)-järjestelyjä ei ole rajattu yhtä vahvasti kuin puhtaille tiloille, ja $(2, 2)$ sisältyy mahdollisten järjestelyjen joukkoon.

Kvanttisalaisuuksien jakamisella on ilmeisiä sovelluksia kvanttiteknologiassa. Esimerkkinä voidaan kuvitella tilanne, jossa yrityksellä on kvanttikryptattuun säilöön

talletettuna yrityksen liikesalaisuudet. Säilön kryptauksen purkavana avaimena toimiva kvantti-informaatio jaetaan yrityksen johdon kesken siten, että yhdenkään yksittäisen toimijan systeemi ei sisällä säilön avaamiseen vaadittavaa informaatiota, mutta useamman osapuolen toimiessa yhdessä säilö on mahdollista avata. Tällainen järjestely tekee mahdottomaksi yhden pahantahtoisen toimijan aikeet varastaa liikesalaisuudet, mutta toisaalta sallii salaisuuksiin käsiksipääsyn, vaikka joku toimija ei pystyisi osallistumaan. Tässä kuvitteelisessa järjestelyssä on toki ilmeisiä teknologisia kompastuskiviä, kuten esimerkiksi kvantti-informaation säilöminen pidemmäksi ajaksi, eikä se ole realistisesti tänä päivänä toteutettavissa.

Naamioinnin kieltolause asettaakin rajoituksia tällaiselle sovellukselle, kun salaisuus halutaan jakaa vain kahdelle osapuolelle. Vain naamioitavaan joukkoon kuuluvat tilat on mahdollista jakaa salaisesti, joten kahden osapuolen salaisuuden jakamista toteuttaessa tilojen rajoittuminen on otettava huomioon.

5.2 Kubittiin sitoutuminen

Bittiin sitoutuminen on informaatioprotokolla, jossa yksi toimija, Aliisa, valitsee bitin b ja tallettaa sen lukittuun säilöön. Aliisa antaa säiliön Petrille, mutta pitää avaimen itsellään. Protokollan tavoite on, että Aliisa ei pysty jälkikäteen muuttamaan valintaansa, vaan on sitoutunut bittiinsä, ja toisaalta Petri ei pysty selvittämään, mitä Aliisa on valinnut. Kun Aliisa haluaa paljastaa b:n, hän antaa avaimen Petrille [22].

Kvanttiversio bittiin sitoutumisesta on hyvin samankaltainen: Aliisa valitsee bitikseen 0 tai 1, ja koodaa sen yhdistetylle systeemille lomittuneeseen tilaan $|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ tai $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Toisen systeemeistä Aliisa pitää itsellään, ja toisen hän antaa Petrille. Petri ei saamastaan systeemistä pysty päättelemään, mitä Aliisa on valinnut, mutta kun Aliisa jakaa oman systeeminsä Petrin kanssa, on alkuperäinen bitti selvitettävissä.

Bittiin sitoutuminen on selvästi sovellus informaation naamioinnista, vaikka protokollana onkin huomattavasti vanhempi. Kvantti-informaatiolle määritelty naamiointioperaatio tarjoaakin mahdollisuuden laajentaa protokollaa kubittiin sitoutumiseksi. Tällöin Aliisa valitsee bitin sijaan kubittitilan $|\psi_i\rangle$ koodattavaksi lomittuneeseen tilaan $|\Psi_i\rangle$. Naamioinnin kieltolauseen mukaan $|\psi\rangle$ ei kuitenkaan voi olla mielivaltainen kubitti, vaan se voidaan valita vain sopivasta tilajoukosta.

