Äärellisten yrityskertojen vaikutus kvanttikommunikaation tehokkuuteen

LuK-tutkielma
Turun yliopisto
Fysiikka
2026
LuK Jaakko Ekqvist
Tarkastaja:
FT Johannes Nokkala

TURUN YLIOPISTO
Fysiikan ja tähtitieteen laitos

Jaakko Ekqvist Äärellisten yrityskertojen vaikutus kvanttikommunikaation tehokkuuteen

LuK-tutkielma, 28 s., 0 liites.
Fysiikka
Maaliskuu 2026

Kvanttikommunikaatioverkot ovat monimutkaisia tietoliikkenneverkkoja, jotka hyödyntävät informaation siirrossa kvanttimekaanisia ilmiöitä. Tässä tutkielmassa keskitytään kvanttiverkkohin, jotka perustuvat lomittuneiden tilojen jakamiseen. Tutkielmassa keskitytään tarvittavien operaatioiden kuvaamiseen yksinkertaistavien mallien avulla.

Tekstissä keskitytään erityisesti kvanttikommunikaatioverkkojen kapasiteetin aikariippuuvuuteen. Kapasiteetti kertoo kuinka paljon informaatiota verkko kykenee välittämään. Lomittumiseen perustuvissa verkoissa tämä voidaan rinnaistaa lomittuneiden tilojen määrään. Kapasiteettia mallinnetaan yksinkertaisille verkkotopoligioille Python-simulaatioilla, jotka perustuvat Markovin ketjuihin.

Asiasanat: Kvanttikommunikaatioverkot, Verkkoteoria, Markovin ketjut, Kvanttiverkon kapasiteetti

Sisällys

Johdanto

Kommunikaatioverkkojen tehtävä on välittää informaatiota kahden tai useamman käyttäjän välillä. Kvanttikommunikaatioverkoissa hyödyntävät tähän erilaisia kvanttimekaanisia ilmiöitä, kuten lomittumista [1]. Niiden merkittävin etu verrattuna klassisiin verkkoihin on kommunikaation turvallisuus, joka perustuu kvanttimekanisiin periaatteisiin, kuten kloonaamattomuusteoriaan [2]. Nykyään kokeellisia kvanttikommunikaatioverkkoja on rakennettu jo useita, joista tällähetkellä suurin on Kiinassa oleva China Quantum Communication Network (CN-QCN), joka koostuu 145 noodista. Huolimatta nopeasta kehityksestä ala on vielä alkuvaiheessa. Suurinkin kokeellinen kvanttikommunikaatioverkko pystyy yhdistämään vain noin 800 käyttäjää, mikä on hyvin pieni verrattuna klassisiin verkkoihin kuten internettiin [3].

Merkittävä tutkimuskohde on kvanttikommunikaativerkkojen kapasiteetin, eli informaation siirtokyvyn tutkiminen. Kvanttikommunikaatioverkon kapasiteetti saavuttaa maksimiarvonsa, jos lomittuneiden tilojen jakamista voidaan yrittää ääröttämän monta kertaa [4]. Koska todelliset kvanttiverkot voivat olla päällä vain äärellisiä aikoja, ei yrityskertojakaan voi olla ääretöntä määrää. Yleisesti käytetty menetelmä verkon kapasiteetin tutkimiseen on määrittää keskimääräinen odotusaika (engl. waiting time) verkossa [5–7]. Se kuvaa aikaa, joka verkolla kestää muodostaa kommunikointiin käytettävä lomittunut tila. Tässä tekstissä käytetään samaa ideaa, mutta kapasiteetti määritetään mallintamalla suoraan lomittuneiden tilojen määrää verkossa.

Tutkielmassa esitellään ensin verkkoteorian tarvittavat käsitteet, ja kvanttikommunikaatioverkon toiminta yleisesti. Erityisesti painotetaan verkon mallintamista, ja siinä tehtäviä valintoja. Esimerkkinä ominaisuudesta, jota voidaan tutkia simuloimalla, käytetään kvanttiverkon kapasiteettia, eli kykyä välittää informaatiota. Tähän liittyen esitellään hieman teoriaa, jonka jälkeen tutkitaan muutaman yksinkertaisen verkkorakenteen kapasiteetteja. Simulaatiot toteutetaan Pythonilla, ja nii-

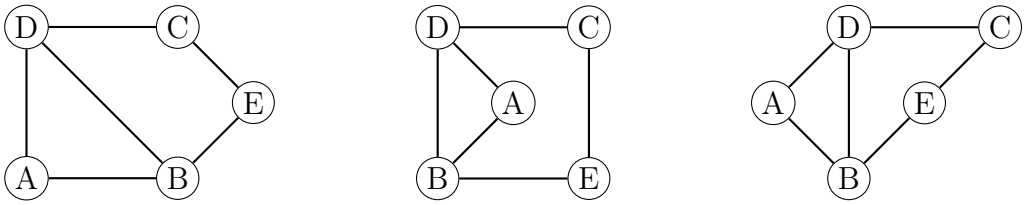
hin esitetään Markovin ketjuihin perustuva menetelmä, jolla kyetään mallintamaan pieniä, korkeintaan muutaman kymmenen noodin kokoisia, mielivaltaisia kvanttikommunikaatioverkkoja.

1 Verkkoteorian tarpeelliset käsitteet

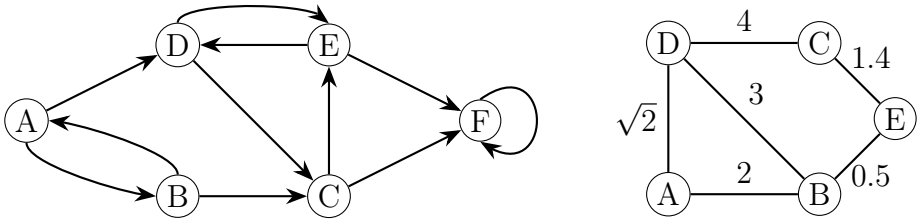
Verkkoteoria, joskus kutsutaan myös graafiteoriaksi ja verkkoja vastaavasti graafeiksi, on matematiikan osa-alue, joka tutkii riippuvuussuhteita kuvaamalla niitä verkkoina. Historiallisesti verkkoteoriaa on ensimmäisen kerran käytetty ratkaisemaan Königsbergin siltaongelma. Siinä etsitään reittiä, joka kiertäisi Königsbergin kulkemalla vain kerran jokaisen seitsemän sillan kautta. Vuonna 1736 Leonhard Euler todisti, ettei tällaista reittiä ole olemassa, ja loi samalla verkkoteorian perusteet. Nykyään verkkoteoriaa käytetään monissa sovelluksissa, kuten jakeluketjuissa, bioinformatiikassa ja ohjelmistotuotannossa [8]. Koska kommunikaatioverkkojen tehtävä on yhdistää usea käyttäjä toisiinsa, on niitä luonnollista kuvata verkkoina. Seuraavaksi esitellään muutamia verkkoteorian peruskäsitteitä, joita tekstissä käytetään. Matemaattinen notaatio noudattelee löyhästi lähteessä [9] käytettyä.

Verkko (engl. graph) G on verkkoteorian perusrakenne. Se koostuu äärellisestä määrästä noodeja (engl. vertex/node) V, sekä linkkejä (engl. edge/link) E. Noodi on verkon yksittäinen piste, eli se kuvaa verkon alkiota. Merkitään yksittäistä noodia $x_i \in V(G)$, missä $V(G)$ on verkon G noodien joukko. Linkit taas yhdistävät noodeja, eli ne kuvaavat alkioiden keskinäistä riippuvuussuhdetta. Vastaavasti linkkien joukosta käytetään merkintää $E(G)$. Jos noodit x_i ja x_j ovat yhdeydessä linkkeillä, merkitään $x_i \sim x_j$.

Verkot voidaan jakaa kahteen osaan riippuen niiden linkkien laadusta, suuntaamattomiin ja suunnattuihin. Suuntaamattomissa verkoissa linkit osoittavat vain, että kaksi noodia on riippuvuussuhteessa. Esimerkiksi Königsbergin siltaongelmaa kuvaa suuntaamaton verkko, jossa sillat ovat linkkejä ja alueet, joita ne yhdistävät,



Kuva 1: Kuvassa on esitetty sama suuntaamaton painoittamaton verkko piirrettynä kolmella eri tavalla. Kaikki verkot kuvaavat siis samanlaista systeemiä.



