KATHOLIEKE UNIVERSITEIT LEUVEN
FACULTEIT INGENIEURSWETENSCHAPPEN
DEPARTEMENT ELEKTROTECHNIEK
Kasteelpark Arenberg 10, 3001 Leuven (Heverlee)

LOCAL EQUIVALENCE OF STABILIZER STATES AND CODES

Promotoren:
Prof. dr. ir. B. De Moor
Prof. dr. M. Fannes

Proefschrift voorgedragen tot
het behalen van het doctoraat
in de ingenieurswetenschappen

door

Maarten VAN DEN NEST

May 2005

KATHOLIEKE UNIVERSITEIT LEUVEN
FACULTEIT INGENIEURSWETENSCHAPPEN
DEPARTEMENT ELEKTROTECHNIEK
Kasteelpark Arenberg 10, 3001 Leuven (Heverlee)

LOCAL EQUIVALENCE OF STABILIZER STATES AND CODES

Jury:
Prof. dr. ir. P. Van Houtte, voorzitter
Prof. dr. ir. B. De Moor, promotor
Prof. dr. M. Fannes, copromotor
Prof. dr. ir. J. Vandewalle
Prof. dr. H. Verschelde (R. U. Gent)
Dr. ir. J. Dehaene
Prof. dr. ir. A. Barbé
Prof. dr. J. Eisert (Imperial College, London)

Proefschrift voorgedragen tot
het behalen van het doctoraat
in de ingenieurswetenschappen

door

Maarten VAN DEN NEST

U.D.C. 681.3*G2

May 2005

D/2005/7515/40

ISBN 90-5682-604-2

Voorwoord

Alleerst wil ik Prof. Bart De Moor, mijn promotor, bedanken voor de kansen die hij me heeft gegeven om in een zeer aangename en stimulerende omgeving onderzoek te doen op een onderwerp dat ik volledig vrij heb kunnen kiezen.

Dank ook aan Prof. Mark Fannes, mijn copromotor, en aan Prof. Joos Vandewalle en Prof. Henri Verschelde, de leden van mijn leescomité, en Prof. André Barbé, voor het zorgvuldig nalezen van mijn verhandeling en het geven van suggesties ter verbetering van dit manuscript.

I am very grateful to Jens Eisert for extending me the honour of residing in my PhD jury, for a careful reading of the manuscript, and for many interesting discussions at several QIT meetings over the past years.

Het is een plezier om Jeroen Dehaene, mijn dagelijkse begeleider, van harte te bedanken voor zijn constante paraatheid om mijn soms op-schrijnende-wijze-van-gebrek-aan-inzicht-getuigende vragen te beantwoorden, voor vele suggesties over hoe hardnekkige onderzoeksproblemen aan te pakken, en voor zijn oog voor detail, dat de kwaliteit van mijn onderzoek en van deze tekst aanzienlijk heeft verbeterd. Ik dank in één adem ook Erik Hostens, het derde lid van onze kwantum-onderzoekscel, voor het verbeteren van talloze kleine en grotere fouten in deze tekst, voor zijn kennis van trivia over The Simpsons, en voor een wezen van een fijne collega tout court.

Ik bedank Sven voor talloze interventies bij mijn vele computerperikelen, Ivan en Kristiaan voor hun behulpzaamheid bij de talloze praktische vragen die ik hen voorschotelde in de aanloop naar mijn doctoraatsverdediging, en al mijn SCD-collega's voor een fijne werksfeer.

Ik bedank ook Ida, Pela, Ilse en Bart, het kwartet dat de ruggegraat van onze afdeling vormt, voor alle logistieke en andere steun.

It is a pleasure to extend my deep gratitude to Prof. Hans Briegel, Prof. Martin Plenio, Koenraad Audenaert, and Prof. Philliphe Jorrand, who have invited me for academic visits to their groups over the past years. In my opinion every one of these visits has been a success, both from a professional as from a personal point of view, and I am very grateful for these experiences. In the past years I have also had the pleasure to meet many fellow researchers, with whom I have had a lot of fun discussing about something-or-other physics topic or simply going to a bar and having a beer: Marc Hein, Robert Raussendorf, Dirk Schlingemann, Nick Jones, Dan Browne, Shashank Virmani, Simon Perdrix,

Mehdi Mhalla, Kai Eckert, Philipp Hyllus, Marcos Curty, and Frank Verstraete, and anyone I may have forgotten − which is undoubtedly the case. I would also like to thank Prof. Gordon Royle for pointing out the existence of a series of articles that have had a substantial impact on my research, and Prof. Nicolas Cerf for being a referee of my FWO application.

Ten slotte hou ik er ook aan om de mensen te bedanken die het dichtst bij me staan: mijn ouders, broer, mijn vriendin, mijn familie en vrienden, bedankt voor ontelbaar-plus-één dingen die niet losjes in een voorwoord van een doctoraat zijn neer te schrijven.

Maarten Van den Nest,
Leuven, mei 2005

Samenvatting

Lokale equivalentie van stabilisator-toestanden en -codes

Inleiding

Het begrijpen van de eigenschappen en het gedrag van kwantumsystemen met vele componenten vormt één van de meest interessante en uitdagende onderzoeksproblemen in de kwantum-informatietheorie (KIT), en niet in het minst is men hard op zoek naar een dieper inzicht in veeldeeltjes-verstrengeling (multiparticle entanglement). De motivatie voor de studie van deze problematiek bestaat er zowel in nieuwe fundamentele inzichten te verwerven als het ontwikkelen van nieuwe toepassingen – één van de meest uitgesproken toepassingen is ongetwijfeld de constructie van een succesvolle kwantum-computer – en natuurlijk zijn beide objectieven sterk met mekaar verweven. In de studie van veeldeeltjes-kwantumsystemen treden er echter vele wiskundige moeilijkheden op omwille van het feit dat het aantal parameters dat nodig is om toestanden van dergelijke systemen, en operaties op deze toestanden, te beschrijven, exponentieel groeit met het aantal componenten van het systeem – om het, vrij vertaald, met de woorden van C. Caves te zeggen, "Er is veel plaats in een Hilbertruimte".

Aangezien de structuur van willekeurige veeldeeltjes-systemen uitermate complex is, is het aangewezen dat men zich in deze studie beperkt tot deelklassen van systemen en operaties die van belang zijn vanuit een fysisch standpunt, en die tegelijk een voldoende transparante beschrijving toelaten, zodanig dat inzicht in de eigenschappen van deze systemen en in het effect van operaties op deze systemen mogelijk wordt. Dit is echter een delicate zaak; uiteraard is het eenvoudig om één of andere marginale klasse van systemen te bedenken die gemakkelijk kan worden beschreven – men dient slechts een verzameling te construeren die door een voldoende klein aantal parameters wordt beschreven – maar dergelijke wiskundige transparantie gaat vaak gepaard met een oververeenvoudiging die van dergelijke aard is dat vele fysisch interessante aspecten van de beschrijving verloren gaan.

In de jaren negentig werd in de KIT het zogenaamde *stabilisator-formalisme* geïntroduceerd, een wiskundig formalisme dat wordt gekenmerkt door de bovenstaande combinatie van wiskundige handelbaarheid en fysisch belang. Het stabilisator-formalisme beschrijft een belangrijke klasse van veeldeeltjes-kwantumtoestanden en operaties op een transparante wijze, met vele toepassingen in de domeinen van kwantum-foutenverbeterende codes, kwantum-computing en kwantum-cryptografie. Het conceptuele vertrekpunt van het stabilisator-formalisme is de observatie dat verscheidene interessante pure n-qubit-toestanden worden gekarakteriseerd door hun *stabilisator*, welke de deelverzameling is van alle Pauli-operatoren die deze toestand invariant laten; hier is de Pauli-groep de eindige deelgroep van $U(2^n)$ die essentieel bestaat uit alle n-voudige tensorproducten van de Paulimatrices en de identiteit. Toestanden die gekarakteriseerd worden door hun stabilisator worden *stabilisator-toestanden* genoemd. Natuurlijk volgt uit hun definitie dat stabilisator-toestanden zeer niet-generische toestanden zijn – de verzameling van alle stabilisator-toestanden op n qubits heeft voor elke n zelfs een eindige cardinaliteit. Niettemin zijn vele belangrijke veelqubit-toestanden stabilisator-toestanden, zoals bijvoorbeeld de spin-singlettoestand, de GHZ-toestand, de kat-toestand en de cluster-toestanden, welke alle frequent worden gebruikt in zowel theoretisch als toegepast onderzoek in de KIT.

Het blijkt dat stabilisator-toestanden compacter kunnen worden beschreven aan de hand van hun stabilisator dan aan de hand van de gangbare voorstelling van een n-qubit pure toestand door een 2^n-dimensionale complexe vector. De belangrijkste reden voor dit opmerkelijke feit is dat de stabilisator van een toestand een deel*groep* van de Pauligroep is, en de compacte beschrijving van stabilisator-toestanden kan vervolgens worden bekomen door deze groep-theoretische structuur uit te buiten. Ook verscheidene interessante operaties op stabilisator-toestanden kunnen op efficiënte wijze worden beschreven door gebruik te maken van de representatie van een stabilisator-toestand door zijn stabilisator (namelijk de *Cliffordoperaties*).

De voorbije jaren werd het stabilisator-formalisme in verscheidene domeinen in de KIT gebruikt. Een van de meest prominente (en eerste) toepassingen van het stabilisator-formalisme situeert zich in het domein van de kwantum-foutenverbeterende codes. Dit zijn constructies die onworpen zijn om de informatie die opgeslagen en verwerkt wordt in een kwantum-computer te beschermen tegen ongewenste maar onvermijdelijke interacties met de omgeving, die deze informatie kunnen beschadigen – een proces dat "decoherentie"wordt genoemd. Daarom zijn kwantum-foutenverbeterende codes essentiële ingrediënten in elk werkbaar model van kwantum-computing. Gottesman [19] en, onafhankelijk daarvan, Calderbank et al. [7] gebruikten het stabilisator-formalisme om een brede en gevierde klasse van kwantum-foutenverbeterende codes te construeren, de *stabilisator-codes*, die sinds hun introductie door vele auteurs zijn bestudeerd en die tegenwoordig tot de standaardleerstof behoren in de KIT.