Lomittuneeseen kvanttisysteemiin koodattuun bittiin tai kubittiin sitoutuminen ei ole pitävä protokolla — Aliisa pystyy aina huijaamaan ja muuttamaan tilaa ennen paljastamista. Tämä on nähtävissä kun tarkastellaan tilaa $|\Psi_i\rangle$ Petrin systeemin P purifikaationa. Koska Petrin systeemi ei sisällä naamioitua informaatiota, ρ_P ei riipu tilasta $|\Psi_i\rangle$, joten naamiointiehdon mukaisesti $\rho_P = \mathrm{Tr}|\Psi_i\rangle\langle\Psi_i|$ kaikille i. Tilat $|\Psi_i\rangle$ voidaan siis kirjoittaa Schmidtin hajotelman muotoon $|\Psi_i\rangle = \sum_k \sqrt{\lambda_k}|a_k^{(i)}\rangle|b_k\rangle$. Nyt nähdään tilojen eroavan ainoastaan systeemin A kantavektoreissaan, joten Aliisa pystyy pelkällä lokaalilla unitaarioperaattorilla vaihtamaan tilan haluamakseen: $|\Psi_i\rangle = U_A^{ij} \otimes \mathbb{I}_B|\Psi_j\rangle$ [2].

Bittiin sitoutumisen mahdottomuus on jo pitkään tunnettu tulos, mutta määrittelemällä kvantti-informaation naamiointioperaatio pystytään osoittamaan, että esitellyllä yksinkertaisella protokollalla myöskään kubittiin ei ole mahdollista sitoutua. Protokollaa on mahdollista muokata jakamalla osapuolille kertakäyttöinen erikseen preparoitu lomittunut tila, joka toimii salausavaimena valitulle kubitille. Hyödyntämällä tilan lomittuneisuutta on mahdollista pitävästi sitoutua kubittiin [23]. Muokattu protokolla on kuitenkin paljon monimutkaisempi ja vaatii enemmän resursseja sekä kolmannen osapuolen preparoimaan salausavaimena toimivan tilan.

5.3 Klassisen ja kvantti-informaation raja

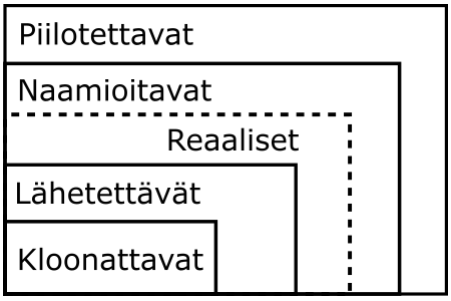
Luvussa 3.3 selvitettiin, että naamioitava joukko koostuu aina jostain hyperkiekkojen yhdisteestä. Palautetaan mieleen m-ulotteisen hyperkiekon tilojen matemaatti-

nen muoto,

$$|\psi(\boldsymbol{\theta})\rangle = \sum_{j=1}^{m} r_j e^{i\theta_j} |\phi_j\rangle. \tag{121}$$

Naamiointioperaatiossa kvantti-informaatio koodataan tilan vaiheparametreihin θ_j. Koska hyperkiekoista koostuva joukko on ainoa mahdollinen naamioitavan joukon rakenne, informaatio naamioidaan aina vain tilan vaiheisiin. Tämä on mielenkiintoinen havainto, sillä tilan vaihe on puhtaan kvanttimekaaninen ominaisuus, jolla ei ole klassista vastinetta. Kvantti-informaatiota on siis mahdollista naamioida vain hyödyntämällä tilojen kvanttimekaanisia ominaisuuksia. Naamioinnin kieltolause muodostaa selkeän rajan klassisen ja kvantti-informaation välille.

6 Kieltolauseiden hierarkia



Kuva 3. Kieltolauseita vastaavien joukkojen hierarkia. Kloonattavien tilojen joukkoon kuuluvat ortogonaaliset tilat kuuluvat myös lähetettävien tilojen joukkoon, joka koostuu keskenään kommutoivista tiloista. Nämä tilajoukot ovat ekvivalentteja jonkin reaalisten tilojen osajoukon kanssa. Kaikki reaaliset tilat on mahdollista naamioida yhdellä naamiointioperaatiolla, mutta naamioitavien tilojen joukkoon voi kuulua myös ei-reaalisia tiloja. Piilotettavien tilojen joukon rakennetta ei ole tutkittu tarkemmin, mutta siihen sisältyy ainakin kaikki naamioitavissa olevat tilat. Artikkelia [9] mukaillen.