(a) Suunnattu verkko

(b) suuntaamaton painoitettu verkko

Kuva 2: Esimerkit a, suunnatusta painoittamattomasta verkkorakenteesta, sekä b, suuntaamattomasta painotetusta verkkorakenteesta. Kuvassa b oleva verkko on samanmuotoinen kuin kuvan 1 painoittamaton verkko.

noodeja. Verkko on suuntaamaton, koska ongelmassa siltaa voidaan kulkea kumpaan suuntaan tahansa. Suunnatuissa verkoissa taas linkit ovat vain yksisuuntaisia. Näitä käytetään, jos riippuvuussuhteessa suunnalla on merkitys. Esimerkiksi alueen vesijohtoverkkoa voitaisiin kuvata tällaisella verkolla, jossa vesiputket ovat suunnattuja linkkejä. Vesi kulkee vain yhteen suuntaan, joten nyt mallissa on tarpeen määritellä suunta.

Graafisesti verkon noodit kuvataan pisteinä. Suuntaamattomassa verkossa näitä yhdistävät linkit kuvataan pisteitä yhdistävinä viivoina. Vastaavasti suunnatussa verkossa linkit ovat nuolia, joilla implikoidaan riippuvuussuhteen suunta. On huomattava, että verkon graafinen esitys ei ole yksikäsitteinen, vaan sama verkko voidaan piirtää usealla eri tavalla. Kuvassa 1 on piirretty sama suuntaamaton verkko kolmella eri tavalla. Matemaattisesti verkkoa kuvataan viereisyysmatriisilla M_G, mistä nähdään, ovatko kaksi noodia yhteydessä. Numeroidaan verkon G noodit

$V(G) = \{x_1,x_2,x_3,...,x_{v_g}\}$, missä $v_g = |V(G)|$ noodien lukumäärä verkossa. Vierekkäisyysmatriisi M_G suuntaamattomalle verkolle matriisi, jonka matriisialkiot ovat

$$m_{ij} = \begin{cases} 1 \text{ jos } x_i \sim x_j \\ 0 \text{ muuten.} \end{cases} \tag{1}$$

Selvästi suuntaamattomalla verkolla matriisi on aina symmetrinen. Esimerkiksi kuvan 1 verkon vierekkäisyysmatriisiksi saadaan

$$(m_{ij}) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \tag{2}$$

kun $x_1 = A$, $x_2 = B$, ja niin edelleen. Vastaavasti suunnatulla verkolla vierekkäisyysmatriisin alkiot ovat

$$m_{ij} = \begin{cases} 1 \text{ jos on olemassa linkki } x_i\text{:stä } x_j\text{:hin} \\ 0 \text{ muuten.} \end{cases} \tag{3}$$

Tässä on huomattava, että matriisista ei tule enää symmetristä. Kuvassa 2a esitetylle suunnatulle verkolle saadaan matriisiksi

$$(m_{ij}) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4}$$

Näin kirjoittamalla jokaista verkkoa vastaa yksikäsitteinen matriisi. Voidaankin määritellä, että kaksi verkkoa ovat samat, jos niiden vierekkäisyysmatriisit ovat samat.

Tietyissä sovelluksissa kuten kvanttikommunikaatioverkoissa kaikki linkit eivät kuitenkaan ole samanarvoisia. Esimerkiksi vesijohtoverkon kaikki putket eivät välttämättä ole saman kokoisia. Jos verkkoteoreettisesti haluttaisiin tarkastella sen kapasiteettia, tämä pitäisi ottaa huomioon. Näissä sovelluksissa käytettään painoitettuja verkkoja, joissa linkeille annetaan painokertoimet. Vesijohtoverkossa ne olisivat siis putkien kapasiteetteja. Tällöin vierekkäisyysmatriisiin sijoitetaan 1:sen tilalle linkin painokerroin. Kuvassa 2b on esimerkki kuvan 1 verkosta painoitettuna. Tämän verkon vierekkäisyysmatriisi on siis

$$(m_{ij}) = \begin{pmatrix} 0 & 2 & 0 & \sqrt{2} & 0 \\ 2 & 0 & 0 & 3 & 0.5 \\ 0 & 0 & 0 & 4 & 1.5 \\ \sqrt{2} & 3 & 4 & 0 & 0 \\ 0 & 0.5 & 1.5 & 0 & 0 \end{pmatrix}. \tag{5}$$

2 Kvanttikommunikaatioverkko

2.1 Kvanttikommunikaation käyttökohteet

Kvanttikommunikaatioverkot hyödyntävät kvanttimekaniikan ilmiöitä, kuten lomittumista, tiedonsiirrossa, mikä tuottaa monia etuja klassisiin verkkoihin nähden. Näitä ovat muun muassa tiiviskoodauksella (engl. superdense coding) informaation siirtäminen tiiviimmässä muodossa [10], sekä huomattavasti nykyisiä tarkempi kello synkronoimalla usea atomikello keskenään kvanttiverkossa [11].

Yksi pisimmälle kehitetyistä sovelluksista on kuitenkin kvanttikryptografiset menetelmät, jotka tekevät kvanttikommunikaatiosta huomattavasti klassista turvallisempia [2]. Ensimmäisen kvanttikryptografisen protokollan BB84 esittivät Bennett ja Brassard vuonna 1984. Se mahdollistaa turvallisen avaimenjaon avoimen yhteyden yli [12]. Vaikka kyseinen protokolla ei vaadi lomittumiseen perustuvia kvanttiverkkoja, vähentää niiden käyttö protokollassa tapahtuvia häiriöitä [2]. Monia muita

kvanttiavaimenjakoprotokollia on BB84:n jälkeen esitelty, joista osa tarvitsee myös lomittumista toimiakseen. Näistä esimerkiksi 1991 Ekertin esittämä ERB-protokolla käyttää lomittuneita Bellin tiloja avaimenjakoon [2].

Kvanttikryptografisten menetelmien perustana on suurilta osin kloonaamattomuusteoreema, jonka mukaan tuntematonta kvanttitilaa ei ole mahdollista kopioida täydellisesti [13]. Salakuuntelija ei siis kykene tuottamaan salausavaimesta kopiota ilman, että hän joutuu mittamaan kubittien tilan. Kubittien tilan mittaus taas muuttaa sitä, joten salakuuntelija kyetään havaitsemaan muuttuneesta viestistä [14].

2.2 Kvanttikommunikaatioverkon toimintaperiaate

Kvanttikommunikaatioverkot siirtävät informaatiota kubiteilla. Kuten klassisilla biteillä, kubiteilla on kaksi toisistaan erotettavaa tilaa. Esimerkiksi ne voivat olla fotonin pysty- ja vaakapolarisaatiotilat. Kvantti-informaatiossa usein, ja myös tässä tekstissä, kubitin tiloista käytetään vain yleisnimityksiä $|0\rangle$ ja $|1\rangle$, ottamatta kantaa fysikaaliseen systeemiin, jota se kuvaa. Erona klassisiin bitteihin, kubitti voi kuitenkin olla näiden superpositiossa, mikä mahdollistaa kvanttimekaaniset ilmiöt [14].

Kvanttikommunikaatioverkot koostuvat kvanttitoistimista (engl. quantum repeater), sekä näiden välisistä viestintäkanavista. Kvanttitoistimet koostuvat kvanttimuisteista sekä kvanttiporteista. Kvanttiportit operoivat kubitteihin muuttaen niiden tiloja. Tämä mahdollistaa lomittumisen vaihdot sekä korjausoperaatiot [15]. Kvanttimuistit taas säilyttävät kubitin tilan muuttumattomana niin, että se on mahdollista nopeasti siirtää muistiin ja sieltä pois. Viestintäkanavia on kvanttikommunikaatioverkossa kahdenlaisia: klassisia ja kvanttikanavia. Kvanttikanavia pitkin siirretään fyysisiä kubitteja kvanttitoistimien välillä. Klassiset kanavat vastaavasti käyttävät klasissia bittejä. Näitä hyödynnetään muun muassa virheenkorjausoperaatiossa, jossa toinen kvanttitoistin tarvitsee toisen tekemästä operaatiosta jonkun

tiedon [1].