Een recentere belangrijke toepassing van het stabilisator-formalisme is een model van kwantum-computing dat op metingen is gebaseerd, de *1-richting-kwantum-computer* of *one-way quantum computer* (1WKC), ontwikkeld door Raussendorf en Briegel [38]. Dit veelbelovend model is een alternatief voor het meer standaard model van een kwantumcomputer als een logisch netwerk van kwantum-poorten. In de 1WKC worden algoritmen geïmplementeerd door één-qubit-metingen uit te voeren op een in hoge mate verstrengelde substraat-toestand, weke een stabilisator-toestand is (i.e., een cluster-toestand).

Om de rol van stabilisator-toestanden in bestaande en mogelijk nieuwe toepassingen te begrijpen, is het noodzakelijk dat men inzicht heeft in de niet-lokale eigenschappen van deze toestanden. Inderdaad speelt de hoge graad van veelpartijen-verstrengeling in stabilisator-toestanden een grote rol in de meeste toepassingen van het stabilisator-formalisme in KIT.

De objectieven van ons onderzoek situeren zich in het kader van de theoretische studie van de niet-lokale eigenschappen van stabilisator-toestanden; meer specifiek bestuderen we in deze verhandeling drie verschillende *lokale-equivalentierelaties* op de verzamelingen van stabilisator-toestanden en -codes, namelijk *equivalentie onder stochastische lokale operaties en klassieke communicatie (SLOKC-equivalentie), equivalentie onder lokale unitaire operaties (LU-equivalentie)* en *equivalentie onder lokale Clifford-operaties (LC-equivalentie).* Deze studie is relevant in de context van kwantum-foutenverbeterende codes, kwantum-computing en de theorie van meerpartijen-verstrengeling. We bestuderen verscheidene aspecten inzake bovenstaande lokale-equivalentierelaties, waarbij de nadruk ligt op de volgende drie punten:

(i) de verbanden tussen de drie verschillende lokale-equivalentierelaties,

(ii) de karakterisatie van equivalentieklassen aan de hand van invarianten, en

(iii) het ontwerp van algoritmen om te detecteren of twee stabilisator-toestanden (-codes) tot dezelfde equivalentieklasse behoren.

In het bijzonder boeken we in deze verhandeling de volgende resultaten: we tonen aan dat elke twee SLOKC-equivalente stabilisator-toestanden ook LU-equivalent zijn; we construeren een grote subklasse van stabilisator-toestanden zodat elke twee LU-equivalente toestanden in deze klasse ook LC-equivalent zijn, en formuleren het vermoeden dat dit resultaat geldt voor twee willekeurige stabilisator-toestanden; we leggen een verband tussen LC-equivalentie van n-deeltjes-stabilisator-toestanden en een equivalentierelatie op de verzameling van grafen op n nodes t.o.v. een grafentransformatieregel die in de literatuur gekend is onder de naam *lokale complementatie*; dit resultaat vertaalt het probleem van LC-equivalentie van stabilisator-toestanden in een equivalent probleem in de grafentheorie; we bekomen een efficient algoritme (i.e., polynomiaal in het aantal deeltjes) om te testen of twee gegeven stabilisator-toestanden LC-equivalent zijn; ten slotte construeren we volledige verzamelingen van LU- en LC-invarianten en leggen verbanden tussen deze invarianten.

De wiskundige technieken die worden gehanteerd om bovenstaande problematiek te bestuderen, liggen voornamelijk in het domein van de discrete wiskunde. In dit doctoraatsonderzoek maken we veelvuldig gebruik van technieken uit de lineaire en kwadratische algebra over GF(2), eindige groepentheorie, klassieke codetheorie en grafentheorie.

Hoofdstuk 2: Stabilisator-formalisme en toepassingen

In dit hoofdstuk introduceren we de basisbegrippen die we in het vervolg van de verhandeling bestuderen. We beginnen met de definitie van de *Pauligroep* $\mathcal{G}_n$, welke de groep is die bestaat uit alle n-voudige tensorproducten van de Pauli matrices en de eenheidsmatrix (met een bijkomende globale fasefactor). De Pauligroep heeft verscheidene interessante eigenschappen, die deze groep zeer handelbaar maken; bijvoorbeeld, zijn de elementen van $\mathcal{G}_n$ unitaire, (anti-)Hermitische operatoren die paarsgewijs commuteren of anticommuteren. Een centrale eigenschap is het bestaan van een homomorfisme $\mathcal{B}$ van $\mathcal{G}_n$ naar de additieve groep $\mathbb{F}_2^{2n}$. Dit homomorfisme laat toe om elementen van de Pauli groep (op een fasefactor na) voor te stellen door $2n$-dimensionale binaire vectoren, en het is één van de belangrijke redenen voor het frequente gebruik van de Pauligroep in verscheidene toepassingen in de kwantum-informatietheorie. Vervolgens ontwikkelen we de theorie van *stabilisatoren*; dit zijn deelgroepen van $\mathcal{G}_n$ zodanig dat alle elementen binnen de deelgroep minstens één gezamelijk vast punt hebben (welk een 2^n-dimensionale complexe vector is en daarom een pure toestand op n qubits definieert). In de binaire voorstelling $\mathcal{B}(\mathcal{G}_n) = \mathbb{F}_2^{2n}$ van de Pauligroep komen stabilisatoren overeen met lineaire deelruimten van $\mathbb{F}_2^{2n}$ die zelf-duaal zijn t.o.v. een symplectisch scalair product op deze ruimte. We zullen zien dat bepaalde stabilisatoren juist één gezamelijk vast punt hebben, welk een *stabilisator-toestand* wordt genoemd; stabilisator-toestanden zijn het hoofdonderwerp van deze verhandeling. Omwille van hun relatie met het stabilisator-formalisme kunnen stabilisator-toestanden efficiënt worden beschreven met behulp van het homomorfisme $\mathcal{B}$. In dit hoofdstuk behandelen we de basiseigenschappen van stabilisator-toestanden in relatie tot het binaire formalisme, en bespreken we twee belangrijke toepassingen van stabilisator-toestanden. Eerst beschouwen het model van de 1-wegs-kwantum-computer (one-way quantum computer), welk een universeel model van kwantum-computing is waar algoritmen geïmplementeerd worden door lokale metingen uit te voeren op een substraat-toestand (de *cluster-toestand*), die een stabilisator-toestand is. Ten tweede beschrijven we de basisnoties van de theorie van de stabilisator-codes; deze vormen een uitgebreide klasse van kwantum-foutenverbeterende codes en worden gebruikt om de informatie in een kwantum-computer te beschermen tegen decoherentie.

Een deelklasse van stabilisatortoestanden die van centraal belang is, is de verzameling van *graf-toestanden*. Graf-toestanden op n qubits zijn stabilisatortoestanden die kunnen worden gedefinieerd aan de hand van een graf op n nodes. In hoofdstuk 3 wordt aangetoond dat elke stabilisator-toestand op een graf-toestand kan worden afgebeeld door een lokale unitaire operatie; deze graf-toestand heeft daarom identiek dezelfde niet-lokale eigenschappen als de initiële stabilisator-toestand, zodat het in onze studie van lokale equivalentie geen beperking inhoudt om enkel graf-toestanden te beschouwen. Daarom zijn een belangrijk deel van dit hoofdstuk en deze verhandeling gewijd aan de studie van graf-toestanden.

Dit hoofdstuk heeft de volgende structuur: in paragraaf 2.2 introduceren we de Pauligroep en bespreken we het verband tussen de Pauligroep en binaire algebra. Dan definiëren we stabilisatoren in paragraaf 2.3 en beschrijven we deze groepen in termen van de binaire voorstelling van de Pauligroep. In paragraaf 2.4 definiëren we stabilisator- en graf-toestanden; we geven verscheidene voorbeelden en behandelen de basiseigenschappen van deze toestanden. In paragrafen 2.5 en 2.6 geven we twee toepassingen van het stabilisator-formalisme in kwantum-informatie-theorie, namelijk de 1-wegs-kwantum-computer (paragraaf 2.5) en de theorie van stabilisator-codes (paragraaf 2.6). We formuleren een conclusie in paragraaf 2.7.

Hoofdstuk 3: Lokale equivalentie

In dit hoofdstuk definiëren we de drie types van lokale equivalentie die we in deze verhandeling bestuderen. Deze verschillende types van lokale equivalentie komen tot stand door bepaalde groepen van $2^n \times 2^n$-matrices te beschouwen; twee stabilisator-toestanden (of -codes) op n qubits worden dan equivalent t.o.v. dergelijke groep genoemd als er een element in deze groep bestaat dat de eerste toestand (code) op de tweede afbeeldt. In deze verhandeling zijn we geïnteresseerd in *lokale* operatoren, die op elk van de n qubits afzonderlijk inwerken; deze operatoren hebben de vorm $A_1 \otimes \cdots \otimes A_n$, waarbij de A_i's inverteerbare 2×2-matrices zijn. In het bijzonder zullen we de volgende drie groepen van lokale operaties beschouwen:

- $SL(2,\mathbb{C})^{\otimes n}$ (equivalentie onder stochastische lokale operaties en klassieke communicatie of *SLOKC-equivalentie*);
- $U(2)^{\otimes n}$ (equivalentie onder lokale unitaire operaties of *LU-equivalentie*);
- $\mathcal{C}_n^l = \mathcal{C}_1^{\otimes n}$ (equivalentie onder lokale-Clifford-operaties of *LC-equivalentie*).

Ten eerste is $SL(2,\mathbb{C})$ de groep van alle 2×2-matrices met determinant gelijk aan 1. Een één-qubit-toestand ρ afbeelden op $B\rho B^\dagger$, met $B \in SL(2,\mathbb{C})$, komt overeen met het selecteren van één uitkomst van een POVM-meting die op het systeem in de toestand ρ wordt uitgevoerd. De overeenkomstige lokale equivalentierelatie wordt *equivalentie onder stochastische lokale operaties en klassieke communicatie* of *SLOKC-equivalentie* genoemd. Deze wordt beschouwd als de meest algemene lokale equivalentierelatie. Twee stabilisator-toestanden op n qubits $|\psi\rangle$ en $|\psi'\rangle$ worden SLOKC-equivalent genoemd als er een operator $A \in SL(2,\mathbb{C})^{\otimes n}$ bestaat zodat $A|\psi\rangle \sim |\psi'\rangle$; de verzameling van alle stabilisator-toestanden die SLOKC-equivalent met $|\psi\rangle$ zijn, wordt genoteerd door SLOKC(ψ).