Kvantti-informaation matemaattinen rakenne sallii monia operaatioita, mutta moni klassiselle informaatiolle triviaali toimitus ei ole mahdollista kvanttimekaanikassa. Esimerkiksi tutkielmassa tarkasteltu informaation naamiointi on tällainen

operaatio. Vaikka kieltolauseet sinänsä ovat erillisiä ja kullakin on omat oletuksensa ja implikaationsa, ne voidaan järjestää sen mukaan, minkälaisella tilajoukolla operaatio on mahdollista suorittaa. Merkittävimmillä kieltolauseilla tämä järjestys on selkeä: heikompaan kieltolauseeseen liittyvä tilojen joukko sisältää aina vahvemman kieltolauseen vastaavan joukon.

Kuvassa 3 on esitetty kieltolauseita vastaavien sallittujen joukkojen järjestys. Kloonattavaan joukkoon kuuluvat tilat ovat keskenään ortogonaalisia, ja sisältyvät lähetettävien tilojen joukkoon, joka koostuu keskenään kommutoivista tiloista. Nämä joukot sisältävät vain reaalisia tiloja — tiloja, joiden tiheysmatriisien alkiot ovat puhtaan reaalisia — tai ovat ekvivalentteja jonkin reaalisten tilojen osajoukon kanssa. Naamioitavien tilojen joukkoon sisältyy kaikki reaaliset tilat ja hieman enemmän, ja piilotettavien tilojen joukko sisältää kaikki naamioitavat tilat. Luvun sisältö perustuu enimmäkseen artikkeliin [9].

6.1 Kloonauksen kieltolause

Kloonauksen kieltolause (engl. *no-cloning theorem*) on kieltolauseista vanhin ja tunnetuin, jo vuonna 1982 esitetty [1]. Kloonaamisoperaatiossa systeemin alkutilasta tuotetaan täydellinen kopio häiritsemättä alkuperäistä systeemiä. Mikäli kloonaaminen olisi mahdollista, voitaisiin mielivaltaisen tarkasti selvittää minkä tahansa kvanttisysteemin tila tuottamalla siitä useita kopioita ja suorittamalla eri mittaukset eri kopioille. Tämä kumoaisi tilan fundamentaalin epätarkkuuden vaikutukset, yhden kvanttimekaniikan peruspilareista. Melko lyhyellä laskulla voidaan kuitenkin osoittaa, että yleinen kloonausoperaatio ei ole mahdollinen mielivaltaisille kubiteille. Todistus yleistyy ilmeisellä tavalla useampiulotteisillekin systeemeille.

Kloonausoperaatio on kuvaus $|A\rangle|\Psi\rangle \rightarrow |A'\rangle|\Psi\rangle \otimes |\Psi\rangle$, missä $|\Psi\rangle$ on kloonattavan kubitin alkutila. Lineaarisuuden nojalla riittäisi olettaa, että kloonauslaite pystyy

kloonaamaan kubitin puhtaat tilat, eli

$$|0\rangle \to |0\rangle|0\rangle \quad \text{ja} \quad |A\rangle|1\rangle \to |A_1'\rangle|1\rangle|1\rangle. \tag{122}$$

Toisaalta yleisen kloonausoperaation tulisi myös kyetä kloonaamaan mielivaltainen superpositiotila $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, missä $\alpha, \beta \in \mathbb{C}$, jolloin kubitin lopputilaksi saataisiin