Kvanttiverkot siis siirtävät kubitin tilan lähettäjältä vastaanottajalle. Jos matka on lyhyt, voidaan kubitti lähettää fyysistä kanavaa, esimerkiksi fotonien tapauksessa valokuitua, pitkin. Mikään todellinen kvanttikanava ei kuitenkaan ole täydellinen, vaan siellä on häiriöitä, jotka aiheuttavat kubitin tilaa virheitä. Tämä rajoittaa voimakkaasti etäisyyksiä, joilla näin voidaan kommunikoida, koska virheiden kertyessä informaatiota ei enää saa luettua kubiteista [16]. Käytännössä maanpäällä valokuidussa maksimietäisyyksiksi on mahdollista saada satojen kilometrien suuruusluokkaa [17]. Avaruudessa satelliittien välillä on mahdollista saavuttaa pidempiäkin etäisyyksiä [18].

Pidemmillä matkoilla fyysisesti kubittien siirtäminen paikasta toiseen ei siis ole enää kannattavaa. Tämän sijaan kubitin tila siirretään kvanttiteleportaatiolla. Siinä tila siirretään lomittuneen tilan avulla ilman, että fyysistä kanavaa tarvitaan. Tämä siirto tuhoaa lomittuneen tilan, eli jokaista kubittia varten tarvitaan oma tila [19]. Siten kvanttikommunikaatioverkon merkittäväksi tehtäväksi tulee lomittuneiden tilojen luominen ja jakaminen kvanttimuistien välillä. Kvanttitoistimissa tämä toteutetaan käyttäen klassista kommunikaatiota ja lokaaleja operaatoita, eli operaatioita jotka voidaan toteuttaa kokonaan yhden kvanttitoistimen sisällä (LOCC) [15]. Käytännössä siis, jos A:n ja B:n välillä on lomittunut tila, ja B:n ja C:n välillä toinen, saadaan lomittumisen vaihdolla luotua näistä yksi lomittunut tila A:n ja C:n välille.

Kahden muistin välille lomittuneen tilan luonti onnistuu siis seuraavasti. Kvanttimuisteissa luodaan kahden tai useamman kubitin lomittunut tila. Kubitit jaetaan vierekkäisten muistien välillä. Kvanttitoistimissa suoritetaan lomittumisen vaihtoja niin, että saadaan lomittunut tila haluttujen muistien välille [20]. Monimutkaisemmissa verkkorakenteissa ei välttämättä ole ilmeistä, mitkä lomittumisen vaihdot kannattaa tehdä, sillä kaksi kvanttimuistia on mahdollista yhdistää montaa eri kaut-

ta. Tällöin käytetään hyödyksi reititysalgoritmeja, jotka laskevat optimaalisen reitin haluttujen parametrien mukaan, esimerkiksi minimoimalla tarvittavat lomittumisen vaihdot [21].

Kaikissa edellämainituissa operaatioissa lomittuneeseen tilaan on mahdollista syntyä virheitä, jolloin tilan lomittuminen heikkenee, tai mahdollisesti jopa tuhoutuu kokonaan. Näitä aiheuttavat muun muassa lomittumisen vaihdossa käytettyjen kvanttiporttien epätäydellisyys sekä ympäristön häiriöt [22]. Myöskään kvanttimuistit eivät kykene säilyttämään tilaa muuttumattomana mielivaltaisen kauaa, vaan muistissa tapahtuu dekoherenssia, joka muuttaa sitä. Dekoherenssi siis rajoittaa aikaa, jota kubitti voi odottaa lomittumisen vaihtoa ja kvanttiteleportaatiota. Mainittakoon, että nykyään kyetään tuottamaan muisteja, joissa tila säilyy tarpeeksi hyvin yli 6 ms, mikä mahdollistaa kokeellisten lomittumisen vaihtoon perustuvien kvanttiverkkojen rakentamisen [23]. Virheitä varten on myös kehitetty virheenkorjausalgoritmejä, jotka muun muassa kykenevät tislaamaan (engl. distilling) lomittumista, eli muodostamaan useasta heikosti lomittuneesta tilasta yhden voimakkaammin lomittuneen [7].

2.3 Kvanttikommunikaatioverkon mallintaminen

Matemaattisesti kvanttikommunikaatioverkkoja voidaan kuvata verkkoteoreettisesti. Verkon noodit ovat kvanttitoistimia ja/tai muisteja ja niiden väliset linkit klassisia ja kvanttikanavia. Mallinnettaessa esimerkiksi verkon kapasiteettia annetaan linkeille painokertoimet kanavien kapasiteettien, eli informaation välityskyvyn perusteella. Tällöin mallinnuksessa voidaan hyödyntää verkkoteorian tuloksia, ja yksinkertaisilla verkoilla analysointi voidaan tehdä jopa täysin teoreettisesti. [5]

Verkon koon kasvaessa sen analyyttinen käsittely muuttuu nopeasti työlääksi jolloin verkkoja kannattaa mallintaa numeerisesti [6]. Numeerisissa malleissa joudutaan aina tekemään jotain yksinkertaistuksia ja oletuksia. Kvanttiverkkoja tutkiessa

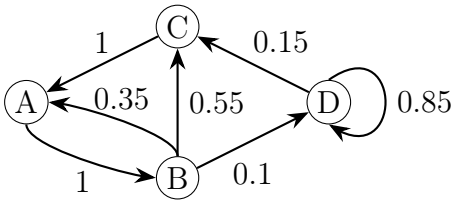
joudutaan valitsemaan, miten lomittumisen vaihdon operaatiota mallinnetaan ja miten verkossa tapahtuvat virheet otetaan huomioon. Yksinkertaisemmissa malleissa lomittumisen tislaus voidaan jättää huomiotta. Jos syntyneen tilan lomittuneisuus on liian heikko, silloin se hylätään. Tällöin voidaan lomittuneen tilan luomiselle ja lomittumisen vaihdoille ottaa vain kiinteät onnistumistodennäköisyydet. Malleissa, jossa lomittumisen tislaus otetaan huomioon, tarkastellaan vielä erikseen sen onnistumista, jolloin lomittumisen vaihdon todennäköisyyden arvo riippuu tislauksella saadusta tilasta [5].

Vastaavasti kvanttimuistien dekoherenssi taas on yksinkertaisin huomioida olettamalla, että tila säilyy muuttumattomana muistissa tietyn ajan, jonka jälkeen se poistetaan sieltä. Tässä mallissa siis käytännössä hylätään tilat sitten kun niihin on kertynyt virhettä niin paljon, että se vaikuttaisi muiden operaatoiden onnistumisiin [5]. Tarkemmissa malleissa dekoherenssin aiheuttama lomittumisen heikentyminen voidaan huomioida lomittumisen vaihdon yhteydessä, valitsemalla sen onnistumistodennäköisyys riippumaan lomittuneiden tilojen olemassaoloajasta. Käytännössä siis todennäköisyys lomittumisen vaihdolle on sitä pienempi, mitä kauemmin tilat ovat olleet muistissa [24].

Kvanttikommunikaatioverkon mallinnukseen on useita erilaisia numeerisia menetelmiä, kuten Monte Carlo simulaatiot, ja todennäköisyysjakaumiin perustuvat [25]. Tutkielmassa keskitytään Markovin ketjuiin, jotka ovat laajasti käytetty numeerinen menetelmä. Kvanttikommunikaatioverkkojen toiminnan mallintamisessa niitä on käytetty erityisesti kvanttitoistimien [6, 7] , sekä kvanttikytkimien (engl quantum switch) [26–28] tutkimiseen.

2.3.1 Markovin ketjujen toimintaperiaate

Markovin ketjut ovat menetelmä, jolla mallinnetaan Markovilaisia satunnaisprosesseja. Näissä oletetaan, että systeemin seuraava tila riippuu vain tämänhetkisestä



Kuva 3: Esimerkki yksinkertaisesta Markovin ketjusta systeemille, jolla on 4 tilaa. Noodit esittävät systeemin eri tiloja, ja linkit todennäköisyyksiä siirtyä tilasta toiseen. Jokaisesta noodista lähtevien linkkien painokertoimet summautuvat siten 1

tilasta [29]. Kvanttiverkkojen tapauksessa tämä on järkevä oletus, sillä lomittumisen vaihdossa tehtävät prosesssit riippuvat vain siitä, onko lomittuneita tiloja sillä hetkellä käytössä. Tällöin pystytään määräämään yksikäsitteisesti todennäköisyydet siirtyä tietystä tilasta toiseen, vain sen perusteella, mistä aloitettiin.

