

Kvantti-informaatioverkostojen kapasiteetti ja simulointi

LuK-tutkielma
Turun yliopisto
Teoreettinen fysiikka
2024
Fil. yo. Artturi Korhonen
Tarkastaja:
Dosentti J. N

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck-järjestelmällä

TURUN YLIOPISTO
Fysiikan laitos

Korhonen, Artturi Kvantti-informaatioverkostojen kapasiteetti ja simulointi

Pro Gradu, 30 s., 3 liites.
Fysiikka
Tammikuu 2024

Tutkielmassa generoidaan kvantti-informaatioverkostoja erinäisiä satunnaismalleja käyttäen, joiden parametrit ovat valittu mallintamaan amerikkalaisia valokuituverkkoja. Koska kvantti-informaatioverkostojen tehtävä on siirtää informaatiota noodien välillä, herää kysymys siitä, kuinka paljon informaatiota saadaan siirrettyä verkon jokaisella käyttökerralla, ja kuinka luotettavasti.

Koska kvantti-informaatioverkostot käyttävät kvanttimekaanisia ilmiöitä, niiden toimintaan tarvittavaa fysiikkaa ja matematiikkaa esitellään, erityisesti painopisteenä ovat lomittuminen sekä Bellin tilat. Verkostoteorian puolelta esitellään satunnisverkkojen käsite ja verkostojen ominaisuuksiin liittyviä suureita.

Kvanttimekaanikan ja verkostoteorian aihealueet yhdistävä suure on kanavan kapasiteetti. Kvanttikanavan kapasiteetille häviöllisiä kanavia käyttäen on teoreettinen yläraja, jota ei voi ylittää käyttäen lokaaleja operaatioita ja klassista kommunikointia. Tutkielmassa simuloitujen verkkojen kapasiteetit määritetään tämän teoreettisen ylärajan kautta.

Asiasanat: kvantti-informaatioverkostot, kvanttiteleportaatio, lomittuminen, kvanttikanavat, kapasiteetti, satunnaisverkot, Waxman-verkot, minimileikkaus, simulatio, skaalavapaa

Sisällys

Johdanto	1
1 Kvanttimekaniikka	2
1.1 Kubitti	2
1.2 Lomittuminen	3
1.3 Bellin epäyhtälö ja tilat	6
1.3.1 Bellin epäyhtälö	6
1.3.2 Bellin tilat	8
1.4 Lomittumisen tislauk	9
1.4.1 LOCC	9
1.4.2 Puhtaat ja sekoittuneet tilat	10
1.5 Kvanttikanavat ja kapasiteetti	11
1.6 Kvanttiteleportaatio	12
2 Verkostot	14
2.1 Graafi	14
2.1.1 Aste ja astejakauma	15
2.2 Satunnaisverkot	15
2.2.1 Satunnaisverkoista ja $G(n, m)$ -verkko	15
2.2.2 Erdős–Rényi, $G(n, p)$ -verkko	17
2.2.3 Waxman	17
2.2.4 Skaalavapaa-malli	18
2.3 Leikkaus	19
2.4 Vierekkäisyysmatriisi	21
3 Simulaatiot	22
3.1 Pohjustus	22

3.2	Esimerkkejä	23
3.2.1	Esimerkkien esittely	27
4	Yhteenveto	28

Johdanto

Kvantti-verkostot ovat keskeisiä kvantti-informaation prosessoinnissa jaetuissa ongelmissa, kuten jaetuissa algoritmeissa [1], kvanttisensoriverkoissa [2] ja kryptografisten avainten jakamisessa kvanttimekaniikkaa hyödyntäen [3]. Erityisesti kyseiset kvanttiverkostot tähtäävät lomittumisen jakoon ja kvantti-informaation siirtämiseen. Internet on pääasiassa rakennettu valokuituverkoista, jossa fotonit ovat informaation siirtäjiä, ja ovat myös todennäköisesti informaation siirtäjiä myös kvantti-verkostoissa [4]. Kummassakin tilanteessa kanavan häviöllisyys on merkittävä ongelma kommunikaatiossa, mutta toisin kuin klassista informaatiota, kvantti-informaatiota ei voi kloonata. Tämän takia on kallista lisätä edes toistinnodeja, jotka vastaanottavat kvantti-informaatiota, poistavat niistä kohinaa ja häiriöitä sekä lähettävät puhdistetun informaation eteenpäin verkostossa.

Avainkohtana kvanttiverkoston suunnittelussa on vaihtokauppa noodien tiheyden ja lomittumisen jakamisen taaajuuden kanssa: kuinka paljon noodeja vaaditaan, jotta voidaan taata luotettava kvantti-informaation siirtäminen monen käyttäjän välillä määritellyllä alueella. Vastaus ei riipu vain käyttäjien välisistä kokonaisuusyksistä, vaan myös kvanttiverkoston rakenteesta [5].

Tutkielma jaetaan kolmeen aihealueeseen: kvanttimekaniikkaan, verkostoihin ja verkostojen simuloiteihin. Ensimmäisessä esittelemme ne kvanttimekaniikan osa-alueet, jotka ovat kvantti-informaatioverkostojen kannalta oleellimmat ja käymme läpi erityisesti ne aihealueet, jotka liittyvät kvantti-informaation siirtämiseen. Kubittien lomittuminen, kvanttiteleportaatio sekä kvanttikanavat ovat kvantti-informaation siirtämisessä oleellimmat käsiteltävät osa-alueet ja siten ne saavat sanallisten selitysten lisäksi matemaattisen katsauksen. Tässä tutkielmassa olevat esimerkit noudattelevat Peter Kiokin "An Introduction to Quantum Physics" [6] tekstejä. Bellin tilat ovat keskeisiä kvanttiteleportaation ja lomittumisen ymmärtämiseksi, joten ne ansaitsevat oman osionsa.

Kvanttimekaaniset verkostot ovat pohjimmiltaan verkostoja, joissa lähetetään teleportaatiota käyttäen lomittuneita tiloja sijainnista toiseen ja kvanttimekaanisen osuuden ymmärtäminen on keskeistä kvanttimekaanisten verkkojen mallien rakentamista ja tutkimista varten.

Toisessa luvussa aiheina ovat verkostojen perusteet, satunnaismallit ja leikkauksen käsite verkostossa. Koska simulaatioissa simuloidaan Waxman-verkkoja, skaalavapaita verkkoja ja Erdős–Rényi-verkkoja, tutkielmassa esitellään niiden teoriaa ennen analysointia. Satunnaismalleista perustavanlaatuisimmat, eli $G(n, m)$ -verkot sekä $G(n, p)$ -verkot esitellään ja kuinka satunnaisverkkojen ominaisuuksia kuuluu määritellä. Erityisesti kiinnostuksen kohteena ovat $G(n, p)$ -verkkojen alakategoriaan kuuluvat Waxman-verkot ja skaalavapaat verkot.

Kolmannessa luvussa esitellään ja vertaillaan generoituja satunnaisverkkoja. Osiossa pohjustetaan malleille käytettäviä oletuksia, parametreja ja mitattavia suureita. Tärkeimmät tutkittavat suureet tutkielman verkoille ovat verkon kokonaiskapasiteetti, pääte pisteiden kapasiteetti ja noodikapasiteetti. Jokaiselle näistä esitellään matemaattinen määritelmä ja lasketaan joidenkin niistä arvoja erinäisille verkoille.

1 Kvanttimekaniikka

1.1 Kubitti

Kvanttimekaniikassa fysikaalisen systeemin tilaa kuvataan vektorilla Hilbertin avaruudessa \mathcal{H} : kompleksiarvoisessa vektorivaruudessa, jossa on määritelty sisätulo, joka indusoi etäisyysfunktion. Kvanttimekaniikassa systeemin tiloja kuvataan vektoreina Hilbertin avaruudessa ja kubittien tapauksessa vektorit kuuluvat ℓ^2 , kaksiulotteiseen Hilbertin avaruuteen, jossa avaruuden dimensio kuvaa kubiteille olevien kantatilojen määrää. Diracin notaatiota [7] käyttäen aaltofunktio ψ , joka kuvaa

kvanttisysteemin tilaa ilmaistaan muodossa:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (1)$$

jossa $\alpha, \beta \in \mathbb{C}$ ja joille pätee $|\alpha|^2 + |\beta|^2 = 1$.

Toisin kuin klassiset bitit, jotka voivat olla vain yhdessä kahdesta tilasta, kubiteilla on kvanttimekaniikalle erityinen ominaisuus: kubitin superpositiotila on myöskin käypä tila. Superpositiossa mittaustulos ei ole selvästi määritelty ennen mittausta ja Bornin säännön mukaan todennäköisyys löytää kubitin jommasta kummasta kantatilastaan määräytyy sen kertoimen itseisarvon neliöstä [8]. Tästä seuraa kertoimien α ja β normalisoinnin tarve.