Ten tweede is $U(2)$ de groep van alle unitaire 2×2-matrices, die de 'standaard' unitaire evolutie van een één-qubitsysteem definieert. De overeenkomstige lokale equivalentierelatie wordt *equivalentie onder lokale unitaire operaties* of *LU-equivalentie* genoemd. Twee stabilisator-toestanden op n qubits $|\psi\rangle$ en $|\psi'\rangle$ worden LU-equivalent genoemd als er een operator $U \in U(2)^{\otimes n}$ bestaat zodat $U|\psi\rangle = |\psi'\rangle$; de verzameling van alle stabilisator-toestanden die LU-equivalent met $|\psi\rangle$ zijn, wordt genoteerd met LU(ψ). Noteer dat elke twee LU-equivalente toestanden ook SLOKC-equivalent zijn.

Ten derde is $\mathcal{C}_1$ de Cliffordgroep, gedefinieerd door

$$\mathcal{C}_1 = \left\langle \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \right\rangle. \tag{0.1}$$

De Cliffordgroep is een deelgroep van $U(2)$ die op natuurlijke wijze verschijnt in de context van stabilisator-theorie; het is (een quotiëntgroep van) de groep van alle 2×2 unitaire matrices die de Pauli groep $\mathcal{G}_1$ op zichzelf afbeelden onder conjugatie. De groep $\mathcal{C}_n^l = \mathcal{C}_1^{\otimes n}$ is de *lokale Cliffordgroep* en definieert *equivalentie onder Lokale Clifford-operaties* of *LC-equivalentie*. Twee stabilisator-toestanden op n qubits $|\psi\rangle$ en $|\psi'\rangle$ worden LC-equivalent genoemd als er een operator $V \in \mathcal{C}_n^l$ bestaat zodat $V|\psi\rangle \sim |\psi'\rangle$; de verzameling van alle stabilisator-toestanden die LC-equivalent met $|\psi\rangle$ zijn, wordt genoteerd met LC(ψ). Noteer dat elke twee LC-equivalente toestanden ook LU-equivalent zijn.

Merk op dat we, voor elke stabilisator-toestand $|\psi\rangle$, de volgende sequentie van inclusies hebben:

$$\text{LC}(\psi) \subseteq \text{ LU}(\psi) \subseteq \text{ SLOKC}(\psi). \tag{0.2}$$

Een van de hoofddoelen van dit onderzoek bestaat erin na te gaan of de omgekeerde inclusies ook gelden.

In dit hoofdstuk behandelen we de basiseigenschappen en -begrippen aangaande bovenstaande types van lokale equivalentie. In latere hoofdstukken gaan we over tot een meer diepgaand onderzoek. De structuur van dit hoofdstuk is de volgende. In paragraaf 3.2 bewijzen we dat elke twee SLOKC-equivalente stabilisator-toestanden ook LU-equivalent zijn. Dit resultaat toont aan dat we ons in het vervolg van de verhandeling kunnen beperken tot LU- en LC-equivalentie van stabilisator-toestanden. In paragraaf 3.3 definiëren we de basisbegrippen aangaande LU-equivalentie van stabilisator-toestanden en introduceren we de gerelateerde notie van lokale equivalentie van stabilisator-codes.

In paragraaf 3.4 geven we een formele behandeling van de lokale Clifford-groep en LC-equivalentie van stabilisator-toestanden en codes. Omwille van zijn definitie kan LC-equivalentie van stabilisator-toestanden en codes volledig binnen het binaire stabilisator-formalisme worden behandeld. We gebruiken deze binaire wiskunde om het bekende resultaat aan te tonen dat elke stabilisator-toestand LC-equivalent met een graf-toestand is. Dit resultaat toont aan dat we ons in feite kunnen beperken tot een studie van LC- en LU-equivalentie tussen graf-toestanden onderling. Ten slotte behandelen we de relevantie van LC-equivalentie in de context van de 1WKC. In het bijzonder zien we dat LC-equivalentie van graf-toestanden in dit model de interpretatie heeft van een equivalentierelatie tussen kwantum-algoritmen.

Hoofdstuk 4: LC-equivalentie van graf-toestanden

In het vorige hoofdstuk hebben we gezien dat elke stabilisator-toestand LC-equivalent is met een graf-toestand. Echter, een stabilisator-toestand is typisch LC-equivalent met meerdere graf-toestanden, zodat een studie van LC-equivalentie van graf-toestanden onderling aangewezen is − en deze studie is het onderwerp van dit hoofdstuk.

Het blijkt dat de problematiek van LC-equivalentie van graf-toestanden een heel rijke en mooie structuur heeft en bovendien allesbehalve triviaal is. Eerst zullen we zien dat LC-equivalentie van n-qubit graf-toestanden op natuurlijke wijze een equivalentierelatie induceert op de verzameling van $n \times n$ adjacentie-matrices, zodanig dat twee graf-toestanden LC-equivalent zijn als hun overeenkomstige adjacentie-matrices θ, θ' verbonden zijn door een fractionele lineaire transformatie over $\mathbb{F}_2$ van de vorm

$$(A\theta + B)(C\theta + D)^{-1} = \theta', \tag{0.3}$$

waarbij A, B, C, D diagonale $n \times n$-matrices zijn die voldoen aan $AD + BC = I$. Dergelijke transformaties kunnen worden beschouwd als discrete analogons annex veralgemeningen van *Möbius-transformaties*, die gedefinieerd zijn door

$$x \mapsto \frac{ax + b}{cx + d}, \tag{0.4}$$

waar $x, a, b, c, d \in \mathbb{C}$ en $ad + bc \neq 0$. In dit hoofdstuk bestuderen we de transformaties (0.3) en gebruiken we ze om inzicht te krijgen in het aantal graf-toestanden in een LC-equivalentieklasse en het aantal verschillende LC-equivalentieklassen. Daarna stellen we de vraag of bovenstaande lineaire fractionele transformaties op een combinatorische manier kunnen worden geïnterpreteerd in termen van grafen-transformaties. Met andere woorden onderzoeken we hoe de transformaties (0.3) de topologie van een graf veranderen. In deze context bekomen we het volgende resultaat: we tonen aan dat één enkele elementaire grafen-transformatieregel, genaamd *lokale complementatie*, volstaat om de hele LC-equivalentieklasse van een willekeurige graf te genereren; meer bepaald bewijzen we dat twee adjacentie-matrices gerelateerd zijn door een transformatie (0.3) als en slechts als hun overeenkomstige grafen gerelateerd zijn door een sequentie van lokale complementaties. Dit levert een volledige vertaling van de matrixtransformaties (0.3), en dus van LC-equivalentie van graf-toestanden, in termen van eenvoudige grafentransformaties.

We stellen vast dat lokale complementatie al door verscheidene auteurs bestudeerd is in de grafentheorie, meest in het bijzonder door A. Bouchet. Daarom kunnen interessante inzichten worden verworven door de resultaten in deze literatuur te bestuderen en na te gaan welke van deze resultaten interessant zijn in onze KIT-problematiek. In dit hoofdstuk behandelen we het voor ons meest interesante resultaat, welk een efficiënt algoritme is dat detecteert of twee gegeven grafen gerelateerd zijn door een sequentie van lokale complementaties. Het algoritme heeft een polynomiale complexiteit in het aantal nodes van de grafen. De verbanden tussen LC-equivalentie van graf-toestanden, lineaire fractionele transformaties van adjacentie-matrices en lokale complementatie van grafen, brengt ons tot de conclusie dat dit algoritme kan worden gebruikt om na te gaan of twee stabilisator-toestanden LC-equivalent zijn.

Dit hoofdstuk heeft de volgende structuur: in paragraaf 4.2 leggen we het verband tussen LC-equivalentie van graf-toestanden en equivalentie van adjacentie-matrices onder de fractionele lineaire transformaties (0.3), en we bestuderen een aantal basiseigenschappen van deze transformaties. Dan gebruiken we deze formulering van LC-equivalentie om het aantal grafen in een LC-equivalentieklasse te tellen (paragraaf 4.3). We raken ook kort het probleem aan van het tellen van het aantal LC-equivalentieklassen in paragraaf 4.4. In paragraaf 4.5 geven we de definitie van lokale complementatie en tonen dat dat twee adjacentie-matrices gerelateerd zijn door een transformatie (0.3) als en slechts als hun overeenkomstige grafen gerelateerd zijn door een sequentie van lokale complementaties. In paragraaf 4.6 gebruiken we dit resultaat om een efficiënt algoritme te bekomen dat herkent of twee stabilisator-toestanden LC-equivalent zijn. In paragraaf 4.7 bestuderen we het effect van lokale Paulimetingen op graf-toestanden. Ten slotte formuleren we een besluit in paragraaf 4.8.

Hoofdstuk 5: lokale invarianten

In dit hoofdstuk willen we de lokale equivalentieklasse van een stabilisatortoestand of -code karakteriseren aan de hand van lokale *invarianten*. Dit zijn complexe functies $F(\rho_{\mathcal{S}})$, waarbij $\rho_{\mathcal{S}}$ een willekeurige n-qubit-stabilisatortoestand of -code is, die invariant zijn onder de actie van alle elementen in een groep $\mathcal{L}$ van lokale operatoren, i.e.,

$$F(U\rho_{\mathcal{S}}U^{\dagger}) = F(\rho_{\mathcal{S}}), \tag{0.5}$$

voor elke $U \in \mathcal{L}$. Aangezien we geïnteresseerd zijn in LC- en LU-operaties, zal de groep $\mathcal{L}$ in wat volgt gelijk zijn aan de lokale unitaire groep $U(2)^{\otimes n}$ of de lokale Cliffordgroep $\mathcal{C}_n^l$. In de studie van lokale invarianten bestaat het algemene opzet erin om een *volledige verzameling* van invarianten te vinden, i.e., een verzameling van invarianten $\{F_1, F_2, \dots\}$ zodanig dat twee stabilisator-toestanden of -codes $\rho_{\mathcal{S}}$ en $\rho_{\mathcal{S}'}$ op mekaar kunnen worden afgebeeld worden door een operatie in $\mathcal{L}$ als en slechts als $F_i(\rho_{\mathcal{S}}) = F_i(\rho_{\mathcal{S}'})$ voor elke i. Een volledige verzameling van invarianten definieert een toestand of code $\rho_{\mathcal{S}}$ modulo een operatie in $\mathcal{L}$. Om een volledige verzameling van lokale invarianten te bekomen, zullen we verschillende technieken gebruiken naargelang we LU- of LC-equivalentie beschouwen. In het laatste geval kunnen we in het binaire formalisme werken, en enkele ad hoc methoden zullen volstaan om een eindige volledige verzameling van LC-invarianten te construeren. Algemene lokale unitaire operaties kunnen niet in het binaire formalisme worden beschreven, en we zullen daarom meer gesofistikeerde technieken gebruiken om LU-invarianten te bestuderen. Deze technieken vinden we in een tak van de wiskunde die invariantentheorie wordt genoemd. Onze voornaamste doelstelling bestaat er, ten eerste, in om de beschikbare algemene methoden uit invariantentheorie te gebruiken om LU-invarianten te construeren; ten tweede gaan we na of en hoe deze invarianten kunnen worden vertaald in het binaire stabilisator-formalisme.