Markovin ketjuja kuvataan suunnatulla painotetuilla verkkoilla, kuten kuvassa 3 on havainnollistettu. Tällöin systeemin tilat ovat Markovin ketjun noodeja, ja painotetut linkit todennäköisyyksiä siirtyä tilasta toiseen. Tällöin verkon vierekkäisyysmatriisilla on tilasiirtomatriisi (TPM, transformation probability matrix), joka kuvaa todennäköisyyksiä siirtyä tilasta toiseen. Esimerkiksi kuvan 3 TPM on

$$\mathrm{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0.35 & 0 & 0.55 & 0.1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0.15 & 0.85 \end{pmatrix}. \tag{6}$$

Koska TPM:n rivit kuvaavat todennäköisyyksiä siirtyä tilasta toiseen, täytyy sen jokaisen rivisumman olla 1. Tällöin esimerkiksi todennäköisyydet siirtyä tilasta B muihin tiloihin nähdään suoraan riviltä 2. Matemaattisesti sijainti Markovin ketjussa voidaan kuvata vektorilla. Tässä esimerkissä tila A olisi vektori $\mathbf{v}_1 = (1,0,0,0)$ ja niin edelleen. Suorittamalla kertolasku

$$\mathbf{v}_2 = \mathbf{v_1}\mathrm{P} \tag{7}$$

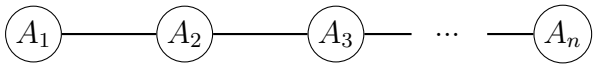
saadaan todennäköisyydet siirtyä seuraavaan tilaan. Valitsemalla näiden perusteella uusi alkutila ja toistamalla tätä monta kertaa saadaan suoritettua satunnaiskävely, jossa simuloidaan systeemin kehitystä . Kvanttiverkkoissa satunnaiskävelyn päätepiste on siis se tila, mihin verkko lopulta päätyy. Toinen tapa määrittää satunnaiskävelyn päätepiste on laskea lopputilan todennäköisyydet suorittamalla matriisikertolasku (7) sen askelmäärän verran [29]. Esimerkki TPM:llä ja lähtiessä noodista A, suorittamalla 100 askelta pitkä satunnaiskävely saadaan siis lopputilatodennäköisyyksiksi

$$\begin{aligned}\mathbf{v}_{loppu} &= \mathbf{v}_{alku}\mathrm{P}^{100} \\ &= (1,0,0,0)\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0.35 & 0 & 0.55 & 0.1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0.15 & 0.85 \end{pmatrix}^{100} \\ &= (0.301508,0.301508,0.19598,0.201005). \end{aligned} \tag{8}$$

Lopputilan selvittäminen ei kuitenkaan ole ainoa tapa hyödyntää Markovin ketjuja. Tutkimuksessa [6], jossa mallinnettiin kvanttitoistimen aikaa tuottaa yksi lomittunut tila, Markovin ketjun päätepiste oli kiintopiste, eli siihen päädyttyä satunnaiskävely ei enää pääse pois. Tällöin satunnaiskävelyllä voidaan hakea keskimääräistä aikaa, eli iteraatiokertoja, mitä verkolla menee päästä haluttuun tilaan. Tässä tekstissä käytetään samaa ideaa, mutta verkon haluttu tila ei ole Markovin ketjun kiintopiste, vaan satunnaiskävelyn suoritettua lasketaan, kuinka monta kertaa verkko kävi sen pisteen kautta.

2.3.2 Markovin ketjujen rajoitukset

Huolimatta Markovin ketjujen yleiskäyttöisyydestä, kvanttikommunikaatioverkkojen mallinnus tuottaa hankaluuksia verkon koon kasvaessa. Tämä johtuu suurelta



Kuva 4: Yksittäinen n mittainen ketju kvanttitoistimia. Kvanttiverkon tavoitteena on muodostaa lomittunut tila noodejen A_1 ja A_n välille

osin kvanttiverkon tilojen määrän nopeasta lisääntymisestä. Jos verkossa on n noodia, niin ne voidaan lomittaa $\binom{n}{2}$:lla tavalla. Vaikka kvanttiverkon mallintamisessa oltaisiin kiinnostuneita vain siitä, mitkä noodit ovat lomittuneet, eli tilojen määrällä ei ole merkitystä, johtaisi tämä silti Markovin ketjuun, jolla olisi $2^{\binom{n}{2}}$ noodia. Nähdään siis, että TPM:n koko kasvaa hyvin nopeasti. Käytännössä, jos Markovin ketjuja halutaan käyttää mallintamaan suurempia kvanttiverkkoja, täytyy TPM:n olla tuotettavissa algoritmisesti. Lisäksi jossain vaiheessa TPM:n koko kasvaa niin suureksi, että simulaatioista tulee liian raskaita suorittaa. Esimerkiksi tutkimuksessa [6] käytetyllä mallilla ei kyetä simuloimaan tarkasti kvanttiverkkoja, jotka koostuvat yli 32 noodista, vaikka he esittävät rekursiivisen algoritmin TPM:n rakentamiseen. Tällöin simulaatioissa joudutaan käyttämään muita menetelmiä tai yksinkertaistavia approksimaatioita.

3 Äärellisten yrityskertojen ongelma

3.1 Verkon kapasiteetti

Kommunikaatioverkon kapasiteetti kertoo kuinka paljon informaatiota, eli kubitteja verkko kykenee siirtämään noodien välillä. Tämä riippuu tietysti siitä, kuinka paljon virheitä eri operaatioissa tapahtuu. Tämän lisäksi verkon kapasiteetti riippuu merkittävästi myös verkon rakenteesta. Yksinkertaisin rakenne on vain ketju kvanttitoistimia vakioetäisyyksillä toisistaan. Tällainen rakenne on esitetty kuvassa 4. Määrittelmällä kvanttikanavan johtokyky (engl. transmissivity) η, mikä on onnistuneesti kahden noodin välillä lähetettyjen kubittien osuus kaikista saadaan

kapasiteetin ylärajaksi

$$C(\eta,N) = -\log_2(1 - \sqrt[N+1]{\eta}), \tag{9}$$

missä N on toistimien määrä verkossa. Jos kvanttitoistimet eivät ole tasavälein, tai muusta syystä noodien välinen johtokyky ei ole kaikissa sama, riippuu verkon kapasiteetti vain pienimmästä johtokyvyn arvosta [30]

$$C(\eta,N) = -\log_2(1 - \eta_{min}). \tag{10}$$

Myös paljon monimutkaisemmillekin verkoille määritetty kapasiteetin teoreettisia rajoja [30], [31].

Teoreettisten rajojen määrittämisessä on hyödynnetty monia verkkoteoreettisia ja sen ulkopuolisia tuloksia. Mainittakoon näistä erityisesti max-flow min-cut -teoria, jonka mukaan verkon maksimaallinen kapasiteetti on aina yhtä suuri, kuin sen leikkausjoukon kapasiteetti, joka on pienin [32]. Lause on oleellisesti muodoltaan samanlainen, kuin kaavassa (10) esitetty tulos, vaikkei kumpaakaan voida toisesta suoraan johtaa. Tämä on hyödyllinen tulos erityisesti suurempia verkkorakenteita tutkiessa, koska verkko voidaan jakaa leikkausjoukkoihin ja tarkastella niitä erikseen. Koko verkon kapasiteetin yläraja on pienin leikkausjoukkojen kapasiteeteista.

Lomittumiseen perustuvissa kvanttiverkoissa yhden kubittitilan siirron kuluu aina yksi lomittunut tila, joten verkon kapasiteetti riippuu suoraan siinä olevien lomittuneiden tilojen määrästä [14]. Jatkossa verkon kapasiteetti rinnastetaankin siinä olevien lomittuneiden tilojen määrään.

3.2 Kapasiteetin riippuvuus ajasta

Kvanttikommunikaatioverkossa lomittuneita tiloja kyetään jokaisella ajanhetkellä luomaan vain rajoitettu määrä. Siten verkon päälläoloaika vaikuttaa suoraan kapasiteettiin. On osoitettu, että kapasiteetin teoreettiset ylärajat saavutetaan vasta,

kun verkko on ollut päällä äärettömän kauan [4]. Tulos on helpoin ymmärtää ajattelemalla tilannetta, jossa dekoherenssi on vähäistä. Mitä kauemmin verkolla on ollut aikaa muodostaa lomittuneita tiloja, sitä enemmän niitä on verkossa. Todellisissa kvanttimuisteissa, joissa dekoherenssi on merkittävä lomittuneiden tilojen maksimimäärä verkossa on tietysti äärellinen.