1.2 Lomittuminen

Systeemi, joka koostuu useammasta kuin yhdestä kubitista voi olla lomittunut tai separoituva. Hilbertin avaruus \mathcal{H} kokonaissysteemille, joka muodostuu alisysteemeistä \mathcal{H}_l , on tensoritulo alisysteemeistä $\mathcal{H} = \otimes_{l=1}^n \mathcal{H}_l$ [9]. Superpositioperiaatteen mukaisesti kokonaissysteemin tila voidaan kirjoittaa muodossa:

$$|\psi\rangle = \sum_{\mathbf{i}_n} c_{\mathbf{i}_n} |\mathbf{i}_n\rangle \quad (2)$$

jossa $\mathbf{i}_n = i_1, i_2, \dots, i_n$ on multi-indeksi ja $|\mathbf{i}_n\rangle = |i_1\rangle \otimes |i_2\rangle \cdots \otimes |i_n\rangle$. Tarkastellaan esimerkin avulla, mitä fyysisiä ominaisuuksia lomittumisesta seuraa ja kuinka lomittuminen voidaan ilmaista matemaattisesti.

Mitataan kahden elektronin spinejä z-suunnassa. Ensimmäisen elektronin tilaa merkitään:

$$|\psi\rangle_1 = a |\uparrow\rangle_1 + b |\downarrow\rangle_1 \quad (3)$$

ja toisen elektronin:

$$|\phi\rangle_2 = c |\uparrow\rangle_2 + d |\downarrow\rangle_2 \quad (4)$$

Luonnollisesti pätee, että $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$. Mitattaessa elektronien spiniä z-suunnassa saadaan kahden elektronin systeemille neljä eri mahdollista mittaustulosta:

$$|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle \quad (5)$$

jossa ketin ensimmäinen alkio viittaa aina ensimmäisen elektronin mitattuun spiniin ja jälkimmäinen alkio toisen elektronin mitattuun spiniin.

Valitaan systeemin tilaksi:

$$|\psi\rangle = \frac{1}{2}[|\uparrow\uparrow\rangle + |\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle + |\downarrow\downarrow\rangle] \quad (6)$$

Oletetaan seuraavaksi, että elektronit ovat tiloissa, jotka ovat annettu yhtälöissä 3 ja 4. Koska mittaukset ovat riippumattomia, ovat systeemin tilan todennäköisyydet yksittäisten elektronien tilojen todennäköisyyksien tuloja. Todennäköisyydet saada elektroneille yhtälössä 5 esiintyvät tilat ovat seuraavat:

$$\begin{aligned} \mathbb{P}(\uparrow\uparrow) &= |a|^2|c|^2 \\ \mathbb{P}(\uparrow\downarrow) &= |a|^2|d|^2 \\ \mathbb{P}(\downarrow\uparrow) &= |b|^2|c|^2 \\ \mathbb{P}(\downarrow\downarrow) &= |b|^2|d|^2 \end{aligned} \quad (7)$$

Suoralla sijoituksella saadaan, että $\mathbb{P}(\uparrow\uparrow) + \mathbb{P}(\uparrow\downarrow) + \mathbb{P}(\downarrow\uparrow) + \mathbb{P}(\downarrow\downarrow) = 1$.

Kahdesta elektronista muodostuva systeemi, jonka tila toteuttaa edellä mainitut todennäköisyydet on seuraavanlainen:

$$|\psi\rangle = ac|\uparrow\uparrow\rangle + ad|\uparrow\downarrow\rangle + bc|\downarrow\uparrow\rangle + bd|\downarrow\downarrow\rangle \quad (8)$$

Yhtälön 8 tila on kuitenkin yhtälöiden 3 ja 4 tulo:

$$\begin{aligned} |\psi\rangle_1 |\phi\rangle_2 &= \\ (a|\uparrow\rangle_1 + b|\downarrow\rangle_1) + (c|\uparrow\rangle_2 + d|\downarrow\rangle_2) &= \\ ac|\uparrow\uparrow\rangle + ad|\uparrow\downarrow\rangle + bc|\downarrow\uparrow\rangle + bd|\downarrow\downarrow\rangle \end{aligned} \quad (9)$$

Tästä nähdään, että tila yhtälössä 6 on sama kuin kahden tilan tulo, jossa elektronit ovat tiloissa:

$$|\psi\rangle_1 = |\phi\rangle_2 = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\rangle \quad (10)$$

Aiemmin yhtälössä 5 esiteltyt tilat muodostavat kannan kahden elektronin systeemille. Tiloista voidaan ottaa mielivaltainen superpositio ja superpositiotila kelpaa kvantttilaksi, kunhan kertoimien normalisaatio toteutuu.

Tarkastellaan seuraavaksi, millaisia ominaisuuksia näillä tiloilla on ja mitä niistä seuraa.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} |\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\downarrow\rangle \quad (11)$$

Yhtälöä 11 ei voi mitenkään esittää yhtälön 9 muodossa siten, että sen kertoimet toteuttaisivat yhtälön 11 tilan. Tämä tarkoittaa, että ei ole *mitään* tiloja yksittäisille elektroneille yhtälöistä 3 ja 4, jotka toteuttaisivat yhtälön 11. Tämä merkitsee elektronien olevan lomittuneita, sillä kahden elektronin tilaa ei voida kirjoittaa kahden yksittäisen elektronin tilan tulona. Jos kokonaistilan voi kirjoittaa kahden yksittäisen tilan tulona, tilaa kutsutaan separoituvaksi [10]. Lomittuneilla ja separoituvilla tiloilla on fysikaalisia eroja, joita voidaan hahmottaa ajatuskokeella.

Elektronilähde lähettää elektroneita vastakkaisiin suuntiin, yhden Alicelle ja toisen Bobille ja kummatkin mittaavat vastaanottamansa elektronin spinin z-suunnassa. Jos elektronit ovat tilassa Φ^+ , saavat Alice ja Bob puolet kerroista mittaustuloksi spinin arvoksi \uparrow ja puolet kerroista \downarrow . Oleellisesti, kun Alice saa mittaustulokseksi \uparrow , niin myös Bob saa mittaustulokseksi \uparrow ja vastaavasti kun Alice saa mittaustuloksen \downarrow , myös Bob saa mittaustulokseksi \downarrow .

Jatketaan ajatuskoetta seuraavanlaisesti: elektronilähde lähettää tilan $|\uparrow\uparrow\rangle$, mutta tällä kertaa Alice ja Bob mittaavat spinin x-suunnassa. Tilat $|\uparrow\rangle$ ja $|\downarrow\rangle$ voidaan kirjoittaa S_x havainnoitavan ominaisarvojen $|+\rangle$ ja $|-\rangle$ avulla:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle \quad (12)$$

$$|\downarrow\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle \quad (13)$$

Tila $|\uparrow\uparrow\rangle$ on tilojen $|+\rangle$ ja $|-\rangle$ kannassa ilmaistuna:

$$|\uparrow\uparrow\rangle = \frac{1}{2}|++\rangle + \frac{1}{2}|+-\rangle + \frac{1}{2}|-+\rangle + \frac{1}{2}|--\rangle \quad (14)$$

ja tila $|\downarrow\downarrow\rangle$:

$$|\downarrow\downarrow\rangle = \frac{1}{2}|++\rangle - \frac{1}{2}|+-\rangle - \frac{1}{2}|-+\rangle + \frac{1}{2}|--\rangle \quad (15)$$

Kun tila $|\Phi^+\rangle$ mitataan x-suunnassa saadaan

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|++\rangle + \frac{1}{\sqrt{2}}|--\rangle \quad (16)$$

Tästä nähdään, että mittauksissa on täydellinen korrelaatio, kun Alice ja Bob mittaavat spinin x-suunnassa ja mittaukset korreloivat sekä $\{\uparrow, \downarrow\}$ että $\{+, -\}$ suunnissa.

1.3 Bellin epäyhtälö ja tilat

1.3.1 Bellin epäyhtälö

John Bell osoitti artikkelissaan [11], että paikallisesti piilossa olevia muuttujia ei ole olemassa, vaan kvanttihiukkasten välillä on vahvempia korrelaatioita kuin mitä klassisesti voisi odottaa. Bellin teoreeman mukaan lomittumisesta seuraavia ominaisuuksia ei voida toistaa teorioilla, jotka puoltavat paikallisesti piilotettuja muuttujia.

Tarkastellaan seuraavanlaista koeasetelmaa: Alice ja Bob ovat hyvin kaukana toisistaan ja kolmas osapuoli Victor valmisteleo hiukkasparin ja lähettää yhden Alicelle ja toisen Bobille. Hiukkasilla on kaksi binääristä ominaisuutta, Alicen vastaanottamalla hiukkasella a_0 ja a_1 ja Bobin vastaanottamalla hiukkasella b_0 ja b_1 . Alice valitsee yhden kahdesta binäärisestä mittausoperaatiosta, joita merkitään A_0 :lla ja A_1 :llä.

Mittausoperaatio A_0 mittaa hiukkasen ominaisuutta a_0 ja voi saada arvokseen ± 1 . Vastaavat pätevät mittaukselle A_1 , Bobin mittauksille B_0 ja B_1 ja ominaisuuksille a_1 , b_0 ja b_1 . Tarkastellaan seuraavaa yhtälöä:

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = (A_0 + A_1)B_0 + (A_0 - A_1)B_1 \quad (17)$$

jota käytetään Bellin teoreeman todistamiseen.