Dit hoofdstuk is als volgt gestructureerd. In paragraaf 5.2 behandelen we LC-invarianten van stabilisator-toestanden en -codes. Gebruik makend van het binaire formalisme geven we voorbeelden van eenvoudige maar belangrijke invarianten en we bespreken hun relevantie vanuit een KIT-standpunt. Dan veralgemenen we deze eenvoudige invarianten en bekomen zo een eindige volledige verzameling van LC-invarianten van stabilisator-toestanden en -codes. In paragraaf 5.3 beschouwen we LU-invarianten. Eerst geven we een overzicht van de relevante gekende resultaten en dan passen we deze resultaten toe op onze concrete situatie. Uiteindelijk bekomen we een beschrijving van een volledige (oneindige) verzameling van LU-invarianten binnen het binaire stabilisator-formalisme. Ten slotte bespreken we gelijkenissen tussen onze verzamelingen van LC- en LU-invarianten.

Hoofdstuk 6: LU- versus LC-equivalentie

In vorige hoofdstukken hebben we verscheidene aspecten van LC- en LU-equivalentie van stabilisator-toestanden en -codes in detail onderzocht. Tijdens dit onderzoek – en voornamelijk in hoofdstuk 5, dat lokale invarianten behandelde – hebben we meerdere gelijkenissen gezien tussen LC- en LU-equivalentie van stabilisator-toetanden (codes). Vandaar dat de natuurlijke vraag of er in feite een verschil is tussen deze twee equivalenties, zich opdringt. Deze vraag wordt behandeld in dit hoofdstuk; m.a.w., we onderzoeken of elke twee LU-equivalente stabilisator-toestanden ook LC-equivalent zijn.

We tonen aan dat het antwoord op bovenstaande vraag positief is voor een grote deelklasse van stabilisator-toestanden en het is ons doel om met dit resultaat de eerste stappen te zetten naar een volledig antwoord op deze vraag. Het belangrijkste concept dat we gebruiken voor de constructie van onze klasse is dat van *minimale drager* van een stabilisator. Eerst definiëren we dit begrip, waarna we het gebruiken om onze klasse van stabilisator-toestanden te construren zodanig dat elke twee LU-equivalente stabilisator-toestanden in deze klasse ook LC-equivalent zijn. Vervolgens formuleren we het vermoeden dat dit resultaat geldt voor elke twee stabilisator-toestanden.

Noteer dat bovenstaand resultaat, en een mogelijk algemeen bewijs van de bewering dat $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$ voor elke stabilisator-toestand $|\psi\rangle$, een aantal interessante implicaties heeft. Ten eerste toonden we in hoofstuk 3 aan dat $\mathrm{SLOKC}(\psi) = \mathrm{LC}(\psi)$ voor elke stabilisator-toestand. Samen met het huidige resultaat, toont dit aan dat SLOKC-, LU- en LC-equivalentie identieke noties zijn binnen de beschouwede deelklasse van stabilisator-toestanden (en mogelijk voor alle stabilisator-toestanden). Daarom kan men binnen deze klasse spreken van één enkele notie van lokale equivalentie. Ten tweede toonden we in hoofdstuk 4 aan dat LC-equivalentie van graf-toestanden (en bijgevolg van alle stabilisator-toestanden) volledig kan worden begrepen in termen van lokale complementatie. Ten slotte, ook in hoofdstuk 4 construeerden we een efficiënt algoritme om te detecteren of twee stabilisator-toestanden LC-equivalent zijn. Dit toont aan dat de drie lokale equivalentie efficiënt kunnen worden herkend binnen onze klasse.

Dit hoofdstuk heeft de volgende structuur: in paragraaf 6.2 definiëren we de notie van minimale drager. In paragraaf 6.3 presenteren we onze klasse van stabilisator-toestanden zodat $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$ voor elke stabilisator-toestand $|\psi\rangle$ in deze klasse. In paragraaf 6.4 bespreken we de rol van lokale invarianten in de discussie betreffende LU = LC. Ten slotte formuleren we een conclusie in paragraaf 6.5.

Conclusie

In deze verhandeling hebben we lokale equivalentie van stabilisator-toestanden en -codes bestudeerd. Dit probleem is relevant in de studie van veeldeeltjes-verstrengeling, kwantum-computing en kwantum-foutenverbetering. In onze studie van lokale equivalentie hebben we voornamelijk gebruik gemaakt van een beschrijving van stabilisator-toestanden en -codes in termen van binaire algebra; onze bewijzen, berekeningen en resultaten zijn meestal geformuleerd binnen deze beschrijving.

We hebben verscheidene aspecten van lokale equivalentie van stabilisator-toestanden en -codes bestudeerd. Onze voornaamste bijdragen zijn de volgende:

- We bewijzen dat elke twee SLOKC-equivalente stabilisator-toestanden ook LU-equivalent zijn. [48].

- We geven een karakterisatie van wanneer een stabilisator-toestand overeenkomt met een GF(4)-lineare klasieke code [50].
- We voeren een gedetailleerde studie van LC-equivalentie van graf-toestanden uit in termen van transformaties van de geassocieerde grafen en adjacentie-matrices.
  - We beschouwen fractionele lineaire transformaties van adjacentie-matrices en gebruikten deze transformaties om het aantal graf-toestanden in een LC-equivalentieklasse te tellen.
  - We beschrijven LC-equivalentie van graf-toestanden in termen van lokale complementatie van grafen [47].
  - We gebruiken deze karakterisatie in termen van lokale complementatie om een polynomiaal algoritme te bekomen dat detecteert of twee gegeven stabilisator-toestanden LC-equivalent zijn. [45].
- We construeren een volledige, eindige verzameling van LC-invarianten, die de LC-equivalentieklasse van een willekeurige stabilisator-toestand of -code karakteriseert. [46].
- We bestuderen een bestaande volledige verzameling van LU-invariante veeltermen en evalueren deze veeltermen in een willekeurige stabilisator-toestand of -code; dit levert een volledige vertaling van deze invarianten in het binaire stabilisator-formalisme. We tonen dat deze invarianten bij lage graden samenvallen met de bovenstaande LC-invarianten. [49]
- We construeren een grote klasse van stabilisator-toestanden zodanig dat elke twee LU-equivalente toestanden in deze klasse ook LC-equivalent zijn. We formuleren het vermoeden dat dit resultaat geldt voor twee willekeurige stabilisator-toestanden. [50]

Abstract

The stabilizer states constitute a class of multipartite pure quantum states that is of considerable interest in the field of quantum information theory (QIT). A stabilizer state on n qubits is defined as a simultaneous eigenvector of a maximal set of commuting observables in the Pauli group, where the latter essentially consists of all n-fold tensor products of the Pauli matrices and the identity. Stabilizer states are studied in numerous domains in QIT, with particular applications in quantum stabilizer coding theory and measurement-based quantum computation.

In this dissertation we study different local equivalence relations on the sets of stabilizer states and codes, namely equivalence under stochastic local operations and classical communication (SLOCC equivalence), local unitary (LU) equivalence, and local Clifford (LC) equivalence. This study is relevant in stabilizer coding theory, quantum computing and multipartite entanglement theory. The main goals put forward in this work are (i) studying the relations between SLOCC, LU and LC equivalence of stabilizer states, (ii) giving characterizations of different local equivalence classes by means of invariants, and (iii) finding algorithms which detect whether two given stabilizer states or codes lie in the same equivalence class.

The results obtained in this research include the following: we show that every two SLOCC equivalent stabilizer states are also LU equivalent; we construct a large subclass of stabilizer states such that any two LU equivalent states in this class are also LC equivalent, and we conjecture that this results holds for every two LU equivalent stabilizer states; we translate the problem of LC equivalence of stabilizer states to an equivalent problem in graph theory; we obtain an efficient algorithm to recognize whether two stabilizer states are LC equivalent; we obtain complete sets of LC and LU invariants and discuss the relations between these invariants.