Käytettäessä kvanttiverkkoja, ne ovat kuitenkin ehtineet olla päällä vain äärellisen ajan. Näissä tapauksissa kommunikaation kannalta tärkeää onkin se, kuinka nopeasti verkon kapasiteetti lähestyy teoreettista ylärajaa. Tässä tutkielmassa tarkastellaan erityisesti miten käyttämättömän verkon kapasiteetti käyttäytyy, kun verkossa ei aluksi ole yhtään lomittunutta tilaa. Koska tiloja ei käytetä, tulee verkko pääsemään lähelle teoreettista maksimikapasiteettia varmasti jossain ajanjaksossa.

4 Python-simulaatiot

Simulaatiot toteutettiin Python V3.11.5:lla, missä hyödynnettiin Numpy V2.4 ja Matplotlib V3.10.0 kirjastoja. Näissä mallinnetaan vain verkkoja, jotka pyrkivät yhdistämään kaksi noodia keskenään. Tehdyissä simulaatoissa käytetään seuraavia oletuksia kvanttikommunikaatioverkon mallintamiseen

1. Aika jaetaan diskreetteihin palasiin, ja verkon tilaa tarkastellaan jokaisen aika-askeleen lopussa

2. Jokaisella aika-askeleella kvanttimuistit pyrkivät luomaan lomittuneen tilan kaikkien viereisten kanssa. Onnistumistodennäköisyys lomittumisen luomiselle on vakio p, joka on sama kaikilla linkeillä.

3. Jokaisella aika-askeleella toteutetaan kaikki mahdolliset lomittumisen vaihdot, jotka edistävät lopullisen halutun tilan saavuttamista. Siis ei toteuteta sellaisia lomittumisen vaihtoja, joiden jälkeen lopullisen tilan saavuttamiseen tarvittaisiin enemmän lomittumisen vaihtoja kuin ennen sitä. Valitaan myös lomit-

tumisen vaihdon onnistumistodennäköisyydeksi vakio q, joka on sama kaikilla operaatioilla.

4. Lomittumisen tislausta ei mallinneta erikseen, vaan se sisältyy lomittumisen vaihdon onnistumistodennäköisyyteen. Siis oletetaan, että onnistuneella lomittumisen vaihdolla syntynyt lomittunut tila on aina tarpeeksi vahvasti lomittunut.

5. Dekoherenssia mallinnetaan tilastollisesti. Jokaisen aika-askeleen lopussa käydään läpi jokainen verkossa oleva lomittunut tila, ja poistetaan se todennäköisyydellä r. Tällöin todennäköisyys, että tila säilyisi verkossa T aika-askelta on $(1-r)^T$.

Nämä oletukset on valittu tarkoituksella mahdollisimman yksinkertaisiksi, jotta simulaatioiden suoritusaika ei kasva liian nopeasti. Erityisesti käytettävä Dekoherenssimalli on huomattavasti kevyempi toteuttaa, kuin malli, jossa jokaisen lomittuneen tilan olemassaoloajasta pidettäisiin kirjaa erikseen.

4.1 Toimintaperiaate

Simulaatioiden toimintaperiaate perustuu Markovin ketjujen osalta tutkimuksessa [6] käytettyyn malliin. Kuitenkin niitä käytetään vain mallintamaan lomittumisen luomista, eikä koko verkon tila kehitystä. Näin kyetään rajoittamaan TPM:n kasvua verkon koon kasvaessa. Tarkastellaan simulaatioiden toimintaa yksinkertaisimmassa tapauksessa kolmesta noodista koostuvassa kvanttitoistinketjussa.

Yleisen n-mittaisen ketjun rakenne on esitetty kuvassa 4. Ketjussa luodaan lomittuneita tiloja päätepisteiden välille, eli kolmen noodin tapauksessa A_1:n ja A_3:n välille. Verkon tilaa kuvataan simulaatioissa binääriluvulla, jossa numero 1 tarkoittaa, että kyseisiä lomittuneita tiloja on verkossa vähintään yksi ja 0, ettei tiloja ole ollenkaan Kolmen noodin tapauksessa tähän riittää kolmen numeron mittainen lu-

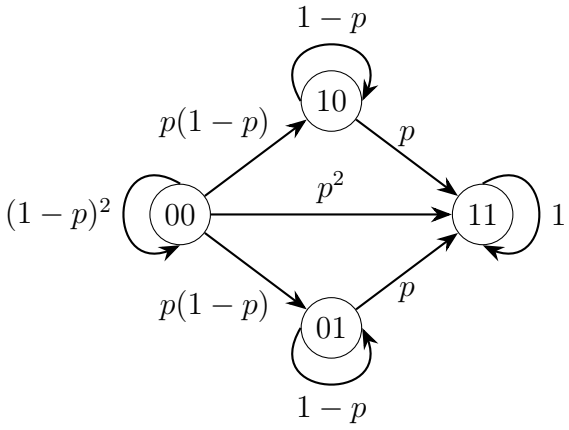
Taulukko I: Alku- ja lopputilan perusteella määräytyvät kertoimet TPM:matriisiin

Alkutila	Lopputila	kerroin
0	0	$1-p$
0	1	p
1	0	0
1	1	1

ku. Luvun ensimmäinen numero kertoo onko noodien A_1 ja A_2 välissä lomittunutta tilaa, toinen onko A_2 ja A_3 lomittuneita ja viimeinen onko A_1 ja A_3 lomittuneet. Siis esimerkiksi tila 000 on verkon alkutila, lomittuneisuutta ei ole missään, ja kaikki muotoa xx1 tilat ovat sellaisia, jossa haluttu lomittunut tila on saatu muodostettua. Binäärisanan lisäksi verkon tilaa kuvaa sen pituinen lista, jossa listan i:nes alkio kertoo numeroa i vastaavien lomittuneiden tilojen määrän. Periaatteessa pelkkä lista riittäisi kuvaamaan verkon tilaa, mutta suurimmassa osassa simulaation vaiheita binäärisana on riittävä ja samalla yksinkertaisempi kuvaus.

Käyttämällä binäärisanoja hyödyksi saadaan Markovin ketjussa käytettävä TPM matriisi muodostettua helposti. Matriisiin tulee vain tieto lomittumisen luontien vaikutuksesta verkon tilaan. Kolmen noodin tapauksessa siis TPM on 2x2 matriisi ja alku ja lopputilan binäärisanan kaksi ensimmäistä merkkiä määräävät TPM:n alkiot. Taulukossa I on esitetty saatavat kertoimet. Kokonaisuudessaan siirtymätodennäköisyydet saadaan ottamalla jokaista merkkiä kohden kerroin taulukosta I, ja kertomalla ne keskenään. Esimerkiksi siis todennäköisyys siirtymälle $00 \to 10$ on $p(1-p)$. Asettamalla kolmen noodin kvanttitoistinketjun tilat vektoriin muodossa

$$(00, 01, 10, 11), \tag{11}$$



Kuva 5: Kolmen noodin kvanttitoistinketjun lomittumisen luontia kuvaava Markovin ketju

saadaan ketjun lomittumisen luontia kuvaavan Markovin ketjun TPM matriisiksi

$$\begin{pmatrix} (1-p)^2 & p(1-p) & p(1-p) & p^2 \\ 0 & 1-p & 0 & p \\ 0 & 0 & 1-p & p \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{12}$$

Kuvassa 5 on vielä esitetty kolmen noodin ketjun tapausta kuvaava Markovin ketju. Tarkastellaan seuraavaksi tarkemmin mitä simulaatiossa tapahtuu yhden aika-askeleen aikana.

Jokaisen aika-askeleen alussa tarkastetaan, voidaanko verkossa tehdä lomittumisen vaihtoja verkon tilaa kuvaavan binäärisana perusteella. Kolmen noodin ketjussa siis, jos tila on muotoa 11x, lomittumisen vaihtoa voidaan yrittää, kun taas muilla tiloilla ei. Kun lomittumisen vaihtoa yritetään, poistetaan listasta siihen kuluneet lomittuneet tilat, ja lisätään uusi tila, jos lomittumisen vaihto onnistui. Jos verkossa on monta mahdollista lomittumisen vaihtoa, jotka voitaisiin tehdä, toteutetaan aina lähimmäs tavoitetilaa tuottavat ensimmäisenä. Lisäksi tällöin kirjanpidollisesti varmistetaan, ettei syntyneitä lomittuneita tiloja käytetä samassa aika-askeleessa uudelleen. Tässä tekstissä simuloitavissa verkoissa nämä molemmat voidaan toteuttaa

vaan valitsemalla tilojen tarkistus tietyllä tavalla. Monimutkaisemmissa verkoissa täytyisi erikseen tallentaa muistiin tieto verkon tilasta ennen yhtään lomittumisen vaihtoa ja varmistaa sen avulla, ettei uusia tiloja käytetä vahingossa. Lomittumisen vaihtojen järjestyksen päättämiseen taas täytyisi käyttää jotain reititysalgoritmia.