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle. \tag{123}$$

Suorittamalla kloonausoperaatio (122) superpositiotilaan $|\Psi\rangle$ saadaan kuitenkin lopputilaksi

$$(\alpha|0\rangle + \beta|1\rangle) \to \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle, \tag{124}$$

joka selvästi ei vastaa tilaa (123). Näin ollen kloonausoperaation ei ole mahdollista kloonata mielivaltaista kubitin tilaa, ja todistus yleistyy suoraan useampiulotteisille kvanttisysteemeille. On kuitenkin huomionarvoista, että kuvatun kaltainen kloonausoperaatio pystyy kloonaamaan kaksi ortogonaalista tilaa, $|0\rangle$ ja $|1\rangle$. Yleisesti käykin ilmi, että kutakin kloonausoperaatiota vastaava kloonattava joukko on joukko ortogonaalisia tiloja.

6.2 Lähettämisen kieltolause

Lähettämisen kieltolause (engl. *no-broadcasting theorem*) kieltää hyvin samankaltaisen operaation kuin kloonaamisen kieltolause. Lähettämisoperaatiossa mielivaltainen kvanttitila lähetetään kahdelle erilliselle kvanttisysteemille siten, että kummankin systeemin tila näyttää samalta kuin alkuperäinen tila, toisin sanoen yhdistetyn systeemin lopputilan marginaalit vastaavat alkuperäistä tilaa [24]. Yhteys kloonaamiseen on selkeä: kloonausoperaation tuloksena yhdistetyn systeemin kumpikin osapuoli on samassa tilassa kuin alkuperäinen kloonattava tila, lähetysoperaatiossa

lopputilassa kummallekin osapuolelle näyttää, että systeemi on alkutilaa vastaavassa tilassa.

Olkoon R, A ja B kvanttisysteemejä, joiden Hilbertin avaruudet ovat $\mathcal{H}_R$, $\mathcal{H}_A$ ja $\mathcal{H}_B$, ja olkoon $\{\rho_k\}$ joukko tiloja $\mathcal{H}_R$:ssa. Lähettämisoperaatiossa $\mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B$ tila ρ_k kuvataan yhdistetyn systeemin tilaksi ρ'_s siten, että

$$\mathrm{Tr}_A[\rho'_s] = \mathrm{Tr}_B[\rho'_s] = \rho_s. \tag{125}$$

Erikoistapauksena tällaisesta operaatiosta voidaan tarkastella kuvausta, jossa tila ρ_s kuvautuu tilaksi $\rho'_s = \rho_s \otimes \rho_s$. Tällöin selvästi ehto (125) pitää. Tämä operaatio on määritelmän mukaan yhtäpitävä kloonausoperaation kanssa, joten kloonaaminen nähdään lähettämisen erikoistapaukseksi.

Lähettämisen kieltolauseen mukaan mikään lähetysoperaatio ei pysty lähettämään mielivaltaisia tiloja. Lähetettävien tilojen joukon rakennetta koskevan lauseen todistus on yksinkertaisessakin tapauksessa huomattavasti monimutkaisempi kuin edellisessä alaluvussa esitetty todistus kloonauksen kieltolausetta vastaavalle joukolle, joten se jätetään esittelemättä. Tuloksena kuitenkin saadaan, että jokaista lähettämisoperaatiota vastaava lähetettävien tilojen joukko koostuu keskenään kommutoivista tiloista, eli tiloista, joiden tiheysmatriisit kommutoivat. Suoraviivaisesti nähdään myös, että kloonattavien tilojen joukko sisältyy tähän joukkoon: ortogonaaliset tilat kommutoivat triviaalisti.