Glossary of symbols

Mathematical Notation

$A = (a_{ij})$	matrix A with entries a_{ij}
A^T	transpose of matrix A
$A^\dagger$	Hermitian conjugate of matrix A
A^{-1}	inverse of matrix A
$\det(A)$	determinant of matrix A
$\mathrm{Tr}(A)$	trace of matrix A
$\mathrm{Tr}_{\{i_1 i_2 \ldots\}}(A)$	partial trace of matrix A over subsystems $i_1, i_2, \ldots$
$A \otimes B$	Kronecker product (or tensor product) of matrices A and B
$\mathrm{diag}(v)$	square diagonal matrix with vector v as diagonal

Fixed Symbols

$\mathbb{N}$	set of natural numbers
$\mathbb{N}_0$	set of natural numbers except 0
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{F}_q$	finite field with q elements (exists only when q is a prime power)
$\mathbb{F}_q^n$	n-fold cartesian product of $\mathbb{F}_q$ with itself
$\mathbb{F}^{d\times d'}$	set of $d \times d'$ matrices with entries in the field $\mathbb{F}$
$GL(d, \mathbb{F})$	group of $d \times d$ invertible matrices with entries in the field $\mathbb{F}$
$SL(d, \mathbb{F})$	group of determinant one $d \times d$ matrices with entries in the field $\mathbb{F}$
$U(d)$	group of complex $d \times d$ unitary matrices
$SU(d)$	group of determinant one complex $d \times d$ unitary matrices
$O(d)$	group of real $d \times d$ orthogonal matrices
$SO(d)$	group of determinant one real $d \times d$ orthogonal matrices
$\mathbb{H}_n$	n-qubit Hilbert space, $\mathbb{H}_n \cong \mathbb{C}^{2^n}$
$\mathcal{G}_n$	Pauli group on n qubits
$\mathcal{C}_n^l$	local Clifford group on n qubits
I	identity matrix (dimensions follow from context)
$\sigma_x, \sigma_y, \sigma_z$	Pauli matrices
σ_0	2×2 identity matrix

$\mathcal{S}$	stabilizer in the Pauli group
$\rho_{\mathcal{S}}$	projector associated with the stabilizer $\mathcal{S}$
$\mathcal{S}(\psi)$	stabilizer of stabilizer state $\lvert\psi\rangle$
$G = (V, E)$	graph G with vertex set V and edge set E
$\lvert G\rangle$	graph state associated with graph G
$\theta(G)$	adjacency matrix of the graph G
Θ_n	set of all symmetric $n \times n$ matrices over $\mathbb{F}_2$ with zero diagonal

Acronyms and Abbreviations

LC	local Clifford
LU	local unitary
SLOCC	stochastic local operations assisted by classical communication
POVM	positive operator-valued measure

Contents

Chapter 1

Introduction

Some of the most challenging and interesting problems in quantum information theory (QIT) involve understanding the properties and behavior of quantum systems with many constituents, and not in the least is a deeper insight in multi-particle entanglement most eagerly sought after. The motivations to study this topic are both to gain new fundamental physical insights as to develop new applications, among which the building of a successful quantum computer is certainly one of the most outspoken – and, of course, the above two motivations are deeply intertwined. However, in considering many-body quantum systems many mathematical difficulties arise due to the fact that the number of parameters needed to describe states of such systems, and operations on these states, grows exponentially with the number of constituents – to put it in the words of C. Caves, "Hilbert space is a big place ".

Seeing that the structure of general many-particle systems is exceedingly complex, it is appropriate to restrict oneself to subclasses of systems and operations which are both of interest from a physical point of view and which at the same time allow a sufficiently transparent mathematical description, such that insight in the properties of such systems, and in the effect of operations on these systems, becomes possible. This is, however, a delicate issue; of course, it is very easy to conceive some marginal class of systems which allow a simple mathematical description – one simply has to construct some set specified by a sufficiently small number of parameters – however, such a mathematical transparency is often at the risk of oversimplifying to such an extent that every interesting physical aspect of this description is lost.

In the last decade the QIT community saw the introduction of the *stabilizer formalism*, which is a mathematical framework that exhibits the above desired combination of mathematical transparency and physical interest; the stabilizer formalism describes an important class of many-qubit quantum states and operations in a transparent way, with many applications in quantum error-correction, quantum computing and quantum cryptography. The conceptual starting point of the stabilizer formalism is the observation that a number of interesting n-qubit pure quantum states are uniquely defined by their *stabilizer*, which is the subset of all those Pauli group elements that leave the state invariant; here, the Pauli group is a finite subgroup of $U(2^n)$ essentially consisting of all n-fold tensor products of the Pauli matrices and the identity. States with the above property of being characterized by their stabilizer are hence called *stabilizer states*. Of course, it follows from their definition that stabilizer states are highly non-generic states − in fact, the set of stabilizer states on n qubits has a finite cardinality for every n. Nevertheless, many important multi-qubit pure states are stabilizer states, and examples include the spin singlet state, the GHZ state, the cat-state and the cluster states, which are all frequently used in theoretical investigations as well as applications in QIT.

It turns out that stabilizer states can be described more compactly in terms of their stabilizers rather than in terms of the standard representation of an n-qubit pure quantum state as a complex vector with 2^n components. The main reason for this remarkable fact is that the stabilizer of a state is in fact a subgroup of the Pauli group, and the compact description of stabilizer states is subsequently obtained by exploiting this group-theoretic structure. Also, a number of interesting operations on stabilizer states are efficiently described using the representation of a stabilizer state by its stabilizer (namely *Clifford operations*).

In the past decade, the above basic concepts underlying the stabilizer formalism have been employed in numerous subfields in QIT research. Certainly among the most prominent (and also the first) applications of the stabilizer formalism is found within the theory of quantum error-correction codes; the latter are constructions designed to protect the information stored and processed in a quantum computer from unwanted but inevitable interactions with its environment that may corrupt this information − a process called decoherence. Therefore, quantum error-correcting codes constitute an essential ingredient to any viable model of quantum computation. In quantum coding theory, Gottesman [19] and, independently, Calderbank et al. [7] used the stabilizer formalism to construct a broad and celebrated class of error-correcting codes, called *stabilizer codes*, which, since their introduction, have been studied by many authors and are today regarded as textbook material in quantum information theory.

A more recent major application of the stabilizer formalism is *the measurement-based model of quantum computation*, developed by Raussendorf and Briegel [38]. This promising model, also called the one-way quantum computer, provides an alternative to the "standard" model of a quantum computer as a logic network of quantum gates; in the one-way quantum computer quantum algorithms are implemented by performing single-qubit measurements on a highly entangled substrate state, which is a stabilizer state (i.e., a cluster state).

We note that, next to the theoretical interest in stabilizer states, recently several results have been reported on the realization of such states in the laboratory, see e.g. [28, 9, 54, 44].

In order to understand the role of stabilizer states in existing and possibly new applications in QIT, it is imperative that one has insight in the non-local properties of these states. Indeed, the high degree of multipartite entanglement of stabilizer states in one way or another plays a key role in most of the applications of the stabilizer formalism in quantum information theory. E.g., in quantum coding theory the entanglement in these states is used to distribute the information one wants to protect over many parties, and this entanglement is also exploited to correct errors that may corrupt this information; as another example, in the measurement-based model of quantum computation the entanglement in the cluster state induces strong correlations between the outcomes of local measurements performed on different qubits, making this model a true quantum model of computation that has no classical analogue.

The objectives of this thesis are situated within the theoretical study of the non-local properties of stabilizer states and codes. To be precise, we study different *local equivalence relations* on the sets of stabilizer states and codes. These equivalence relations all come about by fixing certain $2^n \times 2^n$ matrix groups and consequently calling two n-qubit stabilizer states (codes) equivalent with respect to such a matrix group if there exists an operator in this group that maps the first state (code) to the second. We are interested in *local* transformations, which act on each of the n qubits separately; these are transformations of the form $A_1 \otimes \cdots \otimes A_n$, where the A_is are (invertible) 2×2 matrices. In this thesis we will study three types of local equivalence, namely local unitary equivalence (LU), local Clifford equivalence (LC) and equivalence under stochastic local operations and classical communication (SLOCC), to be defined in chapter 3. Our study of local equivalence of stabilizer states and codes is of natural relevance in a number of distinct subfields in QIT; there are in fact three immediate motivations for this research. Firstly, and most obviously, this study is natural in the context of multi-particle entanglement theory. In order to gain insight in the multipartite entanglement present in stabilizer states, it is of course appropriate to investigate the natural quantum operations preserving this entanglement, with the aim of e.g. obtaining a classification of states in entanglement-classes, or in order to gain insight in multipartite entanglement measures etc. A second area where our study is relevant, is found in quantum coding theory. In studying quantum error-correcting codes, a natural notion of "equivalence" of two quantum codes is defined, so as to identify codes with exactly the same error-correcting capabilities (similar to equivalence of classical codes); as it turns out, this equivalence of quantum codes is closely related to the study of local equivalence of stabilizer states and we incorporate it in this thesis. Thirdly, in the model of the one-way quantum computer local equivalence of stabilizer states (in fact: LC equivalence) naturally corresponds to equivalence of quantum algorithms.

Thus, there are in fact a number of quite distinct manifestations of the same mathematical problem which is local equivalence of stabilizer states and codes. In this thesis we will consider various aspects of the problem and, when appropriate, make reference to the different domains of application.

In our study of stabilizer states and codes, and local equivalence, we will many times resort to a central feature of the stabilizer formalism, viz. the description of stabilizer states and codes in terms binary algebra, i.e., algebra over the field GF(2), where arithmetic is performed modulo two. This "binary picture"of the stabilizer formalism allows to completely describe states and codes in terms of a very small number of *discrete* parameters; for example, a stabilizer state on n qubits is essentially described by a $2n \times n$ matrix over GF(2). Here one immediately notices the enormous reduction of complexity involved in using the stabilizer formalism, seeing that a generic state on n qubits is described by a 2^n-dimensional complex vector. Therefore, the very compact discrete description of stabilizer states makes that insight in the nonlocal properties of these states is within reach, a task that is near impossible for general many-qubit states.

Interestingly, the binary representation of the stabilizer formalism gives rise to a rich and multi-faced mathematical framework. Firstly, this binary description establishes a bridge between the "binary world", i.e., algebra over finite fields, and the "complex world", i.e., the finite-dimensional Hilbert space of a system of qubits. In this thesis we will encounter many examples of interesting back-and-forth translations from Hilbert space concepts into notions in the binary world and vice versa. We will also see that a rich variety of techniques from discrete mathematics and combinatorics arise very naturally in the study of the stabilizer formalism, such as finite group theory, graph theory, linear and quadratic algebra over GF(2), and classical coding theory. It is in fact somewhat surprising that, although stabilizer states allow such a simplified description, the discrete mathematics problems one encounters in investigating their properties can still be extremely complex. Indeed, in view of the enormous reduction of complexity from generic many-qubit quantum states to the discrete structure that is the stabilizer formalism, one could expect that many problems become trivial or at least easily solvable. This is, however, not at all the case: we will encounter many examples of problems, which are typically very easy to state without many technicalities, but the solutions of which are nevertheless either highly nontrivial or simply completely out of reach. On the other hand, the rich mathematics involved in this topic and the easy-to-state problems make this research a beautiful and challenging enterprise.

In conclusion, in this thesis we study several aspects of the problem of local equivalence of stabilizer states and codes. This study is relevant in multipartite entanglement theory, quantum coding theory and quantum computing. The main mathematical tools for solving problems lie within the domain of discrete mathematics.