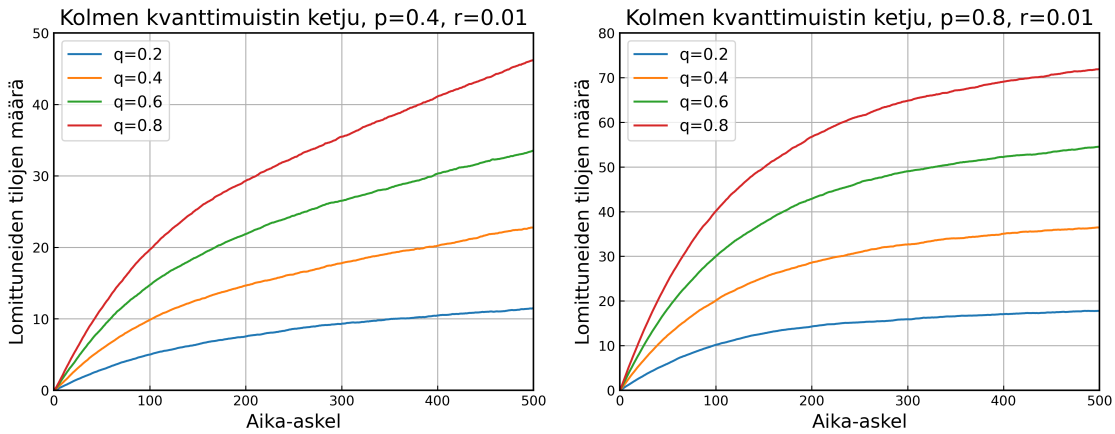
Lomittumisen vaihtojen suorittamisen jälkeen simuloidaan uusien lomittuneiden tilojen luonti. Tähän käytetään Markovin ketjuja luvussa 2.3.1 kuvatulla tavalla, mallintamaan syntynyt verkon tila. Syntyneet lomittuneet tilat tallennetaan taas listaan. Tässä on otettava huomioon, että jos verkon alku- ja lopputilaa kuvaavissa binäärisanoissa on molemmissa 1 samassa paikassa, ei ole tietoa, onnistuiko lomittumisen luonti. Tällöin tila siis lisätään todennäköisyydellä p listaan. Muissa tapauksissa siirtymästä nähdään suoraan syntyikö lomittuneita tiloja vai ei. Lopuksi simuloidaan dekoherenssi luvun 4 alussa kuvatulla tavalla ja tallennetaan aika-askel ja sitä vastannut haluttujen lomittuneiden tilojen määrä talteen. Tämän jälkeen aloitetaa uusi kierros.

Kaikissa simulaatioissa saadut kapasiteetin arvot, eli lomittuneiden tilojen määrät ovat keskiarvoja 1000:n eri satunnaiskävelysimulaation tuloksista. Jokaisessa simulaatiossa valittiin dekoherenssia kuvaavan todennäköisyyden arvoksi $r = 0.01$.

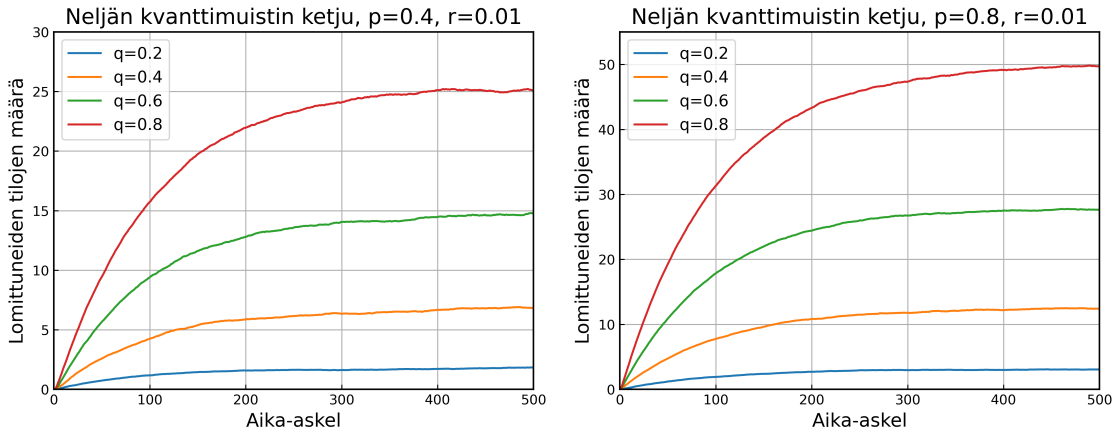
4.2 Yksittäinen ketju

Ensimmäisenä tarkasteltiin yksittäisistä ketjuista koostuvia kvanttiverkkoja, jotka on esitetty kuvassa 4. Näistä mallinnettiin kolmesta ja neljästä kvanttitoistimesta koostuvia ketjuja. Saadut tulokset on esitetty kuvissa 6 ja 7.

Kuvista nähdään, että kvanttiverkkojen kapasiteetti lähestyy maksimiarvoa ajankuluessa. Odotetusti pidemmällä ketjulla kapasiteetti on pienempi, sillä lomittumisen vaihtoa yhden tilan luontiin tarvitaan kaksi yhden sijaan. Vastaavasti neljän kvanttimuistin tapauksessa lomittumisen vaihdon onnistumistodennäköisyys merkitsee huomattavasti enemmän. Kolmen tapauksessa se kasvattaa tilojen määrää li-



Kuva 6: Kolmen kvanttitoistimen ketjun kapasiteetti eri lomittumisen vaihdon ja luomisen todennäköisyyksillä



Kuva 7: Neljän kvanttitoistimen ketjun kapasiteetti eri lomittumisen vaihdon ja luomisen todennäköisyyksillä

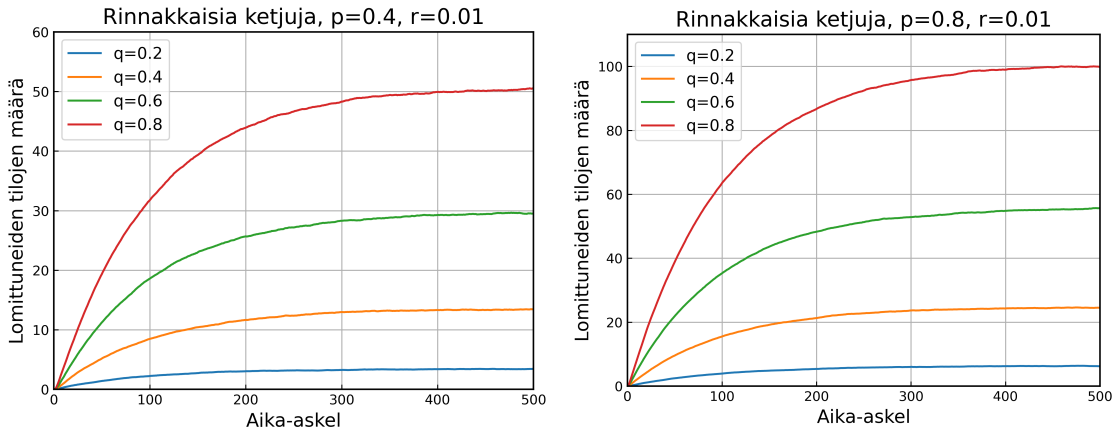
neaarisesti, mutta neljällä jo huomattavasti enemmän. Mielenkiintoisesti, mitä epätodennnäköisempää lomittumisen vaihdon onnistuminen on, sitä nopeammin verkon maksimikapasiteetti saavutetaan. Lisäksi jo näinkin pienessä verkossa nähdään dekoherenssin merkitys selvästi. Neljän muistin tapauksessa kun lomittumisen onnistumisen todennäköisyys on tarpeeksi pieni $q = 0.2$, ei lomittumisen luomisen todennäköisyyden kasvattaminen juurikaan lisää verkon kapasiteettia. Käytännössä tämä johtuu siitä, että dekoherenssi tuhoaa lopullisia tiloja melkein yhtä nopeasti kuin uusia luodaan.