6.3 Naamioinnin kieltolause

Kieltolauseiden hierarkiassa naamioinnin kieltolause asettuu lähettämisen ja piilottamisen väliin. Jokaista lähettämisoperaatiota vastaava tilajoukko sisältyy jonkin naamiointioperaation naamioitavaan joukkoon, ja jokainen naamioitava joukko on jonkin piilottamisoperaation sallitun joukon osajoukko. Artikkelissa [7] esitettiin lause, jonka mukaan jokainen joukko joka koostuu keskenään kommutoivista tiloista on mahdollista naamioida sopivalla lineaarisella isometrialla. Lauseen seurauksena

siis naamiointioperaatio on lähettämisoperaatiota ylempänä kieltolauseiden hierarkiassa. Toisaalta naamiointi nähdään erikoistapaukseksi informaation piilottamisesta, ja näin ollen naamiointi on hierarkiassa piilottamisen alapuolella.

6.4 Piilottamisen kieltolause

Samalla tavalla kuin lähettäminen voidaan nähdä kloonauksen yleistyksenä, naamioinnin oletuksia voidaan lievittää hieman ja saada yleisempi operaatio, kvanttiinformaation piilottaminen [25]. Kun naamioinnissa informaatio naamioidaan molemmilta osasysteemeiltä, piilottamisoperaatiossa informaatio piilotetaan vain toiselta systeemiltä siirtämällä se kokonaan toiseen systeemin tai systeemien välisiin korrelaatioihin. Piilottamisen kieltolauseen (engl. *no-hiding theorem*) mukaan mielivaltaista tilaa ei voida piilottaa joltain osasysteemiltä siten, että informaatiota siirtyy systeemien välisiin korrelaatioihin — piilotettu informaatio siirtyy kokonaisuudessaan systeemin muihin osiin.

Olkoon jälleen R, A ja B kvanttisysteemejä, joiden Hilbertin avaruudet ovat $\mathcal{H}_R$, $\mathcal{H}_A$ ja $\mathcal{H}_B$, ja olkoon $\{\rho_k\}$ joukko tiloja $\mathcal{H}_R$:ssa. Piilottamisoperaatio on kuvaus $M : \mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B$, joka kuvaa lähtösysteemin tilan ρ_k yhdistetyn systeemin tilaksi $\tilde{\varrho_k}$ siten, että naamiointiehto pätee vain toiselle osasysteemille:

$$\rho_A = \mathrm{Tr}_B(\varrho_k) \qquad \rho_B^k = \mathrm{Tr}_A(\varrho_k) \quad \forall k. \tag{126}$$

Systeemin A tila ei siis riipu piilotetusta tilasta, mutta systeemi B saa sisältää informaatiota. Piilottamisen kieltolause kertoo, että mielivaltainen tila on mahdollista piilottaa vain siten, että kaikki informaatio on siirtynyt osasysteemiin B.

Piilotettavien tilojen joukon rakennetta ei ole tutkittu kovin tarkasti, mutta koska operaatio vastaa naamiointioperaatiota lievemmin rajoituksin, vähintään kaikki johonkin naamioitavaan joukkoon kuuluvat tilat on mahdollista piilottaa yhdellä piilotusoperaatiolla. Koska piilottaminen ja naamiointi ovat hyvin samankaltaiset operaatiot, piilottamisesta käytetään myös termiä *osittainen naamiointi* [9].

7 Yhteenveto

Tämän tutkielman pääsisältönä on ollut kvantti-informaation naamiointioperaatio ja siihen liittyvä kieltolause. Naamioinnin kieltolauseen seurauksena yhdellä naamiointikuvauksella on mahdollista naamioida vain jokin tila-avaruuden osajoukko, kuvaukseen liittyvä naamioitava joukko.

Luvussa 3 tarkasteltiin, millaisissa tilanteissa kvantti-informaation naamiointi on mahdollista. Aluksi esiteltiin naamioinnin kieltolause todistuksineen, jonka jälkeen syvennyttiin naamioitavan joukon mahdollisiin rakenteisiin. Joukon rakennetta tarkasteltiin ensin yleisellä tasolla, ja esiteltiin lause, jonka mukaan naamioitava joukko on ylinumeroituvan ääretön, kun informaatio koodataan tilan vaiheparametreihin. Joukon rakenteesta esiteltiin myös joitain konkreettisia esimerkkejä, ja nähtiin naamioitavien joukkojen sijaitsevan yleensä jollakin hyperkiekolla tai useamman hyperkiekon yhdisteellä.