Outline

In **chapter 2** we outline the preliminary material that we will need in the following. We give a detailed account of the stabilizer formalism. In particular, we show how stabilizer states and codes can be described using algebra over GF(2) and how this binary description is related to the Hilbert space description of stabilizer states and codes. This matter will be fundamental to understand the results in the following chapters. We also spend a considerable amount of time studying the set of graph states; graph states are special instances of stabilizer states, which can be constructed on the basis of a graph on n nodes. In chapter 3 we will show that every stabilizer is related to some graph state by a local unitary transformation; this graph state therefore has exactly the same nonlocal properties as the initial stabilizer state, such that there is no restriction in considering only graph states in our study of local equivalence. Therefore, a significant portion of this chapter and this thesis is devoted to the study of graph states.

After having studied the basic properties of stabilizer states and graph states, we discuss two of their applications. First we consider the measurement-based model of quantum computation or the *one-way quantum computer*, which is a universal model of quantum computation where algorithms are implemented by performing one-qubit measurements on a substrate state (the cluster state), which is a stabilizer state. Secondly, we outline the basic concepts of the theory of stabilizer codes. We have two main reasons for considering these two applications; firstly, they serve to illustrate the power of the stabilizer formalism in various fields in QIT and QC; secondly, we will show in chapter 3 that our study of local equivalence has a natural relevance in both of these domains of application.

In **chapter 3** we introduce the three notions of local equivalence of stabilizer states and codes that we will study in this dissertation. We define SLOCC equivalence, LU equivalence and LC equivalence. The main portion of this chapter is devoted to the last of these equivalences, viz. LC equivalence or local Clifford equivalence. The local Clifford group is a finite subgroup of $U(2)^{\otimes n}$ that essentially consists of all local unitary operators that map stabilizer states to stabilizer states. Due to this close connection between stabilizer states and the local Clifford group, LC equivalence of stabilizer states (and codes) can entirely be described within the binary stabilizer formalism. This is one of the main reasons why we will spend a great deal of time investigating LC equivalence. In chapter 3, we simply state the general known theory in this context; e.g., we formally define the local Clifford group, explain the description of LC equivalence within the binary formalism and show that any stabilizer state is LC equivalent to a graph state. We will elaborate on the problem of LC equivalence in later chapters. We also show that every two SLOCC equivalent stabilizer states are also LU equivalent; this is a new result.

Chapters 4, 5 and 6 contain our own contributions. In **chapter 4** we study LC equivalence of graph states. Here our main objective is to translate LC equivalence of graph states into a problem that is purely stated in terms of the corresponding graphs. Using the general theory of chapter 3, one quickly observes that the action of the local Clifford group on graph states corresponds to certain fractional linear transformations of the adjacency matrices of the corresponding graphs. We use this description to count the number of graph states in an LC equivalence class. After this we ask the question how these fractional linear transformations of adjacency matrices affect the topology of the underlying graphs. We will subsequently prove that a single elementary graph transformation rule suffices to generate the entire LC equivalence class of any graph state. This graph transformation rule turns out to be known in graph theory under the name *local complementation*. We use existing results in this context to obtain a polynomial-time algorithm which is able to recognize whether two given stabilizer states are LC equivalent.

In **Chapter 5** we study the characterization of LC and LU equivalence classes of stabilizer states and codes using local invariants. These are functions that take on the same values on locally equivalent states or codes. First we consider LC invariants. Due to the fact that LC equivalence can entirely be described within the binary stabilizer formalism, some ad hoc methods will in fact suffice to construct a finite complete set of LC invariants. i.e., a set that completely characterizes the LC equivalence class of any stabilizer state or code. As for LU equivalence, we will need to resort to more sophisticated methods to describe LU invariants. Here we will use existing general results on the invariant algebra of the local unitary group, which is the set of all polynomials that remain invariant under the natural action of the local unitary group. We will specialize the existing results to our specific setting in order to obtain a complete (yet infinite) set of LU invariants for stabilizer states and codes.

We will in fact observe that there is a striking similarity between the families of LC and LU invariants that we obtain in this chapter. This motivates the question, whether there is in fact a fundamental distinction to be made between LU equivalence and LC equivalence of stabilizer states and codes. That is, we ask the question whether every two LU equivalent stabilizer states (codes) are necessarily LC equivalent (the converse is trivially true). This is the topic of chapter 6.

In **chapter 6** we conjecture that every two LU equivalent stabilizer states are also LC equivalent. We prove this conjecture for a large subclass of stabilizer states, we give examples of states in this class and we discuss some roads towards proving the general conjecture.

Finally, in **chapter 7** we formulate our conclusions, and state some further directions that may be of interest.

Contributions

Parts of this thesis are based on our articles [47, 49, 45, 51, 46, 48, 50] by Van den Nest, Dehaene and De Moor, and [11] by Dehaene, Van den Nest, De Moor and Verstraete.

- In Ref. [47] we translate the action of local Clifford operations on graph states into transformations on their associated graphs - i.e. we provide transformation rules, stated in purely graph theoretical terms, which completely characterize the evolution of graph states under local Clifford operations. As we will show, there is essentially one basic rule, called local complementation, successive application of which generates the orbit of any graph state under local unitary operations within the Clifford group.

- In Ref. [45] we present a polynomial-time algorithm to recognize local Clifford equivalence of stabilizer states.
- In Ref. [49] we study a family of polynomial invariants, introduced in [22], which separate the orbits of multi-qubit density operators ρ under the action of the local unitary group was presented. We consider this family of invariants for the class of those ρ which are the projection operators describing stabilizer codes and give a complete translation of these invariants into the binary framework in which stabilizer codes are described.
- In Ref. [46] we present a finite set of invariants which completely characterizes the LC equivalence class of any stabilizer state.
- In Ref. [50] we study the relation between local unitary (LU) equivalence and local Clifford (LC) equivalence of stabilizer states. We introduce a large subclass of stabilizer states, such that every two LU equivalent states in this class are necessarily LC equivalent. Together with earlier results, this shows that LC, LU and SLOCC equivalence are the same notions for this class of stabilizer states. Moreover, recognizing whether two given stabilizer states in the present subclass are locally equivalent only requires a polynomial number of operations in the number of qubits.
- The article [48] is an overview of the above results on local equivalence of stabilizer states and codes.

The following two articles that are not incorporated in this thesis. The main reason for this is that the contents of these papers are not or only marginally related to the main topic of this dissertation, viz. the study of local equivalence of stabilizer states and codes.

- The article [51] is not incorporated in this thesis. In this reference we study the algebra of complex polynomials which remain invariant under the action of the local Clifford group under conjugation. Within this algebra, we consider the linear spaces of homogeneous polynomials degree by degree and construct bases for these vector spaces for each degree, thereby obtaining a generating set of polynomial invariants.
- The article [11] is not incorporated in this thesis. In this reference we present new algorithms for mixed-state multi-copy entanglement distillation for pairs of qubits. Our algorithms perform significantly better than the best known algorithms. Better algorithms can be derived that are tuned for specific initial states. The new algorithms are based on a characterization of the group of all locally realizable permutations of the 4^n possible tensor products of n Bell states.

Finally, we note that at the end of each chapter there is a "References" section, where we refer in more detail in which of our articles certain results can be retrieved.

Chapter 2

Stabilizer formalism and applications

2.1 Introduction

In the first chapter of this thesis we introduce the preliminary material that we will need in the following. We start by introducing the *Pauli group* $\mathcal{G}_n$, which is the group consisting of all n-fold tensor products of the Pauli matrices and the identity (with an additional phase factor). The Pauli group has several nice properties, which make this group very manageable; e.g., its elements are unitary, (anti-)Hermitian operators that pairwise commute or anticommute. One central feature is that there exists a homomorphism $\mathcal{B}$ between $\mathcal{G}_n$ and $\mathbb{F}_2^{2n}$, where the latter is regarded as an additive group. This homomorphism essentially allows to describe elements of $\mathcal{G}_n$ by $2n$-dimensional binary vectors, and it is one of the main reasons of the wide use of the Pauli group in many applications in QIT. We will subsequently develop the theory of *stabilizers*; these are subgroups of $\mathcal{G}_n$, the elements of which have at least one nontrivial simultaneous fixed point (which is a 2^n-dimensional complex vector and therefore an n-qubit pure state). In the binary description $\mathcal{B}(\mathcal{G}_n) = \mathbb{F}_2^{2n}$ of the Pauli group, stabilizers naturally correspond to linear subspaces of $\mathbb{F}_2^{2n}$ that are self-orthogonal with respect to a symplectic inner product on this space. We will see that certain stabilizers have a unique simultaneous fixed point, which is called a *stabilizer state*; stabilizer states are the main subject of this thesis. Due to their connection with the stabilizer formalism, stabilizer states can be described efficiently using the homomorphism $\mathcal{B}$. In this chapter we consider the basic properties of stabilizer states in relation to the binary formalism, and then we discuss two applications of stabilizer states; first we consider the measurement-based model of quantum computation or the *one-way quantum computer* [38], which is a universal model of quantum computation where algorithms are implemented by performing one-qubit measurements on a substrate state (the cluster state), which is a stabilizer state. Secondly, we outline the very basic concepts of the celebrated theory of stabilizer codes; these constitute a broad class of quantum error-correcting codes and were introduced independently in [19] and [6, 7].

A subclass of stabilizer states of central importance is the set of *graph states*. Graph states on n qubits are stabilizer states that can be defined on the basis of a mathematical graph on n vertices. In chapter 3 we will show that every stabilizer is related to some graph state by a local unitary transformation; this graph state therefore has exactly the same nonlocal properties as the initial stabilizer state, such that there is no restriction in considering only graph states in our study of local equivalence[1]. Therefore, a significant portion of this chapter and this thesis is devoted to the study of graph states.

This chapter is organized as follows: in section 2.2 we introduce the Pauli group and outline the connection between this group and binary algebra. We then define stabilizers in section 2.3 and describe these groups in terms of the binary representation of the Pauli group. In section 2.4 we are then ready to define stabilizer states and graph states; we give several examples and discuss the basic properties of these states. In sections 2.5 and 2.6 we give two applications of the stabilizer formalism in quantum information theory, namely the measurement-based model of quantum computation (section 2.5) and the theory of stabilizer codes (section 2.6). We finally formulate a conclusion in section 2.7.

2.2 Pauli group

In this section we consider the *Pauli group on n qubits*. This group will be the basic mathematical structure that will lead to the definitions of stabilizers and stabilizer states and codes. In this section we perform the ground work needed to introduce these notions and consider the relevant basic properties of the Pauli group.