4.3 Rinnakkaisia ketjuja

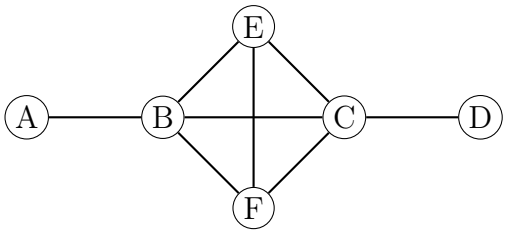
Rinnakkaiset ketjut voitaisiin periaatteessa käsitellä pelkästään yksittäisten ketjujen simulaatioilla. Koska ketjut eivät ole mitenkään yhteydessä toisiinsa, niin ne toimivat täysin riippumattomasti. Siten laittamalla kaksi ketjua vierekkäin pitäisi verkon kapasiteetin kaksinkertaistua, sillä molemmat ketjut luovat keskimäärin yhtä monta lomittunutta tilaa aika-askelta kohti, kuin yksittäinen ketju. Tämä simulaatio on kuitenkin hyvä tarkistus mallin järkevyydestä. Tässä mallinnettiin vain kahdesta neljän kvanttimuistin ketjusta koostuvaa verkkoa. Saadut tulokset on kuvassa 8. Vertaamalla näitä kuvassa 7 esitettyihin tuloksiin nähdään, että lomittuneiden tilojen määrä jokaisessa tapauksessa todella on kaksinkertainen.

4.4 Hila

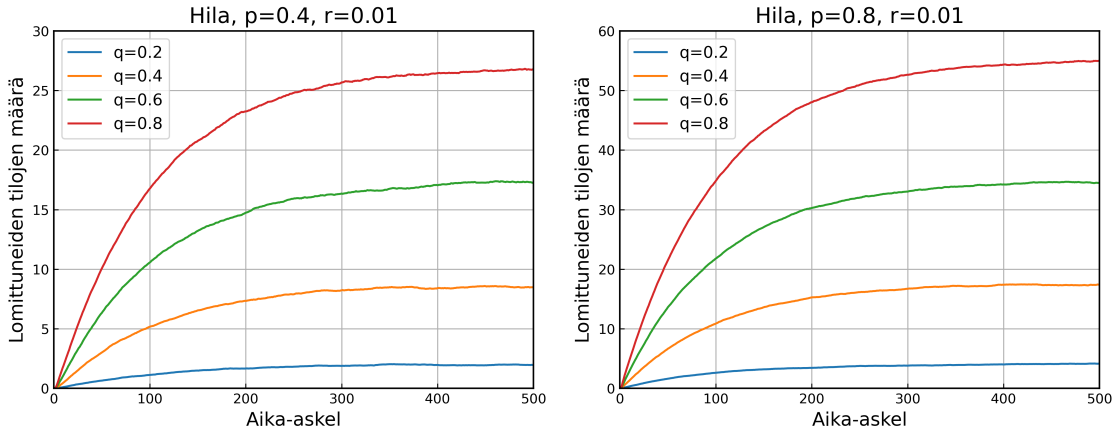
Tarkastellaan monimutkaisempana esimerkkinä verkkoa, jonka verkkorakenne on esitetty kuvassa 9. Verkon rakenne vastaa Wienin SECOQC verkkoa, jolla kykenee kvanttiavaimenjakoon [33]. Mainittakoon, että verkon noodit eivät ole vakioetäisyydellä, vaan lyhin linkki on 80 m ja pisin 85 km pitkiä. Tällöin tietysti lyhemissä linkeissä lomittumisen luomisen onnistumistodennäköisyys on suurempi kuin pidemmissä, eikä tässä käytettävä malli kuvaa tilannetta enää niin hyvin. Lisäksi verkko



Kuva 8: Kahdesta rinnakkaisesta neljän kvanttitoistimen ketjusta koostuvan kvanttikommunikaatioverkon kapasiteetit eri lomittumisen vaihdon ja luomisen todennäköisyyksillä



Kuva 9: Wienin SECOQC-verkon topologinen rakenne.



Kuva 10: Tarkastellun hilan simulaatiotulokset

on jo sen verran monimutkainen, että reititysalgoritmien käyttö tehostaisi verkon lomittumista. Tekemällä lomittumisen vaihto, jossa yksi tiloista on noodien E ja F välinen, ei varsinaisesti saada tilaa lopullisen tilan luontia edistettyä, sillä tarvitaan edelleen yhtä monta operaatiota. Sillä saadaan kuitenkin siirrettyä lomittunut tila eri puolelle kvanttiverkkoa. Dynaamisessa reitityksessä näin pystytään välttämään lomittuneiden tilojen kerääntyminen toiselle puolelle verkkoa. Toteutetuissa simulaatioissa tämä huomioidaan vain siten, että viimeinen tehtävä lomittumisen vaihto on aina se, joka kuluttaa noodien E ja F välisen tilan. Tällöin on mahdollista, että verkossa toteutetaan turhia lomittumisen vaihtoja, jotka heiman heikentävät sen kapasiteettia.

Saadut simulaatiotulokset on esitetty kuvassa 10. Verkon 9 rakenteesta nähdään, että yhdistettävät noodit A ja D ovat lyhimpiä reittejä yhtä kaukana kuin neljän kvanttimuistin ketjussa. Vertaamalla saatuja tuloksia neljän kvanttimuistin ketjuun 7 nähdään, että vaihtoehtoisten reittien lisääminen kvanttiverkkoon on kasvattanut verkon kapasiteettia hieman. Toisaalta suurimmillaankin ero on vain noin 5 lomittunutta tilaa kun $q = 0.8$ ja $p = 0.8$, mikä on huomattavasti vähemmän kuin rinnakkaisten ketjujen tapauksessa 8, missä vastaavilla todennäköisyyksillä on noin 50 lomittunutta tilaa enemmän. Koska rinnakkaisissa ketjuissa tarvitaan vain kaksi

kvanttimuistia enemmän kuin hilassa 9, niin nähdään, että pelkästään kapasiteetin kannalta rinnakkaiset ketjun ovat tehokkaampia kuin hilarakenne.

Tosin max-flow min-cut -teorian perusteella nähdään selvästi, että hilarakenteessa tämän heikkouden aihettuaa kvanttimuistien A ja B sekä C ja D väliset linkit, joita on vain yksi kappale. Tällöin jos sallittaisiin linkeille eri lomittumisen luomisen todenäköisyydet ja siten eri kapasiteetit täytyisi hilassa parantaa vain näitä kahta linkkiä, kun taas rinnakkaisessa ketjussa tarvitsee parantaa vähintään toisen ketjun kaikkien linkkien kapasiteettia, paremman kokonaiskapasiteetin saamiseksi. Lisäksi tarkastelemalla leikkausta nähdään että hilan keskiosa, eli kvanttimuisteista B, C, E ja F koostuva rakenne on kestävämpi. Kahdesta rinnakkaisesta ketjusta riittää poistaa molemmista ketjuista vain yksi linkki siihen, ettei verkossa enää kyetä kommunikoimaan. Hilan keskiosasta taas täytyy katkaista vähintään kolme linkkiä, että viestintä ei enää onnistu. Siis vaikka hilarakenne tässä mallissa ei olekaan tarvittaviin kvanttimuisteihin nähden yhtä tehokas kuin kaksi rinnakkaista ketjua, ei se välttämättä ole käytännön toteutuksena huonompi.

5 Yhteenveto

Tutkielmassa tarkasteltiin kvanttikommunikaatioverkkoja ja niiden mallintamista. Erityisesti on keskitytty kvanttikommunikaatioverkkojen kapasiteetin tutkimiseen yksinkertaisissa verkkorakenteissa. Verkon kapasiteetti riippuu suoraan lomittuneiden tilojen määrästä, joten sitä voitiin tarkastella vain mallintamalla lomittuneiden tilojen määrää kvanttiverkossa. Verkon matemaattista kuvausta varten esiteltiin tarvittavia verkkoteorian käsitteitä ja tuloksia.