A_0 ja A_1 voivat olla joko samanmerkkisiä tai erimerkkisiä. Tästä seuraa, että yhtälön 17 arvot ovat välillä ± 2 . Mistään yksittäisestä mittauksesta ei saada yhtälölle suoraan arvoa, sillä kerralla voidaan tehdä vain toinen mittauksista A_0 ja A_1 sekä mittauksista B_0 ja B_1 . Olettaen, että oletukset realismista, eli fyysiset suureet a_0 , a_1 , b_0 ja b_1 ovat olemassa riippumatta siitä mitataanko tai havainnoidaanko ne ja oletus paikallisuudesta: Alicen valinta ei vaikuta Bobin valintaan tai toisin päin. Näistä seuraa, että yhtälön 17 yläraja on:

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \leq 2 \quad (18)$$

Yhtälö 17 tunnetaan CHSH-epäyhtälönä [12]. Jos oletukset pitävät paikkansa, on summan odotusarvo odotusarvojen summa, joten:

$$\langle A_0, B_0 \rangle + \langle A_0, B_1 \rangle + \langle A_1, B_0 \rangle - \langle A_1, B_1 \rangle \leq 2 \quad (19)$$

Kvanttimekaniikassa CHSH-epäyhtälö voidaan rikkoa. Victor preparoi kubitti-parin, joka on tilassa:

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (20)$$

joista toisen hän lähettää Alicelle ja toisen Bobille. Tilat $|0\rangle$ ja $|1\rangle$ ovat ominaistiloja Pauli-matriisille:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (21)$$

Alicen ja Bobin mahdolliset mittaukset ovat myös määritelty Paulin matriisien avulla. Alice mittaa joko havainnoitavan σ_z tai σ_x :

$$\begin{aligned}
A_0 &= \sigma_z \\
A_1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned} \tag{22}$$

ja Bobin mittaukset ovat määritelty muodossa:

$$\begin{aligned}
B_0 &= \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \\
B_1 &= \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}
\end{aligned} \tag{23}$$

Victor voi laskea odotusarvot havainnoitaville pareille käyttäen Bornin sääntöä:

$$\begin{aligned}
\langle A_0 \otimes B_0 \rangle &= \frac{1}{\sqrt{2}} \\
\langle A_0 \otimes B_1 \rangle &= \frac{1}{\sqrt{2}} \\
\langle A_1 \otimes B_0 \rangle &= \frac{1}{\sqrt{2}} \\
\langle A_1 \otimes B_1 \rangle &= -\frac{1}{\sqrt{2}}
\end{aligned} \tag{24}$$

Vaikka vain yksi näistä neljästä mittauksesta voidaan tehdä kerralla, niiden summa on

$$\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle = 2\sqrt{2} \tag{25}$$

Tämä summa ylittää CHSH-epäyhtälön ylärajan, joka pääteltiin olettaen, että hypoteesi paikallisista piilotetuista muuttujista pitää paikkansa.

1.3.2 Bellin tilat

Bellin tilat ovat kahden lomittuneen kubitin yksinkertaisimmat tilat ja ovat maksimaalisesti lomittuneita. Nämä tilat muodostavat kannan neliulotteiselle Hilbertin avaruudelle.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \tag{26}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle \quad (27)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle \quad (28)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle \quad (29)$$

1.4 Lomittumisen tislaus

1.4.1 LOCC

Lokaalit operaatiot ja klassinen kommunikaatio (LOCC), on metodi kvantti-informaatioteoriassa, jossa paikallinen operaatio tehdään yhdessä osassa systeemiä, operaation tulos viestitetään toiselle osapuolelle käyttäen klassista kommunikaatiota ja jonka jälkeen yleensä toisessa osassa systeemiä tehdään operaatio, joka riippuu saadun viestin sisällöstä.

Hyvin yksinkertaisena esimerkkinä, Alice ja Bob jakavat kaksi Bellin tilaa:

$$\begin{aligned} |\Phi^-\rangle &= \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle \end{aligned} \quad (30)$$

ja he voivat kommunikoida toistensa kanssa klassista kommunikaatiokanavaa käyttäen, esimerkiksi puhelimella. He haluavat tietää, kumpi tiloista heillä on. LOCC:tä hyödyntäen, Alice ja Bob voivat eritellä tilat toisistaan. Alice mittaa oman kubittinsa ja lähettää tiedon mittaustuloksesta Bobille. Bob mittaa oman kubittinsa, ja jos esimerkiksi Alice saa mittaustulokseksi 0 ja Bob tulokseksi 1, tiedetään systeemin olevan tilassa Ψ^- .

1.4.2 Puhtaat ja sekoittuneet tilat

Kvanttimekaaniset systeemit voivat olla tiloissa, joita ei voi ilmaista aaltofunktiolla. Tällaisia tiloja kutsutaan sekoittuneiksi tiloiksi ja ne ovat tilastollinen jakauma puhtaista tiloista kun taas puhdas kvantttila on tila, jonka voi ilmaista yhdellä ket-vektorilla tai summana kantavektoreita. Yleistys kvanttimekaanisten systeemien ilmaisemiseen ovat tiheysmatriisit (tiheysoperaattorit). Tosin kuin klassisessa mekaniikassa, jossa tilastollinen kuvaus systeemistä johtuu vaillinaisesta tiedosta, vaikka kvanttisysteemistä olisi kaikki informaatio, se voi silti olla sekoitetussa tilassa.

Tiheysoperaattori ρ puhtaalle tilalle määritellään:

$$\rho := |\psi\rangle \langle\psi| \quad (31)$$

jolla on seuraavat ominaisuudet:

$$\begin{aligned} \rho^2 &= \rho \text{ projektori} \\ \rho^\dagger &= \rho \text{ hermiittisyys} \\ \text{Tr}[\rho] &= 1 \text{ normalisaatio} \\ \rho &\geq 0 \text{ positiivisuus} \end{aligned} \quad (32)$$

ja sekoitetulle tilalle:

$$\sum_i p_i |\psi_i\rangle \langle\psi_i| \quad (33)$$

jossa p_i on todennäköisyys, että systeemi on tilassa ψ_i .

Monet perustavanlaatuiset vaikutukset kvantti-informaatioteoriassa käyttävät hyväkseen maksimaalisesti lomittunutta tilaa Ψ^+ [13]. Luonnossa ja laboratorioissa on kuitenkin yleensä sekoitettuja tiloja operaatioiden epätäydellisyyden ja dekoherenssin takia. Ratkaisua haettiin ensimmäisenä tutkimuspaperissa [14], jossa käsiteltiin keinoja puhdistaa tai tislata lomittumista. Kun kaksi kaukana toisistaan olevaa tahoa jakavat keskenään n kopiota kaksiosaisesta sekoitetusta tilasta, jossa on kohinaa

lomittumisessa, tahot voivat käyttää LOCC-operaatioita ja saada käyttöönsä k ($< n$) tilaa, jotka ovat lähellä singlettitilaa, joka sisältää puhdasta lomittumista [13].

Prosessia voi kuvata seuraavanlaisesti: kahdella havainnoitsijalla Alicella ja Bobilla on kummallakin hallussaan n kvanttisysteemiä, jotka tulevat lomittuneista pareista, jotka ovat tilassa ρ . Kumpikin voi tehdä lokaaleja operaatioita n :lle hiukkaselle ja vaihtaa klassista informaatiota toisen kanssa. Jos LOCC-operaatioiden jälkeen heillä on pari lomittuneita kubitteja, he ovat onnistuneet tislamaan puhdasta lomittuneisuutta tilasta [15].

Tislauksen jälkeen tahot voivat käyttää saatuja lähes singlettitiloja kvanttiteleportaatioon, lomittumiseen perustuvaan kvanttikryptografiaan ja muihin puhtaan lomittumiseen perustuvia protokollia.

1.5 Kvanttikanavat ja kapasiteetti

Kvanttikanava kuvaa fyysistä prosessia, jossa kvantti-informaatiota siirretään lähettäjältä vastaanottajalle. Kvanttitila lähetetään kvanttikanavaa käyttäen, joka voi käytännössä olla esimerkiksi valokuitukaapeli tai langaton kvanttikommunikaatiokanava [16, s.1]. Tällaiset kanavat ovat väistämättä häviöllisiä [17, s.7], joten on mielekästä määritellä häviöllisen kanavan kapasiteetti. Kommunikaatiokanavan kapasiteetti kuvailee kanavan kykyä välittää informaatiota lähettäjältä vastaanottajalle luotettavasti ja palautettavasti. Koska optinen kommunikaatio langattomasti tai telekuituja pitkin on väistämättä häviöllistä, tavanomainen malli näille kanaville ovat bosoniset, Gaussiset kanavat, joita karakterisoi transmittiivisuusparametri η , joka kvantifoi suhdeluvun niistä fotoneista, jotka selviävät kanavan käytöstä [17].