Luvussa 4 esiteltiin kaksi mahdollista keinoa kieltolauseen kiertämiseksi: approksimatiivinen ja probabilistinen naamiointi. Approksimatiivisessa naamioinnissa luovutaan vaatimuksesta, että kaikki naamioidun tilan marginaalit ovat sama tila, ja sallitaan niiden välillä olevan jonkin verran eroa. Approksimatiiviseen naamiontiin liittyen esitettiin lause, jonka mukaan voidaan saavuttaa hyvinkin korkea uskollisuus marginaalitilojen välille — kubiteilla noin 0,5%. Probabilistisessa naamioinnissa sallitaan operaation epäonnistuminen, ja tarkastellaan tilannetta, jossa satunnaisest vain osa operaatiolla kuvatuista alkutiloista päätyy lopputilassa täydellisesti naamioituun tilaan. Luvussa esitettyjen lauseiden tuloksena nähtiin, että probabilistisella naamioinnilla ei saavuteta etua ei-probabilistiseen naamiointiin nähden.

Luku 5 sisälsi naamioinnin kieltolauseen seurauksena todistuksen kubittiin sitoutumisprotokollan mahdottomuudesta. Naamioitavan joukon rakenteesta puolestaan havaittiin, että informaatiota on mahdollista naamioida vain, jos se on koodattu alkutilan vaihetekijöihin. Koska tilan vaihe on puhtaan kvanttimekaaninen ilmiö,

havainto osoittaa naamioinnin kieltolauseen olevan seurausta nimenomaan kvanttifysiikan laeista.

Lisäksi luvussa esiteltiin havainto, että vaikka kvantti-informaation naamiointi esitettiin vuonna 2018 uutena keksintönä, naamiointi on vain erikoistapaus vuonna 1999 esitellystä kvanttisalaisuuden jakamisesta. Kvanttisalaisuuden jakamisen yhteydessä osoitettiin myös naamioinnin kieltolauseeseen johtava tulos mahdollisten salaisuudenjakamisjärjestelyjen kautta. Tuloksen esittely uudelleen ei kuitenkaan ole täysin turhaa, sillä viime vuosina naamioinnin sovelluksia ja kieltolauseen seurauksia on tutkittu enemmänkin artikkelin [2] innoittamana. Alkuperäinen esitys ei myöskään ottanut lainkaan kantaa naamioitavaan joukkoon, joten joukon rakennetta koskevat tuloksetkin ovat täysin uutta tietoa.

Luvussa 6 esiteltiin lyhyesti muita aiemmin tunnettuja kieltolauseita. Naamiointi nähtiin rajoitetummaksi erikoistapaukseksi informaation piilottamisesta, ja toisaalta nähtiin kloonauksen ja lähettämisen olevan naamiointia tiukempia kieltolauseita. Lauseita vastaavat sallittujen tilojen joukot järjestettiin hierarkisesti sisäkkäin, ja naamioinnin kieltolause sijoitettiin paikalleen tähän kieltolauseiden hierarkiaan.

Kvantti-informaation naamiointiin liittyviä avoimia kysymyksiä on lähinnä sen sovelluksiin liittyen. Kokeellisesti naamiointioperaatio on onnistuttu toteuttamaan erilaisin järjestelyin: artikkelissa [26] informaatiota naamioitiin yhden fotonin eri vapausasteiden välille, ja artikkelin [27] koejärjestelyssä vastaanottavina systeemeinä toimivat kahden fotonin polarisaatiot. Tulosten tuoreudesta johtuen konkreettisia naamioinnin sovelluksia ei vielä ole tarkemmin esitetty. Myös joitain teoreettisia kysymyksiä on avoinna: esimerkiksi approksimatiiviselle naamioinnille luvussa 4 esitetyn rajan optimaalisuus ei ole varmaa. Naamioitavien joukkojen rakennetta käsittelevä artikkeli [6] jätti myös avoimeksi joitain erikoistapauksia koskevia kysymyksiä.