Tunnetusti kvanttikommunikaatioverkkojen kapasiteetti saavuttaa maksimiarvonsa vasta, kun verkko on ollut päällä äärettömän kauan. Siten äärellisillä ajanjaksoilla verkon kapasiteetti on aina pienempi, eli viestien välitysnopeus on teoreettista yläraja-arvoa hitaampi. Käytetyn simulaatiomallin perusteella kvanttiverkon

kapasiteetti vaikuttaa lähestyvän teoreettista maksimia kohtuullisen nopeasti, joten äärellisten yrityskertojen vaikutus ei välttämättä ole kovin merkittävä. Toki on huomattava, että käytetty malli on hyvin yksinkertainen, ja saattaa jättää huomiotta ilmiöitä, jotka heikentävät kapasiteettiä. Lisäksi tarkasteltiin vain kuormittamattomia verkkoja, eli sellaisia, joita ei aktiivisesti käytetä viestintään. Mielenkiintoinen jatkotarkastelu olisi tutkia verkkoja, joita aktiivisesti kuormitetaan. Tällöin lomittuneita tiloja siis käytetäisiin kommunikaatioon koko ajan, jolloin verkon kapasiteetti ei välttämättä samalla tavalla pääsisi lähelle teoreettista maksimia.

Simulaatiot perustuivat Markovin ketjuihin. Menetelmä valittiin, koska niiden perusvaatimus systeemin aikaisempien tilojen riippumattomuudesta sopii kvanttikommunikaatioverkkoihin. Toisaalta kuten todettiin, eivät Markovin ketjut toimi suurille verkoille niiden tilamäärien valtavan kasvun takia. Yhtenä etuna käytetyssä menetelmässä on se, että mallia voidaan tarkentaa helposti, esimerkiksi huomioimalla dekoherenssi laittamalla tiloille aikaleimat tai lisäämällä todennäköisyyksiin lomittumisen tislauksen vaikutukset, ilman että sen toimintaperiaate muuttuu.

Kvanttikommunikaatioverkot ovat nopeasti kehittyvä käytännön sovellus, joka yhdistää monta eri alaa, kuten kvanttimekaniikkaa, informaatioteoriaa ja verkkoteoriaa. Vaikka viimeisen kahdenkymmenen vuoden aikana useita kvanttiavaimenjakoon kykeneviä verkkoja on rakennettu, on ala vielä alkuvaiheessa. Tulevaisuudessa kvanttikommunikaativerkkojen toivotaan vastaavan laajuudeltaan klassisia kommunikaatioverkkoja, mutta alalla on vielä useita ratkaistavia ongelmia. Muun muassa sekä kvanttitoistimet, että kvanttimuistit eivät ole vielä tarpeeksi kehittyneitä suuria alueita tai käyttäjämääriä tukevien verkkojen toteuttamiseen [34].

Tekoälyn käyttö tutkielmassa

Tässä tutkielmassa ei ole käytetty tekoälyä.

Viitteet

[1] R. Bassoli, H. Boche, C. Deppe, R. Ferrara, F. H. P. Fitzek, G. Janssen ja S. Saeedinaeeni, *Quantum Communication Networks*, Vol. 23 of *Foundations in Signal Processing, Communications and Networking* (Springer International PublishingGewerbestrasse 11, 6330 Cham, Switzerland, 2021) doi:10.1007/978-3-030-62938-0.

[2] N. Gisin, G. Ribordy, W. Tittel ja H. Zbinden, Reviews of Modern Physics **74**, 145 (2002) doi:10.1103/RevModPhys.74.145.

[3] H.-Z. Chen, M.-H. Li, Y. Z. Wang, Z.-G. Zhao, C. Ye, F. L. Li, Z. Chen, S.-L. Han, B. Tang, Y. J. Miao ja W. Qi, npj Quantum Information **11**, 137 (2025) doi:10.1038/s41534-025-01089-8.

[4] M. S. Winnel, J. J. Guanzon, N. Hosseinidehaj ja T. C. Ralph, npj quantum information **8**, 129 (2022) doi:10.1038/s41534-022-00641-0.

[5] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss ja B. Li, AVS Quantum Science **3**, 014101 (2021) doi:10.1116/5.0024062.

[6] E. Shchukin, F. Schmidt ja P. v. Loock, Physical Review A **100**, 032322 (2019) doi:10.1103/PhysRevA.100.032322.

[7] L. Hartmann, B. Kraus, H.-J. Briegel ja W. Dür, Physical Review A **75**, 032310 (2007) doi:10.1103/PhysRevA.75.032310.

[8] M. S. Rahman, *Basic Graph Theory*, *Undergraduate Topics in Computer Science* (Springer NatureCham, Switzerland, 2017) doi:10.1007/978-3-319-49475-3.

[9] W. D. Wallis, *A beginner's guide to graph theory*, 2nd ed ed. (BirkhäuserBoston, 2007).

[10] C. H. Bennett ja S. J. Wiesner, Physical Review Letters **69**, 2881 (1992) doi:10.1103/PhysRevLett.69.2881.

[11] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye ja M. D. Lukin, Nature Physics **10**, 582 (2014) doi:10.1038/nphys3000.

[12] G. R. Blakely, *Advances in Cryptology: Proceedings of CRYPTO '84*, No. v.196 in *Lecture Notes in Computer Science Ser* (Springer Berlin / HeidelbergBerlin, Heidelberg, 1985).

[13] W. K. Wootters ja W. H. Zurek, Nature **299**, 802 (1982) doi:10.1038/299802a0.

[14] B. Schumacher ja M. D. Westmoreland, *Quantum Processes, Systems, and Information* (Cambridge University Press, 2010).

[15] H.-J. Briegel, W. Dür, J. I. Cirac ja P. Zoller, Physical Review Letters **81**, 5932 (1998) doi:10.1103/PhysRevLett.81.5932.

[16] S. Pirandola, R. Laurenza, C. Ottaviani ja L. Banchi, Nature Communications **8**, 15043 (2017) doi:10.1038/ncomms15043.

[17] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin ja H. Zbinden, Physical Review Letters **121**, 190502 (2018) doi:10.1103/PhysRevLett.121.190502.

[18] S. Pirandola, Physical Review Research **3**, 023130 (2021) doi:10.1103/PhysRevResearch.3.023130.

[19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres ja W. K. Wootters, Physical Review Letters **70**, 1895 (1993) doi:10.1103/PhysRevLett.70.1895.

[20] A. Patil, M. Pant, D. Englund, D. Towsley ja S. Guha, npj Quantum Information **8**, 51 (2022) doi:10.1038/s41534-022-00536-0.

[21] E. Sutcliffe ja A. Beghelli, IEEE Transactions on Quantum Engineering **6**, 1 (2025) doi:10.1109/tqe.2025.3588783.

[22] S. J. Devitt, K. Nemoto ja W. J. Munro, Reports on Progress in Physics **76**, 076001 (2013) doi:10.1088/0034-4885/76/7/076001.

[23] R. Zhao, Y. O. Dudin, S. D. Jenkins, C. J. Campbell, D. N. Matsukevich, T. A. B. Kennedy ja A. Kuzmich, Nature Physics **5**, 100 (2009) doi:10.1038/nphys1152.

[24] S. Abruzzo, H. Kampermann ja D. Bruß, Physical Review A **89**, 012301 (2014) doi:10.1103/PhysRevA.89.012301.

[25] S. Brand, T. Coopmans ja D. Elkouss, IEEE Journal on Selected Areas in Communications **38**, 619 (2020) doi:10.1109/JSAC.2020.2969037.

[26] G. Vardoyan, S. Guha, P. Nain ja D. Towsley, Performance Evaluation **144**, 102141 (2020) doi:10.1016/j.peva.2020.102141.

[27] G. Vardoyan, S. Guha, P. Nain ja D. Towsley, IEEE Transactions on Quantum Engineering **2**, 1 (2021) doi:10.1109/TQE.2021.3058058.

[28] P. Nain, G. Vardoyan, S. Guha ja D. Towsley, Proceedings of the ACM on Measurement and Analysis of Computing Systems **4**, 1 (2020) doi:10.1145/3392141.

[29] A. Tolver, *An introduction to Markov chains* (Department of Mathematical Sciences, University of Copenhagen, 2016).

[30] S. Pirandola, Communications Physics **2**, 51 (2019) doi:10.1038/s42005-019-0147-3.

[31] S. Bäuml, K. Azuma, G. Kato ja D. Elkouss, Communications Physics **3**, 55 (2020) doi:10.1038/s42005-020-0318-2.

[32] P. Elias, A. Feinstein ja C. Shannon, IEEE Transactions on Information Theory **2**, 117 (1956) doi:10.1109/TIT.1956.1056816.

[33] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden ja A. Zeilinger, New Journal of Physics **11**, 075001 (2009) doi:10.1088/1367-2630/11/7/075001.

[34] P. Zhang, N. Chen, S. Shen, S. Yu, S. Wu ja N. Kumar, IEEE Network Magazine **31**, 141 (2024) doi:10.1109/MWC.012.2200295.