Maksimaalisen kapasiteetin kvanttikanavalle määrittää PLOB-rajaa [18, s.1], Pirandolan, Laurenzan, Ottavianin ja Banchin mukaan, joka rajoittaa kuinka paljon kvantti-informaatiota voidaan luotettavasti lähettää aikayksikössä.

$$\mathcal{C}(\eta) = -\log_2(1 - \eta) \quad (34)$$

Yhtälö 34 määrittää maksimaalisen kapasiteetin kvanttikanavalle. Virheettömiä lähetystyyppejä ei voida taata, jos kanavaa käytetään enemmän kuin kapasiteetti sallii. Rajalla $\eta \rightarrow 1$, kun kaikki fotonit selviävät kanavan käytöstä, kapasiteetti $\mathcal{C}(\eta) \rightarrow \infty$. Tämä kuvastaa sitä, että kanavaa voidaan käyttää mielivaltaisen paljon, ilman että kvantti-informaatiota katoaa.

1.6 Kvanttiteleportaatio

Kvanttikorrelaation eräs erikoisimmista sovellutuksista on kvanttiteleportaatio [19]. Tässä prosessissa kvanttitila siirretään yhdeltä hiukkaselta toiselle, eli kubitin tila vaihtaa paikkaa hiukkasten siirtymättä. Tämän lisäksi, kvanttitilan siirron pitää onnistua ilman, että mitään lisätietoa kvanttitiloista saadaan. Teleportaatioissa kaksi eri taho aloittavat jaetulla Bellin parilla, jonka teleportaatioprotokolla käyttää siirtääksensä kubitin tilan lähettäjältä vastaanottajalle. Toisin kuin klassisten verkostojen, joiden on tarkoitus jakaa informaatiota verkossa, kvanttiverkostojen tarkoitus jakaa lomittuneita tiloja, joita teleportaatio käyttää.

Käytetään esimerkkinä jälleen hiukkasina elektroneja ja spinien mittausta, kuten lomittumisessa. Kahden elektronin kantatilat voidaan ilmaista muodossa, jotka ovat yhtälössä (5) tai vaihtoehtoisesti Bellin kannassa, jotka ovat yhtälöissä (26) - (29).

Alicella on hallussaan elektroni, jota merkataan 1:llä, spin-tilassa

$$|\psi\rangle_1 = a|\uparrow\rangle_1 + b|\downarrow\rangle_1 \quad (35)$$

Lisäksi, Alicella on elektroni 2 ja Bobilla elektroni 3, tilassa

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}|\uparrow_2, \uparrow_3\rangle + \frac{1}{\sqrt{2}}|\downarrow_2, \downarrow_3\rangle \quad (36)$$

Alicella ovat elektronit 1 ja 2, Bobilla on hallussaan elektroni 3. Seuraavaksi yhdistetään kolmen elektronin tilat tilaan:

$$\begin{aligned}
|\Gamma\rangle &= |\psi\rangle_1 |\Phi^+\rangle_{23} = \\
&= (a|\uparrow\rangle_1 + b|\downarrow\rangle_1) \left(\frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle \right) = \\
&= \frac{1}{\sqrt{2}}(a|\uparrow\uparrow\uparrow\rangle + a|\uparrow\downarrow\downarrow\rangle + b|\downarrow\uparrow\uparrow\rangle + b|\downarrow\downarrow\downarrow\rangle)
\end{aligned} \tag{37}$$

Bellin kannassa ilmaistuna tämä yhdistetty tila on:

$$\begin{aligned}
|\Gamma\rangle &= \\
&= \frac{1}{2} [|\Phi^+\rangle_{12} (a|\uparrow\rangle_3 + b|\downarrow\rangle_3) + \\
&+ |\Psi^-\rangle_{12} (a|\uparrow\rangle_3 - b|\downarrow\rangle_3) + \\
&+ |\Psi^+\rangle_{12} (b|\uparrow\rangle_3 + a|\downarrow\rangle_3) + \\
&+ |\Psi^-\rangle_{12} (b|\uparrow\rangle_3 - a|\downarrow\rangle_3)]
\end{aligned} \tag{38}$$

Alice mittaa yhden neljästä tuloksesta Bellin mittauksessaan ja jokaiselle tulokselle voimme tarkistaa Bobin elektronin tilan:

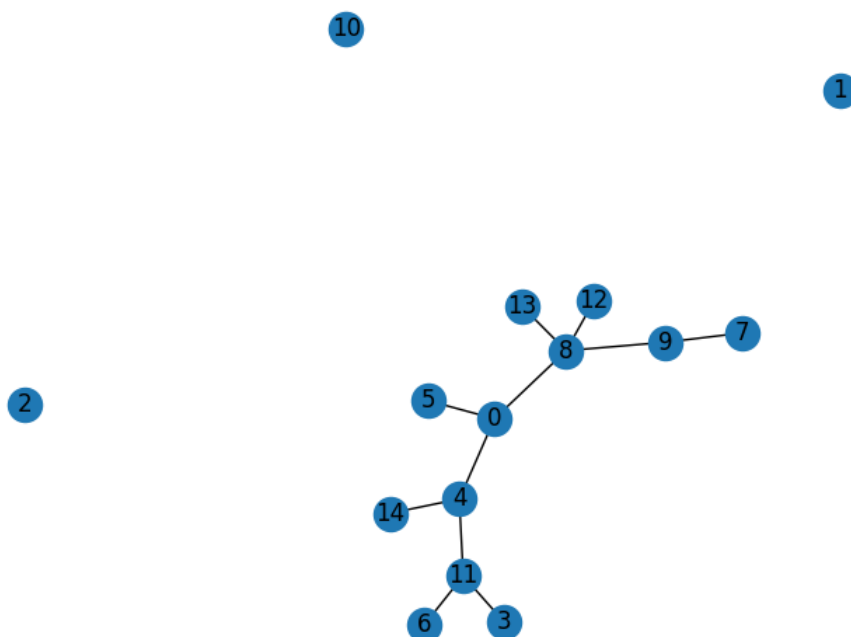
$$\begin{aligned}
\Phi^+ : |\psi\rangle_3 &= a|\uparrow\rangle + b|\downarrow\rangle \\
\Phi^- : |\psi\rangle_3 &= a|\uparrow\rangle - b|\downarrow\rangle \\
\Psi^+ : |\psi\rangle_3 &= a|\downarrow\rangle + b|\uparrow\rangle \\
\Psi^- : |\psi\rangle_3 &= a|\downarrow\rangle - b|\uparrow\rangle
\end{aligned} \tag{39}$$

Tästä nähdään, että Alicen suorittama mittaus muuttaa Bobin hallussa olevan kubitin tilaa, eli kvanttiteleportaatio on onnistunut. Jotta Bob voi muuttaa tilansa siihen samaan, joka Alicella oli alun perin, Bob joutuu odottamaan Alicelta signaalia, joka kertoo missä Bellin tilassa Alicen systeemi oli aluksi. Tämän jälkeen Bob pystyy tekemään vaadittavan unitaarimuunnoksen saadakseen tilansa samaan kuin Alicella. Teleportaation tiedonsiirtoa siis rajoittaa klassinen tiedonsiirto.

2 Verkostot

2.1 Graafi

Verkostot, joita myös kutsutaan graafeiksi matemaattisessa kirjallisuudessa [20] ovat matemaattisia rakenteita, joilla mallinnetaan pareittaisia suhteita olioiden välillä. Määrittelemme verkon järjestetyksi pariksi $G = (V, E)$, jossa V on joukko noodeja ja $E \subseteq \{\{i, j\} | i, j \in V, i \neq j\}$. E :tä kutsutaan verkon linkeiksi.



Kuva 1: Esimerkki graafista, jossa $n = 15$.

Jatkossa merkitsemme noodien lukumäärää verkostossa n :llä ja linkkien lukumäärää m :llä. Tutkielmassa keskitytään *yksinkertaisiin verkostoihin*, eli verkostoihin, joissa noodit eivät yhdisty itseensä ja jossa noodien välillä on korkeintaan yksi linkki. Verkoston jokainen noodi yksilöidään kokonaisluvulla väliltä $[0, n - 1]$ ja linkit lukuparilla (i, j) , jossa i ja j ovat verkoston noodien yksilöivät luvut. Siten lista noodeista ja lista linkeistä noodien välillä riittää määrittelemään verkoston.

Linkejä voidaan myös painottaa, jolloin linkille asetettu (positiivinen) reaali-luku kuvaa graafista riippuen jotakin ominaisuutta, kuten virtausta tai käyttöker-

toja. Tässä tutkielmassa graafien linkkien painot vastaavat verkon linkin kvantti-informaatiokapasiteettia.

2.1.1 Aste ja astejakauma

Verkostoteoriassa noodin aste k verkossa kertoo, kuinka moneen muuhun noodiin tarkasteltava noodi on yhdistetty. Aste on perustavanlaatuinen konsepti, jolla voidaan kvantifioida noodin yhdistyneisyyttä verkostossa ja se kertoo noodin vaikutuksesta ja tärkeydestä verkostossa.

Kaksi tärkeintä astetta ovat noodiaste ja keskimääräinen aste. Noodiasteessa suuntaamattomassa verkossa summataan noodin naapureiden, eli siihen yhdistettyjen noodien lukumäärä. Keskimääräinen aste on verkoston noodien noodiasteiden keskiarvo ja sen arvo kertoo verkoston kokonaisyhdistyneisyydestä.