We start by defining the *Pauli group on one qubit*, denoted by $\mathcal{G}_1$, which is is the finite (multiplicative) matrix group generated by the three Pauli matrices

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.1}$$

Using the elementary properties $\sigma_x\sigma_y = i\sigma_z = -\sigma_y\sigma_x$ and $\sigma_0 = \sigma_x^2 = \sigma_y^2 = \sigma_z^2$, where σ_0 is the 2×2 identity matrix, one finds that

$$\mathcal{G}_1 = \{\pm\sigma_0, \pm i\sigma_0, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}. \tag{2.2}$$

We will call the four matrices σ_0, σ_x, σ_y and σ_z the *sigma matrices*. Thus, the Pauli group on one qubit consists all 16 elements of the form $\alpha\sigma$, where $\alpha \in \{\pm 1, \pm i\}$ is an overall phase factor and σ is one of the sigma matrices. It

[1] This is why most authors deal with graph states rather than with general stabilizer states.

is important to note that the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ are unitary, Hermitian, traceless and pairwise anticommuting operators.

The connection between the Pauli group and binary algebra is obtained by considering the mapping

$$\begin{aligned}
\alpha\ \sigma_0 \equiv \alpha\ \sigma_{00} &\quad \mapsto \quad (0,0) \\
\alpha\ \sigma_x \equiv \alpha\ \sigma_{01} &\quad \mapsto \quad (0,1) \\
\alpha\ \sigma_z \equiv \alpha\ \sigma_{10} &\quad \mapsto \quad (1,0) \\
\alpha\ \sigma_y \equiv \alpha\ \sigma_{11} &\quad \mapsto \quad (1,1),
\end{aligned} \tag{2.3}$$

for every $\alpha \in \{\pm 1, \pm i\}$, which encodes each of the four sigma matrices (up to its overall phase factor) as a pair of bits. This mapping establishes a homomorphism between the multiplicative group $\mathcal{G}_1$ and the additive group $\mathbb{F}_2^2$. This can readily be verified using the elementary properties of the sigma matrices. The set $\mathbb{F}_2 = \mathrm{GF}(2)$ is the finite field with two elements (0 and 1), where arithmetic is performed modulo 2, and $\mathbb{F}_2^2 = \mathbb{F}_2 \times \mathbb{F}_2$ consists of all pairs of bits.

After this brief definition of the Pauli group on one qubit, we now move to our subject of interest, which is the *Pauli group on n qubits*, denoted by $\mathcal{G}_n$ (where $n \in \mathbb{N}_0$.). The group $\mathcal{G}_n$ is the n-fold tensor product of $\mathcal{G}_1$ with itself, i.e.,

$$\begin{aligned}
\mathcal{G}_n &= \mathcal{G}_1 \otimes \cdots \otimes \mathcal{G}_1 \\
&= \{v_1 \otimes \cdots \otimes v_n \mid v_i \in \mathcal{G}_1,\ i = 1, \ldots, n\}.
\end{aligned} \tag{2.4}$$

Therefore, $\mathcal{G}_n$ consists of all 4×4^n elements of the form $\alpha\sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n}$, where $\alpha \in \{\pm 1, \pm i\}$ and $a_i \in \{0, x, y, z\}$, for every $i = 1, \ldots, n$. Elements of $\mathcal{G}_n$ will be called *Pauli operators on n qubits* or simply *Pauli operators*. Pauli operators have the following interesting properties, which are easily verified:

(i) $\mathcal{G}_n$ is a subgroup of $U(2^n)$, i.e., every Pauli operator is unitary;

(ii) If $M = \alpha\sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n} \in \mathcal{G}_n$ has a real overall phase $\alpha \in \{1, -1\}$ then M is Hermitian; otherwise it is anti-Hermitian;

(iii) $M^2 = I$ for every Hermitian $M \in \mathcal{G}_n$ and $M^2 = -I$ for every anti-Hermitian $M \in \mathcal{G}_n$;

(iv) $\mathrm{Tr}(M) = 0$ for every $M \in \mathcal{G}_n \setminus \{\pm I, \pm iI\}$;

(v) every two Pauli operators either commute or anticommute;

(vi) the set $\{\sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n} \mid a_i = 0, x, y, z\}$ is a basis of the vector space of complex $2^n \times 2^n$ matrices.

The mapping (2.3) can readily be generalized to the n-qubit case, yielding an encoding $\mathcal{B}$ of Pauli operators on n qubits as $2n$-dimensional binary vectors:

$$\mathcal{B}:\ M = \alpha\sigma_{u_1 u_1'} \otimes \cdots \otimes \sigma_{u_n u_n'} \ \mapsto\ \mathcal{B}(M) = (u, u') \in \mathbb{F}_2^{2n}, \tag{2.5}$$

where $\alpha \in \{\pm 1, \pm i\}$ and $u = (u_1, \dots, u_n),\ u' = (u'_1, \dots, u'_n) \in \mathbb{F}_2^n$. We will frequently use the notation

$$\sigma_{u_1 u'_1} \otimes \cdots \otimes \sigma_{u_n u'_n} \equiv \sigma_{(u,u')}. \tag{2.6}$$

For example, one has

$$\mathcal{B}(\sigma_x \otimes \sigma_0 \otimes \sigma_z \otimes \sigma_y) = (0,0,1,1,1,0,0,1). \tag{2.7}$$

Note that in (2.5) the information about the ith qubit is distributed over the ith components of the binary vectors u and u'. This is no more than a choice of notation that will simplify calculations below. Also, using the encoding $\mathcal{B}$, all information about overall phases of Pauli operators is lost. However, these overall phases will be irrelevant in (most of) our calculations, and therefore (2.5) contains, for our purposes, all the necessary information about the Pauli operators.

One arrives at the following properties:

Lemma 2.1 *Let $v, w \in \mathbb{F}_2^{2n}$. Then the following statements hold:*

(i) $\sigma_v \sigma_w \sim \sigma_{v+w}$

(ii) *σ_v and σ_w commute if and only if $v^T P w = 0$, where the $2n \times 2n$ matrix P is defined by*

$$P = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \in GL(2n, \mathbb{F}_2). \tag{2.8}$$

Proof: Both properties can easily be verified for the one qubit case $n = 1$ and then generalized to the case of arbitrarily many qubits. □

Corollary 2.2 *The mapping $\mathcal{B}$ is a homomorphism between the multiplicative group $\mathcal{G}_n$ and the additive group $\mathbb{F}_2^{2n}$.*

Proof: This follows immediately from statement (i) in lemma 2.1. □

The matrix P defines a symplectic inner product $\langle v, w \rangle = v^T P w$ on the vector space $\mathbb{F}_2^{2n}$. This can be compared to the case of the complex vector space $\mathbb{C}^{2n}$ carrying a symplectic inner product defined by the matrix

$$\begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}. \tag{2.9}$$

However, as in $\mathbb{F}_2^{2n}$ calculations are performed modulo 2 and therefore $-1 = 1$, we end up with the above symplectic inner product. Lemma 2.1(ii) states that two Pauli operators commute if and only if the corresponding vectors in $\mathbb{F}_2^{2n}$ are orthogonal with respect to the symplectic inner product.

To end this section, we note that it will sometimes be convenient to work with a real variant of the sigma matrices, defined by

$$\begin{aligned} \tau_{00} &= \sigma_{00}, \\ \tau_{01} &= \sigma_{01}, \\ \tau_{10} &= \sigma_{10}, \\ \tau_{11} &= i\sigma_{11} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \end{aligned} \tag{2.10}$$

which we will call the tau matrices. Analogous to (2.5), n-fold products of tau matrices are represented as

$$\tau_{u_1 u_1'} \otimes \cdots \otimes \tau_{u_n u_n'} \equiv \tau_{(u,u')} \mapsto (u, u') \in \mathbb{F}_2^{2n}, \tag{2.11}$$

where $u = (u_1, \ldots, u_n)$, and $u' = (u_1', \ldots, u_n')$.

This concludes our discussion of the basic properties of the Pauli group and the relevance of binary algebra in this context. We are now ready to introduce certain subgroups of the Pauli group called *stabilizers*.

2.3 Stabilizers

Later in this chapter we will be interested in n-qubit states $|\psi\rangle$ that are simultaneous fixed points of several Pauli operators. Of course, not every set of Pauli operators has a common fixed point, and in this section we investigate under which conditions such a simultaneous fixed point exists. We will in particular be interested in subgroups of $\mathcal{G}_n$ that have this property. Note that this does not entail any restriction, since a state $|\psi\rangle$ is a common fixed point of a set of operators $\{M_i\}$ if and only if it is fixed by all operators in the group generated by the set $\{M_i\}$. This leads to the definition of *stabilizers*. Let $\mathbb{H}_n \equiv \mathbb{C}^{2^n}$; for any subgroup $\mathcal{S}$ of $\mathcal{G}_n$, define the space $V_{\mathcal{S}} \subseteq \mathbb{H}_n$ to consist of all $|\psi\rangle$ satisfying

$$M|\psi\rangle = |\psi\rangle \text{ for every } M \in \mathcal{S}. \tag{2.12}$$

A *stabilizer on n qubits* is a subgroup $\mathcal{S}$ for which the space $V_{\mathcal{S}} \subseteq \mathbb{H}_n$ is nontrivial. In other words, $\mathcal{S}$ is a stabilizer if and only if there exists at least one common eigenvector with eigenvalue 1 of all elements in $\mathcal{S}$. The subspace $V_{\mathcal{S}}$ is the *space stabilized by* $\mathcal{S}$. The following properties are easily verified:

Lemma 2.3 *Let $\mathcal{S}$ be a stabilizer on n qubits. Then*

(i) every $M \in \mathcal{S}$ is Hermitian;

(ii) if $M \in \mathcal{S}$ then $-M \notin \mathcal{S}$.