Viitteet

[1] W. K. Wootters ja W. H. Zurek, Nature **299**, 802 (1982).

[2] K. Modi, A. K. Pati, A. Sen ja U. Sen, Physical Review Letters **120**, 230501 (2018).

[3] P. Lahti ja J. Kiukas, *Kvanttimekaniikka II* (Turun yliopisto, 2014).

[4] M. A. Nielsen ja I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2012).

[5] S. Stenholm ja K.-A. Suominen, *Quantum approach to informatics* (John Wiley & Sons, Inc., 2005).

[6] F. Ding ja X. Hu, Physical Review A **102**, 042404 (2020).

[7] Y. Du, Z. Guo, H. Cao, K. Han ja C. Yang, International Journal of Theoretical Physics **60**, 2380 (2021).

[8] M.-S. Li ja Y.-L. Wang, Physical Review A **98**, 062306 (2018).

[9] H. Zhu, Physical Review Research **3**, 033176 (2021).

[10] X. B. Liang, B. Li ja S. M. Fei, Physical Review A **100**, 1 (2019).

[11] X.-B. Liang, B. Li, S.-M. Fei ja H. Fan, Physical Review A **101**, 042321 (2020).

[12] R. C. Bose, S. S. Shrikhande ja E. T. Parker, Canadian Journal of Mathematics **12**, 189 (1960).

[13] K. Y. Han, Z. H. Guo, H. X. Cao, Y. X. Du ja C. Yang, EPL (Europhysics Letters) **131**, 30005 (2020).

[14] M. Grassl, T. Beth ja T. Pellizzari, Physical Review A - Atomic, Molecular, and Optical Physics **56**, 33 (1997).

[15] S. A. Rather, A. Burchardt, W. Bruzda, G. Rajchel-Mieldzioć, A. Lakshminarayan ja K. Zyczkowski, Physical Review Letters **128**, 1 (2022).

[16] F. Shi, M.-S. Li, L. Chen ja X. Zhang, Physical Review A **104**, 032601 (2021).

[17] V. Bužek ja M. Hillery, Physical Review A - Atomic, Molecular, and Optical Physics **54**, 1844 (1996).

[18] M.-S. Li ja K. Modi, Physical Review A **102**, 022418 (2020).

[19] L. M. Duan ja G. C. Guo, Physical Review Letters **80**, 4999 (1998).

[20] B. Li, S. H. Jiang, X. B. Liang, X. Li-Jost, H. Fan ja S. M. Fei, Physical Review A **99**, 1 (2019).

[21] R. Cleve, D. Gottesman ja H. K. Lo, Physical Review Letters **83**, 648 (1999).

[22] D. Mayers, Physical Review Letters **78**, 3414 (1997).

[23] S. H. Lie, H. Kwon, M. S. Kim ja H. Jeong, Quantum **5**, 405 (2021).

[24] H. Barnum, C. M. Caves, C. A. Jozsa, R. Jozsa ja B. Schumacher, Physical Review Letters **76**, 2818 (1996).

[25] S. L. Braunstein ja A. K. Pati, Physical Review Letters **98**, (2007).

[26] R.-Q. Zhang, Z. Hou, Z. Li, H. Zhu, G.-Y. Xiang, C.-F. Li ja G.-C. Guo, Physical Review Applied **16**, 024052 (2021).

[27] Z.-H. Liu, X.-B. Liang, K. Sun, Q. Li, Y. Meng, M. Yang, B. Li, J.-L. Chen, J.-S. Xu, C.-F. Li ja G.-C. Guo, Physical Review Letters **126**, 170505 (2021).