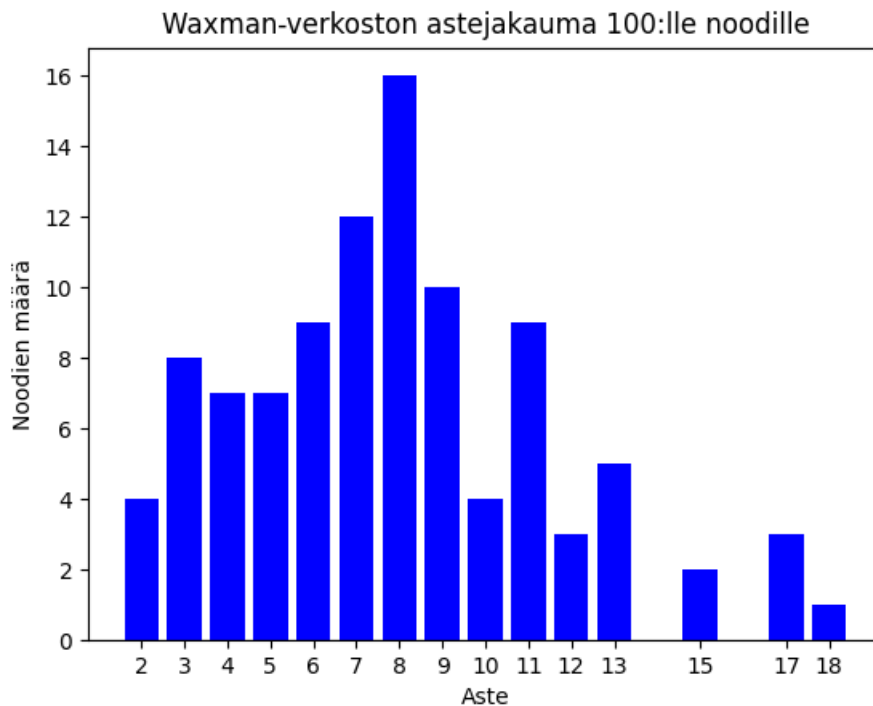
Verkoston astejakauma on myös tärkeä ominaisuus verkostolle. Nimensä mukaisesti jakauma kertoo, kuinka monta monta noodia on tiettyä astetta kohden verkossa.

2.2 Satunnaisverkot

2.2.1 Satunnaisverkoista ja $G(n, m)$ -verkko

Satunnaisverkko on verkko, jossa tietyille parametreille asetetaan kiinteät arvot, mutta verkon muut ominaisuudet määrätään satunnaisesti. Eräs yksinkertaisimmista satunnaisverkoista on $G(n, m)$ -verkko, jossa pidetään kiinteänä noodien ja linkkien lukumäärää, mutta valitaan satunnaisesti noodit joiden välille linkit muodostetaan. Satunnaisverkosta valitaan m noodiparia tasajakautuneesti kaikista mahdollisista pareista ja muodostetaan niiden välille linkki. Yleensä lisävaatimuksena on, että verkko on yksinkertainen [20].

Satunnaisverkon ominaisuuksia ei määritellä yhden generoidun verkon perusteella, vaan ne määritellään verkkojen keskimääräisten ominaisuuksien kautta. Verkois-



Kuva 2: Satunnaisen generoidun Waxman-verkoston astejakauma. $n = 100$

ta muodostetaan siis kokoelma, joka noudattaa todennäköisyysjakaumaa yli mahdollisten verkkojen, ja kokoelman keskimääräiset ominaisuudet määritellään verkon ominaisuuksiksi.

$G(n, m)$ -verkko on siis määritelty todennäköisyysjakaumana $\mathbb{P}(G)$ yli kaikkien graafien G , jossa $\mathbb{P}(G) = \frac{1}{\Omega}$, jossa Ω on graafien lukumäärä, joissa on n noodia ja m linkkiä. Esimerkiksi $G(n, m)$ -verkon halkaisija on

$$\langle l \rangle = \sum_G \mathbb{P}(G) l(G) = \frac{1}{\Omega} \sum_G l(G) \quad (40)$$

Analyttisiä tarkasteluja varten onkin hyödyllisempää tarkastella nimenomaan kokonaisuuksia. Monia satunnaisverkkojen keskimääräisiä ominaisuuksia voidaan laskea tarkasti, ainakin raja-arvona suurille verkoille. Useimmiten ollaankin kiinnostuneita verkkojen tyypillisestä käyttäytymisestä, josta verkkojen keskimääräiset ominaisuudet usein ovat hyviä indikaattoreita.

Selvästikin $G(n, m)$ -verkon keskimääräinen linkkien määrä on m ja keskimääräinen aste $k = \frac{2m}{n}$. Monet muut ominaisuudet ovat kuitenkin vaikeampia laskea ja suurin osa matemaattisesta tutkimuksesta on tehty hieman erilaiselle satunnaisverkolle, nimittäin $G(n, p)$ -verkolle.

2.2.2 Erdős–Rényi, $G(n, p)$ -verkko

$G(n, p)$ -verkostot eriävät $G(n, m)$ -verkostoista siinä, miten linkkejä muodostetaan. Tosin kuin $G(n, m)$ -verkostoissa, jossa linkkien lukumäärä m on vakio ja satunnaisuus tulee noodiparien valitsemisesta linkeille, $G(n, p)$ -verkostoissa linkki noodien välille muodostetaan todennäköisyydellä p . $G(n, p)$ -verkostoja kutsutaan usein Erdős–Rényi-verkostoiksi. Tällaisissa verkoissa todennäköisyys muodostaa verkko, jossa on m linkkiä [21] on:

$$\mathbb{P}(G) = p^m(1 - p)^{\binom{n}{2} - m} \quad (41)$$

Johtuen riippumattomuusoletuksesta linkin muodostamiselle kahden noodin välillä, $G(n, p)$ -verkkoja käytetään usein mallina, sillä sen ominaisuuksien analysointi on verrattain helppoa. Mallilla on kuitenkin paljon rajoituksia oikeiden verkostojen analysoinnissa, jossa erityisesti oletukset linkkien riippumattomuudesta ja yhtäläisistä muodostumistodennäköisyyksistä eivät ole sopivia joihinkin oikean elämän ilmiöihin. Esimerkiksi $G(n, p)$ -verkostoissa on vähäistä ryhmittymistä, toisin kuin monissa sosiaalisissa verkostoissa [22].

2.2.3 Waxman

Waxman-satunnaisverkot ovat $G(n, p)$ -verkkojen alakategoria, joissa todennäköisyys p muodostaa noodien välille linkki ei ole vakio. Waxman-satunnaisverkot [23] heijastavat sitä, että oikean maailman verkostoissa pidemmät linkit ovat usein kal-

liimpia tai hankalampia muodostaa ja siten niiden olemassaolo on vähemmän todennäköistä [24].

Waxman-verkostoissa noodien i ja j välille muodostetaan linkki todennäköisyydellä, joka on etäisyyden d_{ij} funktiona. Vaikka alkuperäinen Waxman-verkko määriteltiin käyttämällä Euklidista etäisyyttä suorakulmiossa tai suoralla viivalla, jolla on pisteet kokonaislukuruudussa ja suurin osa jatkotutkimuksista on tehty verkostoissa, jossa pisteet on asetettu satunnaisesti yksikköneliöön, ei ole mitään estettä valita pisteitä mielivaltaisella konveksilla alueella mielivaltaisella etäisyysmetriikalla [24].

Waxmanin parametrisoinnissa todennäköisyys muodostaa noodien i ja j välille linkki [23] on:

$$\mathbb{P}(d_{ij}) = \beta e^{-d_{ij}/L\alpha} \quad (42)$$

jossa $\alpha > 0$ ja $\beta \in (0,1]$. Parametri α on dimensioton suure ja riippuu tarkasteltavasta systeemistä, L on tarkasteltavan alueen suurin mahdollisin etäisyys kahden pisteen välillä. β säätelee perusmuodostumistodennäköisyyttä ja α sitä, kuinka nopeasti todennäköisyys pienenee etäisyyden kasvaessa.

2.2.4 Skaalavapaa-malli

Skaalavapaissa malleissa verkosto rakennetaan dynaamisesti: lisättäessä noodia \mathbf{x} verkostoon, se yhdistetään m :ään noodiin kaikista jo verkostossa olevista noodeista. m valitaan etukäteen ja riippuu mallinnettavasta verkosta. Noodeja \mathbf{x} ja \mathbf{x}' merkitään vektoreina, sillä niillä on koordinaatit, joita käytetään etäisyyksien laskemiseen. Todennäköisyys, että noodi \mathbf{x}' , joka on jo verkostossa, yhdistetään noodiin \mathbf{x} , on verrannollinen senhetkiseen asteeseen $D_g(\mathbf{x}')$ ja kääntäen verrannollinen etäisyyteen:

$$\Pi(\mathbf{x}, \mathbf{x}') \propto \frac{D_g(\mathbf{x})}{D(\mathbf{x}, \mathbf{x}')} \quad (43)$$

Skaalavapaiden verkkojen keskeisimpiä ominaisuuksia on *keskittyneisyys*. Keskittyneissä verkoissa suurimmalla osalla noodeista on pieni aste, ne eivät muodosta linkkejä monen muun noodin kanssa, ja pienellä osalla noodeja on runsaasti linkkejä. Skaalavapaiden verkkojen astejakauma noudattaa potenssilakia, ainakin asympototisesti:

$$\mathbb{P}(k) \sim k^{-\gamma} \quad (44)$$

Nimitys skaalavapaille verkoille juontuu niiden jakauman skaalaparametrasta: jotkin momentit astejakaumasta eivät ole määriteltyjä, joten skaalavapailta verkoilla ei ole tyypillistä skaalaa tai kokoa.

Eräs tunnetuimmista skaalavapaista verkostoista on Barabási–Albertin algoritmilla generoitu verkosto [25]. Algoritmista on vain yksi parametri m , joka on positiivinen kokonaisluku. Verkosto alustetaan $m_0 \geq m$ noodilla.

Seuraavalla askeleella algoritmista lisätään noodi h , joka yhdistetään m :ään jo verkossa olevaan noodiin. Jokaiselle verkossa jo olevalle noodille i määritellään todennäköisyys:

$$p_i = \frac{k_i}{\sum_j k_j} \quad (45)$$

jossa k_i on noodin i aste ja summa käy läpi kaikkien jo verkossa olevien noodien j asteet. Tästä muodostetusta todennäköisyysjakaumasta saadaan valittua mihin noodeihin lisättävä noodi h yhdistetään.

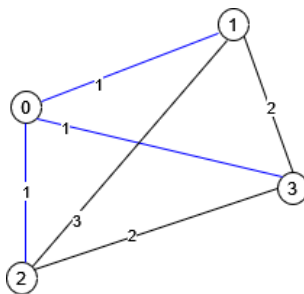
2.3 Leikkaus

Leikkauksen määrittelyyn tarvitaan myös yhdistyneisyyden määritelmä verkostolle. Graafi määritellään olevan yhdistyneeksi, jos jokaisen noodiparin välillä on yh-

teys. Toisin sanoen, jokainen verkostossa oleva noodi on yhdistetty toiseen verkostossa olevaan noodiin katkeamattomalla reitillä. Graafia, jossa on yksikin noodipari johon tämä ei päde, on yhdistämätön.

Leikkaus $C = (S, T)$ jakaa graafin $G = (V, E)$ kahteen osajoukkoon S ja T . Leikkausjoukko leikkauksesta $C = (S, T)$ on joukko linkeistä, joilla on päätepiste kummassakin osajoukossa leikkauksesta, $\{(u, v) \in E \mid u \in S, v \in T\}$. Jos graafi ei ole painotettu, leikkauksen arvo on linkkien lukumäärä jotka risteävät leikkauksen kanssa. Painotetussa tapauksessa arvo on risteävien linkkien painojen summa.

Tärkeä erikoistapaus leikkauksesta on minimileikkaus \mathbb{U} . Nimensä mukaisesti, minimileikkaus on leikkaus, jonka painojen summa on mahdollisimman pieni. Max-flow min-cut teoreeman mukaan [26] virtaus lähteeltä nieluun on yhtä suuri kuin minimileikkaus lähteeltä nielulle. Lähteenä voi kvantti-informaatioverkostoissa toimia esimerkiksi laite, joka tuottaa lomittuneita fotonipareja joita jaetaan verkostossa. Nieluna voi olla kvanttianturijärjestelmä, joka vastaanottaa lähetettyjä kvanttitiloja.



Kuva 3: Minimileikkaus noodien 0 ja 3 välillä, $\mathbb{U}_{0,3} = 3$.

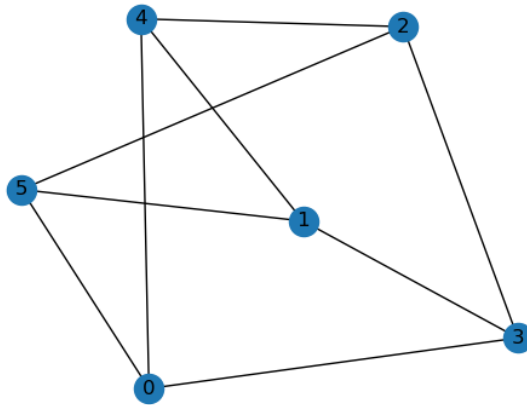
Minimileikkauksella on tärkeä rooli kommunikaatioverkostojen suunnittelussa, joita kvanttiverkostotkin ovat. Jos muutama verkoston linkeistä poistetaan tai muuten eivät toimi, verkoston välillä voi silti siirtyä informaatiota minkä tahansa kahden noodin välillä. Minimileikkaus kertoo, mikä on pienin määrä linkejä, jonka verkostosta voi poistaa kunnes on ainakin yksi noodipari, jotka eivät ole yhdistettynä toisiinsa. Minimileikkaus on siten tärkeä metriikka verkoston luotettavuudessa.

2.4 Vierekkäisyysmatriisi

Vierekkäisyysmatriisi on keino esittää verkoston rakenne ja sitä käytetään tutkielman simulaatioissa verkostojen rakentamiseen. Vierekkäisyysmatriisi \mathbf{A} määritellään seuraavanlaisesti:

$$A_{ij} = \begin{cases} 1 & \text{jos } i\text{:n ja } j\text{:n välillä on linkki} \\ 0 & \text{muuten} \end{cases} \quad (46)$$

Koska tutkielmassa tutkitaan vain yksinkertaisia verkostoja, vierekkäisyysmatriisi on (0,1)-matriisi, jossa diagonaalilla on nollia.



Kuva 4: Verkosto, jolla havainnoidaan vierekkäisyysmatriisia.

Kuvassa 4 olevan verkoston vierekkäisyysmatriisi on:

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Noodien sanotaan olevan yhdistyneitä tai naapureita, kun niiden välillä on linkki.

3 Simulaatiot

3.1 Pohjustus

Tutkielmassa simuloidaan kvantti-informaatioverkkoja, joiden parametrit ovat valittu mallintamaan amerikkalaisia valokuituverkkoja kuten lähteessä [4]. Koska verkkojen noodeilla on maantieteellinen sijainti, jokaiselle noodille asetetaan 2D-koordinaatti. Noodien väliset linkit $E_{\mathbf{x},\mathbf{x}'}$ mallinnetaan bosonisina, puhtaina, häviöllisinä kanavina [4]. Kanavan transmissiivisuus kertoo kanavan käytöstä selviävien fotonien suhdeluvun ja on:

$$\begin{aligned}\eta &= 10^{-\gamma D(\mathbf{x},\mathbf{x}')} \\ \gamma &= 0,02 \frac{1}{\text{km}}\end{aligned}\tag{47}$$

ja $D(\mathbf{x},\mathbf{x}')$ on kahden noodin välisen linkin pituus. Yksinkertaisuuden vuoksi oletetaan, että $D(\mathbf{x},\mathbf{x}')$ ja noodien välinen maantieteellinen etäisyys $\|\mathbf{x} - \mathbf{x}'\|_2$ ovat samat.

Graafin rakenne määrätään asettamalla noodeille sijannit ja generoimalla niiden välille linkit. N :lle noodille valitaan tasajakaumasta neliön muotoisesta alueesta pisteet, joihin ne asetetaan.

$$\begin{aligned}\Omega_R &\equiv [-R, R] \times [-R, R] \\ |\Omega_R| &= 4R^2\end{aligned}\tag{48}$$

R :n arvoksi valittiin simulointeihin $R = 800$ km.

Koska protokollia on erilaisia, tutkitaan simulaatioissa suurinta saavutettavaa lomittumisen jakamistehoa. Toisin kuin klassisessa kommunikaatiossa [18], suurin mahdollinen siirrettävä määrä kvantti-informaatiota jokaiselle linkille rajoittuu perustavanlaatuisesti kanavan häviöllisyyden mukaan. Määritetään linkin kapasiteetiksi:

$$\mathcal{C}_E(E_{\mathbf{x},\mathbf{x}'}) = -\log_2(1 - \eta) = -\log_2(1 - 10^{-\gamma D(\mathbf{x},\mathbf{x}')})\tag{49}$$

joka on yhtä kuin PLOB-yläraja. Verkon kokonaiskapasiteetiksi määritellään yksinkertaisesti verkon linkkien kapasiteetin keskiarvoksi:

$$\langle \mathcal{C} \rangle = \frac{1}{|E|} \sum_{E_{\mathbf{x}, \mathbf{x}'}} \mathcal{C}_E(E_{\mathbf{x}, \mathbf{x}'}) \quad (50)$$

jossa $\frac{1}{|E|}$ on verkon linkkien kardinaliteetti. Yksittäisen noodin tärkeyttä karakterisoidaan määritellään noodikapasiteetti:

$$\sum_{\mathbf{x}' \in \mathcal{N}(x)} \mathcal{C}_N(x) \quad (51)$$

joka on yksittäiseen noodiin tulevien linkkien painojen summa.

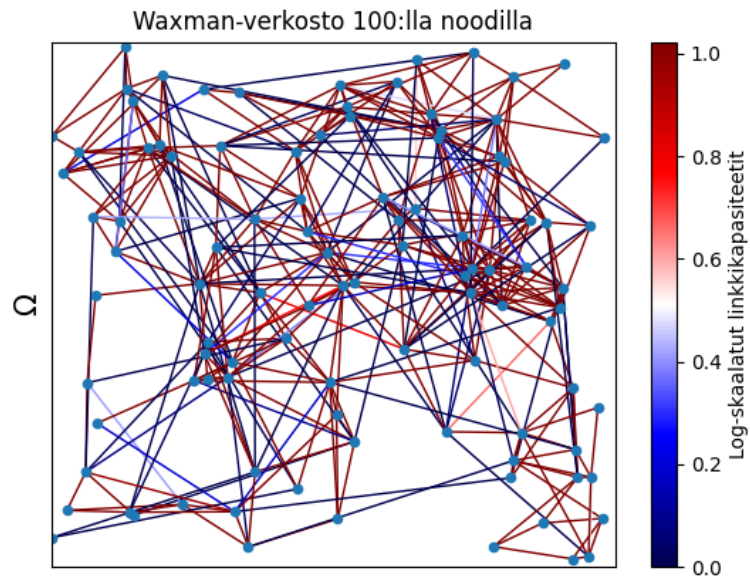
Verkostojen päätepisteiden kapasiteetti saadaan ratkaistua ottamalla minimileikkaus. Täten kapasiteetti kahden noodin välillä \mathbf{x} ja \mathbf{x}' on niiden linkkiyhdistyneisyys [18]:

$$\min_{\mathbb{U}_{\mathbf{x}, \mathbf{x}'}} \mathcal{C}_U(\mathbb{U}_{\mathbf{x}, \mathbf{x}'}) \equiv \min_{\mathbb{U}_{\mathbf{x}, \mathbf{x}'}} = \sum_{E_{\mathbf{y}, \mathbf{y}'} \in \mathbb{U}_{\mathbf{x}, \mathbf{x}'}} \mathcal{C}_E(E_{\mathbf{y}, \mathbf{y}'}) \quad (52)$$

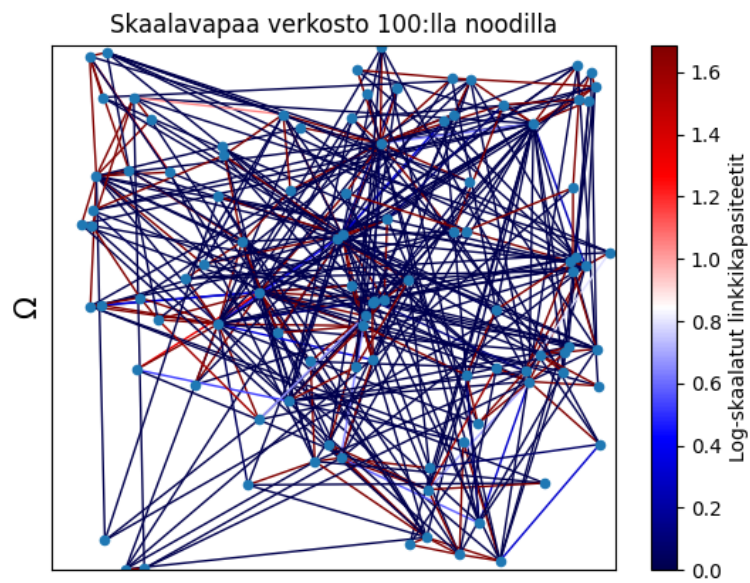
3.2 Esimerkkejä

Tässä osiossa generoidaan muutamia Waxman- ja skaalavapaita verkkoja ja esitellään niiden kapasiteettien sekä astejakaumien kuvaajat. Verkkojen kuvia varten linkit ovat värikoodattu, linkkien väri kuvastaa niiden kapasiteetin suuruutta suhteessa verkon muihin linkkeihin. Linkkien kapasiteeteista otettiin kymmenkantainen logaritmi kuvia varten, sillä kapasiteettien kokoluokat, ja siten myös eroavaisuudet, ovat hyvin pieniä. Ottamalla logaritmi saatiin värikoodaus toimimaan paremmin ja logaritmoidut kapasiteetit myös normalisoitiin.

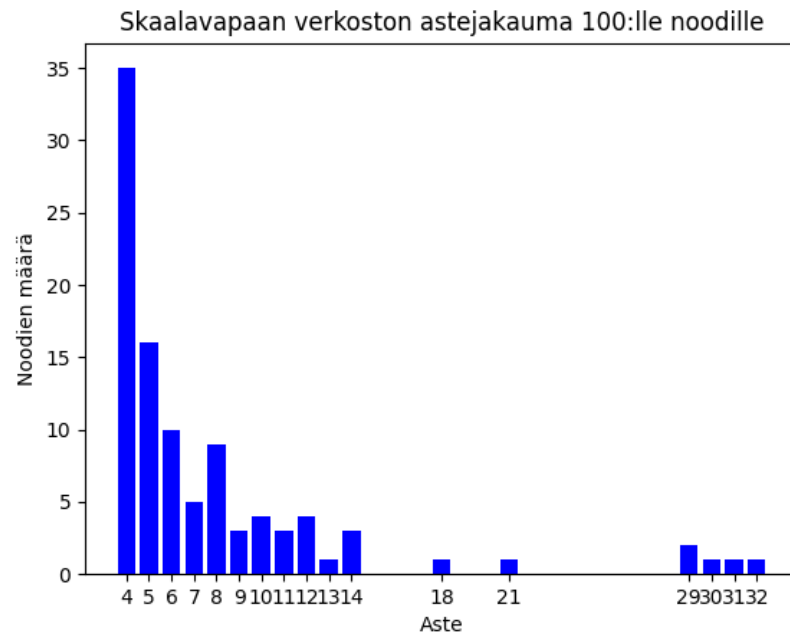
Simulaatio tehtiin Pythonilla, käyttäen networkx-kirjastoa generoimaan verkot ja laskemaan niiden ominaisuuksia.



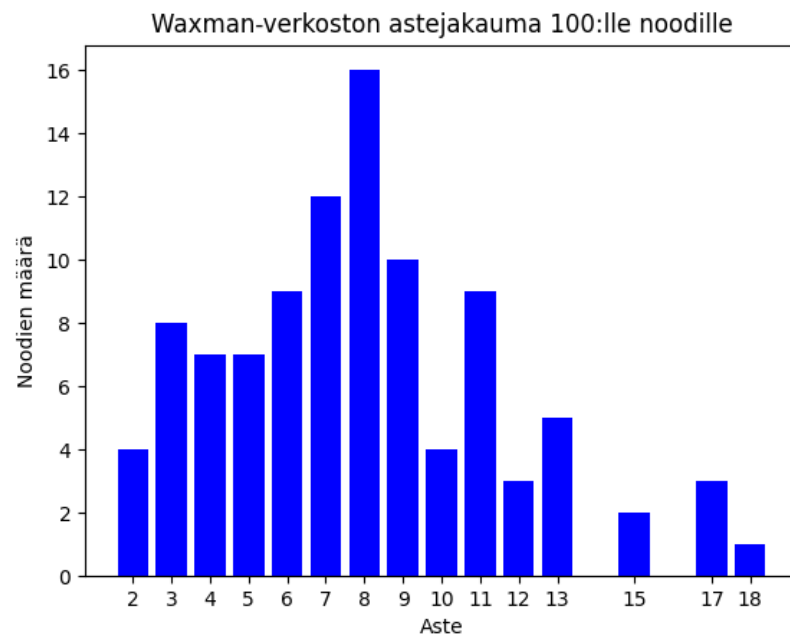
Kuva 5: Erään sadan noodin Waxman-verkosto alueella Ω .



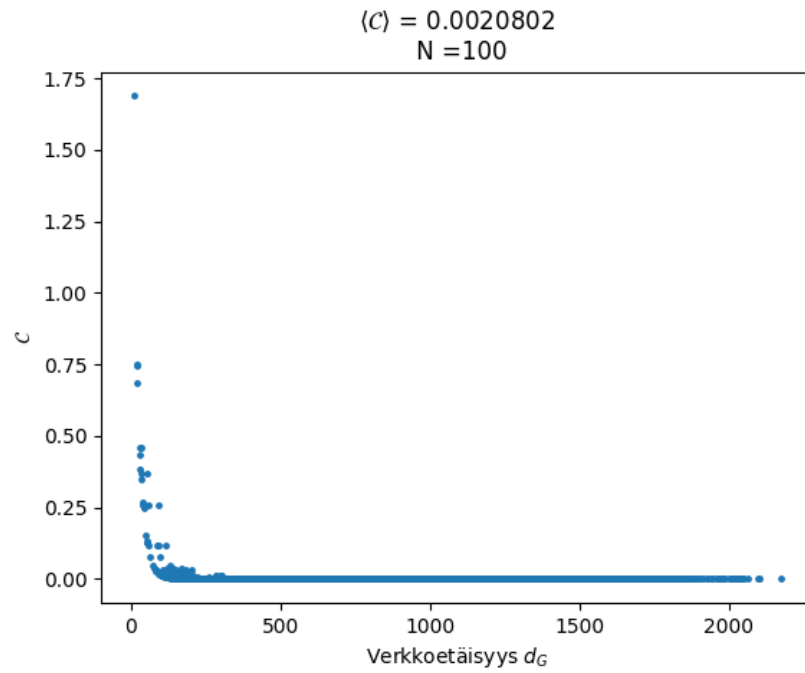
Kuva 6: Erään sadan noodin skaalavapaa verkosto alueella Ω .



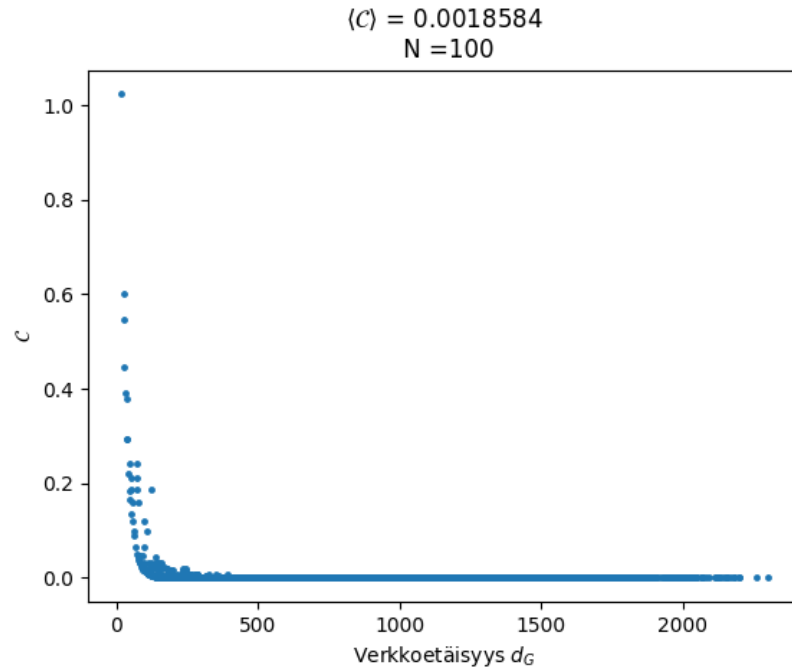
Kuva 7: Yllä olevan sadan noodin skaalavapaan verkon astejakauma



Kuva 8: Yllä olevan sadan noodin Waxman-verkon astejakauma



Kuva 9: Sadan noodin skaalavapaan verkon linkkien kapasiteetti verkkoetäisyyden funktiona.



Kuva 10: Sadan noodin Waxman-verkon verkon linkkien kapasiteetti verkkoetäisyyden funktiona.

3.2.1 Esimerkkien esittely

Waxman-verkoilla ja skaalavapailla on muutamia ominaisuuksia, jotka ovat nähtävissä verkkojen kuvista. Waxman-verkoissa on merkittävästi vähemmän linkkejä kuin skaalavapailla verkoilla ja niiden linkkien kapasiteetit ovat keskimäärin suurempia. Linkkien kapasiteetit ovat tasaisemmin jakautuneet Waxman-verkoissa. Skaalavapaassa verkossa näkyy enemmän keskittyneisyyttä linkkien vahvuuksissa, joka näkyy punaisten rykelmien muodostumisena kuvassa.

Verkkojen astejakaumissa on huomattava ero: ylivoimaisesti suurimmalla osalla noodeista niiden aste on m ja muutamalla noodilla on selvästi tätä suurempi aste, kuvaten hyvin skaalavapaiden ominaisuutta keskuksien muodostamiseen.

Verkkojen linkkien kapasiteetin kuvaajat ovat verkkoetäisyyden funktiona. Verkkoetäisyys kahden nooden välillä määritellään niiden välillä olevien linkkien pituuksien pienimpänä summana, jolla yhdestä noodista pääsee toiseen. Jos noodien välillä ei ole reittiä, verkkoetäisyys määritellään äärettömäksi. Kuvaajissa on jokaisen mahdollisen noodiparin kapasiteetti parin verkkoetäisyyden funktiona koko verkon keskimääräinen kapasiteetti, joka on yksinkertaisesti linkkien kapasiteettien keskiarvo. Kuten kuvaajista näkyy, korkeilla verkkoetäisyyksillä yhteyksiä ei muodostu.

Kuvaajat ovat yksittäisten verkkojen toteuneita ilmentymiä satunnaisjakaumasta, eikä Waxman- tai skaalavapaiden verkkojen ominaisuuksia pystytä vielä määrittelemään yksittäisten ilmentymien perusteella. Kuitenkin esimerkeissä generoidun Waxman-verkon kapasiteetti on odotetusti sadan noodin Waxman-verkkojen keskimääräisen kapasiteetin marginaalien sisällä, jotka ovat esiteltynä artikkelissa "Quantum communication capacity transition of complex quantum networks" [4].

4 Yhteenveto

Tutkielmassa tutkittiin Waxman-verkoston ja skaalavapaiden verkoston päätepisteiden kvanttikapasiteettia ja generoitiin havainnollistusta varten sadan noodin Waxman-verkosto ja skaalavapaa verkosto. Kvantti-informaatioverkoston käsittelemiseen ja ymmärtämiseen määriteltiin linkkien kapasiteetit, kapasiteettien ylärajat PLOB-ylärajaa käyttämällä, minimileikkauksen yhteys verkon kokonaiskapasiteettiin sekä kvanttiteleportaation ja lomittumisen käyttö kvantti-informaation siirtämiseen. Satunnaisverkot ja kuinka niiden tilastolliset ominaisuudet voidaan määrittellä esiteltiin ja Waxman-verkoston sekä skaalavapaiden verkoston ominaisuudet ja muodostaminen määriteltiin. Esiteltyjä konsepteja käyttäen saatiin määriteltyä satunnaisverkon suurin teoreettinen kapasiteetti ja simulaatioissa laskettua konkreettisia arvoja.

Generoidut satunnaisverkot olivat vain yksittäisiä ilmentymiä verkkojen todennäköisyysjakaumista, eikä niiden ominaisuuksista voitu todeta enempää, kuin että ne olivat artikkelissa "Quantum communication capacity transition of complex quantum networks" [4] laskettujen rajojen sisällä. Seuraavana luonnollisena askeleena olisi laskea tilastolliset ominaisuudet verkoille eri määrällä noodeja ja tutkia, noudattavatko ne tunnettuja jakaumia sekä kuinka alueen koon muuttaminen vaikuttaa ominaisuuksiin.

Viitteet

- [1] N. A. Lynch, *Distributed algorithms* (Elsevier, 1996).
- [2] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston ja A. V. Gorshkov, *Physical Review A* **97**, (2018).
- [3] M. Tomamichel ja A. Leverrier, *Quantum* **1**, 14 (2017).

- [4] Q. Zhuang ja B. Zhang, *Physical Review A* **104**, (2021).
- [5] A. Acín, J. I. Cirac ja M. Lewenstein, *Nature Physics* **3**, 256–259 (2007).
- [6] P. Kok, *A first introduction to quantum physics, Undergraduate lecture notes in physics* (SpringerCham, Switzerland, 2018).
- [7] P. A. M. Dirac, *Mathematical Proceedings of the Cambridge Philosophical Society* **35**, 416–418 (1939).
- [8] M. Born, *Zeitschrift fur Physik* **37**, 863 (1926).
- [9] R. Horodecki, P. Horodecki, M. Horodecki ja K. Horodecki, *Reviews of Modern Physics* **81**, 865 (2009).
- [10] R. Horodecki, P. Horodecki, M. Horodecki ja K. Horodecki, *Reviews of Modern Physics* **81**, 865 (2009).
- [11] J. S. Bell, *Physics Physique Fizika* **1**, 195 (1964).
- [12] J. Clauser, M. Horne, A. Shimony ja R. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [13] R. Horodecki, P. Horodecki, M. Horodecki ja K. Horodecki, *Reviews of Modern Physics* **81**, 865–942 (2009).
- [14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin ja W. K. Wootters, *Physical Review Letters* **76**, 722–725 (1996).
- [15] M. Horodecki, P. Horodecki ja R. Horodecki, *Physical Review Letters* **80**, 5239–5242 (1998).
- [16] L. Gyongyosi ja S. Imre, *ArXiv* **abs/1208.1270**, (2012).
- [17] S. Pirandola, R. Laurenza, C. Ottaviani ja L. Banchi, *Nature Communications* **8**, 15043 (2017).

- [18] S. Pirandola, *Communications Physics* **2**, 51 (2019).
- [19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres ja W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [20] M. Newman, kirjassa *Networks, An Introduction* (Oxford University Press Inc., New York, 2010), p. 110.
- [21] P. Erdős ja A. Rényi, *Publicationes Mathematicae Debrecen* **6**, 290 (1959).
- [22] A. Saberi, *Physics Reports* **578**, (2015).
- [23] B. Waxman, *IEEE Journal on Selected Areas in Communications* **6**, 1617 (1988).
- [24] M. Roughan, J. Tuke ja E. Parsonage, (2015).
- [25] R. Albert ja A.-L. Barabási, *Reviews of Modern Physics* **74**, 47 (2002).
- [26] G. B. Dantzig ja D. R. Fulkerson, kirjassa *On the Max Flow Min Cut Theorem of Networks*. (RAND Corporation, 1955).