Proof: Let $|\psi\rangle$ be an element of $V_{\mathcal{S}}$, let $M \in \mathcal{S}$ and suppose that M is anti-Hermitian. Then $-I = M^2 \in \mathcal{S}$ and therefore $-I|\psi\rangle = |\psi\rangle$, showing that

$|\psi\rangle = 0$ for every $|\psi\rangle \in V_{\mathcal{S}}$. But this is in contradiction with the definition of a stabilizer, and we conclude that M must be Hermitian. Secondly, suppose that $-M \in \mathcal{S}$. Then $-I = (-M)M \in \mathcal{S}$ which again yields a contradiction. This shows that $-M \notin \mathcal{S}$. This ends the proof. □

We can now prove the following elegant characterization of stabilizers:

Proposition 2.4 *A subgroup $\mathcal{S}$ of $\mathcal{G}_n$ is a stabilizer on n qubits if and only if $\mathcal{S}$ is Abelian and $-I \notin \mathcal{S}$.*

Proof: Let $\mathcal{S}$ be a stabilizer on n qubits and let $0 \neq |\psi\rangle \in V_{\mathcal{S}}$. Firstly, $-I \notin \mathcal{S}$ trivially. Secondly, suppose $M, N \in \mathcal{S}$. Then

$$\begin{aligned} M|\psi\rangle &= |\psi\rangle \\ N|\psi\rangle &= |\psi\rangle \\ [M,N]\,|\psi\rangle &= 0. \end{aligned} \tag{2.13}$$

Moreover, the operators M and N either commute or anticommute (recall that this holds for any two Pauli operators) and we can conclude that M and N must commute. Therefore, $\mathcal{S}$ is Abelian and $-I \notin \mathcal{S}$. Conversely, let $\mathcal{S}$ be an Abelian subgroup of $\mathcal{G}_n$ that does not contain $-I$. Let $V_{\mathcal{S}}$ be the linear space of all vectors stabilized by $\mathcal{S}$. We have to show that $V_{\mathcal{S}}$ is nontrivial. To this end, associate to $\mathcal{S}$ the linear operator $\rho_{\mathcal{S}}$ on $\mathbb{H}_n$ defined by

$$\rho_{\mathcal{S}} = \frac{1}{2^n} \sum_{M \in \mathcal{S}} M \tag{2.14}$$

(the normalization is chosen such as to yield $\mathrm{Tr}\{\rho_{\mathcal{S}}\} = 1$). We claim that this operator is, up to a normalization, the orthogonal projector on the subspace $V_{\mathcal{S}}$. Let us prove this claim. Firstly, note that every $M \in \mathcal{S}$ is Hermitian from lemma 2.3(i). This shows that $\rho_{\mathcal{S}}^{\dagger} = \rho_{\mathcal{S}}$. Secondly,

$$\rho_{\mathcal{S}}^2 = \frac{1}{2^n} \sum_{M \in \mathcal{S}} M \rho_{\mathcal{S}} = \frac{1}{2^n} \sum_{M \in \mathcal{S}} \rho_{\mathcal{S}} = \frac{|\mathcal{S}|}{2^n} \rho_{\mathcal{S}}, \tag{2.15}$$

where we have used that $M\rho_{\mathcal{S}} = \rho_{\mathcal{S}}$ since $\mathcal{S}$ is a group, and we conclude that $\rho_{\mathcal{S}}$ is proportional to an orthogonal projector. Moreover, it is easily verified that the image of $\rho_{\mathcal{S}}$ is exactly the space $V_{\mathcal{S}}$. The result is now proven if we show that $\rho_{\mathcal{S}} \neq 0$. Note that $\rho_{\mathcal{S}}$ is (up to a normalization) a sum of Pauli operators. As the set $\{\sigma_v \mid v \in \mathbb{F}_2^{2n}\}$ is linearly independent, the only way for this sum to be equal to zero is if for every $M \in \mathcal{S}$ one also has $-M \in \mathcal{S}$. But this is impossible from lemma 2.3(ii). This shows that $\rho_{\mathcal{S}} \neq 0$ and the proof is completed. □

Example. It is straightforward to verify that the set

$$\mathcal{S}_{EPR} = \{I,\ \sigma_x \otimes \sigma_x,\ -\sigma_y \otimes \sigma_y,\ \sigma_z \otimes \sigma_z\} \tag{2.16}$$

is an Abelian subgroup of $\mathcal{G}_2$, and, since it does not contain $-I$, the set $\mathcal{S}_{EPR}$ is a stabilizer. In this case, the space stabilized by $\mathcal{S}_{EPR}$ is in fact one-dimensional[2], such that there is a unique (up to an overall phase factor) normalized state which is stabilized by $\mathcal{S}_{EPR}$. This state is the EPR state on 2 qubits

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.17}$$

$\diamond$

Having obtained the above characterization of stabilizers, a next question is how stabilizers are described within the representation of Pauli operators by $2n$-dimensional binary vectors. Below we will see that the image of a stabilizer on n qubits under the mapping $\mathcal{B}$ is a certain linear subspace of $\mathbb{F}_2^{2n}$ which is self-orthogonal[3] with respect to the symplectic inner product. First we need some additional general terminology and a preliminary result.

A set $\{M_1, \dots, M_l\} \subseteq \mathcal{S}$, where $l \in \mathbb{N}_0$, is called a *generating set* of $\mathcal{S}$ if every $M \in \mathcal{S}$ can be written as a product of operators in this set. The elements M_i $(i = 1, \dots, l)$ are called *generators* of $\mathcal{S}$. One can always choose a generating set to be *independent*, which means that no nontrivial product of the generators yields the identity.

We will need the following lemma:

Lemma 2.5 *Let $\mathcal{S}$ be a stabilizer on n qubits. Then $|\mathcal{S}| = 2^l$ for some $l \in \mathbb{N}$.*

Proof: Let $\mathcal{S}$ be generated by l independent elements $M_1, \dots, M_l$. Since all elements of $\mathcal{S}$ are Hermitian, so are the M_is and therefore $M_i^2 = I$ for every $i = 1, \dots, l$. Together with the fact that $\mathcal{S}$ is Abelian, this shows that an arbitrary element $M \in \mathcal{S}$ can be written in a unique way as a product $M = M_1^{x_1} \dots M_l^{x_l}$, where $(x_1, \dots, x_l) \in \mathbb{F}_2^l$, and consequently $|\mathcal{S}| = 2^l$. This ends the proof. $\square$

Next we show how stabilizers are described within the binary description of the Pauli group.

Proposition 2.6 *Let $\mathcal{S}$ be a stabilizer on n qubits with cardinality $|\mathcal{S}| = 2^l$. Then the set $\mathcal{B}(\mathcal{S})$ is an l-dimensional linear subspace of $\mathbb{F}_2^{2n}$ which is self-orthogonal with respect to the symplectic inner product, i.e., $v^T P w = 0$ for every $v, w \in \mathcal{B}(\mathcal{S})$.*

Proof: Let $\mathcal{S}$ be a stabilizer on n qubits with cardinality $|\mathcal{S}| = 2^l$. Firstly, the fact that $\mathcal{B}(\mathcal{S})$ is a linear subspace of $\mathbb{F}_2^{2n}$ trivially follows from the fact that $\mathcal{S}$ is a group and from the property that $\mathcal{B}$ is a homomorphism form $\mathcal{G}_n$ to $\mathbb{F}_2^{2n}$. Secondly, we show that the space $\mathcal{B}(\mathcal{S}) \subseteq \mathbb{F}_2^{2n}$ has cardinality 2^l and is

[2] We will see in prop 2.11 that this simply follows from the fact that $\mathcal{S}_{EPR}$ contains 4 elements.

[3] We will define self-orthogonality in proposition 2.6.

therefore l-dimensional. To see this, first note that $|\mathcal{B}(\mathcal{S})| \leq |\mathcal{S}| = 2^l$ trivially. We will show that the assumption $|\mathcal{B}(\mathcal{S})| < |\mathcal{S}|$ leads to a contradiction, thereby proving that $|\mathcal{B}(\mathcal{S})| = 2^l$. If $|\mathcal{B}(\mathcal{S})| < |\mathcal{S}|$ then there exist $M \neq M' \in \mathcal{S}$ such that $\mathcal{B}(M) = \mathcal{B}(M')$. This implies that M and M' must be equal up to an overall phase, i.e., $M' = \alpha M$ for some $\alpha \in \{-1, \pm i\}$. As M and M' are elements of a stabilizer, these operators are Hermitian from lemma 2.3 and therefore $\alpha = -1$. Therefore, $M = -M'$, but this is in contradiction with lemma 2.3. This shows that $\mathcal{B}(\mathcal{S})$ has dimension l. Finally, recalling that $\mathcal{S}$ is Abelian, it follows from lemma 2.1 that every two elements $v, w \in \mathcal{B}(\mathcal{S})$ satisfy $v^T P w = 0$. This ends the proof. □

Corollary 2.7 *Let $\mathcal{S}$ be a stabilizer on n qubits generated by l independent elements $M_1, \dots, M_l$. Then the set $\{\mathcal{B}(M_1), \dots, \mathcal{B}(M_l)\}$ is a basis of $\mathcal{B}(\mathcal{S})$.*

Proof: Let $x = (x_1, \dots, x_l) \in \mathbb{F}_2^l$ and denote $M_x := M_1^{x_1} \dots M_l^{x_l}$. Then

$$\mathcal{B}(M_x) = \sum_{i=1}^{l} x_i \mathcal{B}(M_i), \tag{2.18}$$

since $\mathcal{B}$ is a homomorphism of groups. It follows that

$$\text{span}\{\mathcal{B}(M_1), \dots, \mathcal{B}(M_l)\} = \left\{\mathcal{B}(M_x) \mid x \in \mathbb{F}_2^l\right\} = \mathcal{B}(\mathcal{S}). \tag{2.19}$$

Therefore $\{\mathcal{B}(M_1), \dots, \mathcal{B}(M_l)\}$ is a generating set of cardinality l of the l-dimensional vector space $\mathcal{B}(\mathcal{S})$. This shows that this set must be a basis of $\mathcal{B}(\mathcal{S})$. □

The above leads to a refinement of lemma 2.5:

Corollary 2.8 *Let $\mathcal{S}$ be a stabilizer on n qubits. Then $|\mathcal{S}| = 2^{n-k}$ for some $k \leq n$.*

Proof: We already know that $|\mathcal{S}| = 2^l$ for some $l \in \mathbb{N}$. We now show that $l \leq n$. Consider a basis $\{s_1, \dots, s_l\}$ of the space $\mathcal{B}(\mathcal{S})$. Then any $v \in \mathcal{B}(\mathcal{S})$ must satisfy the l independent linear constraints $s_i^T P v = 0$ $(i = 1, \dots, l)$. Therefore, v lies in a $(2n - l)$-dimensional subspace of $\mathbb{F}_2^{2n}$. As the dimension of $\mathcal{B}(\mathcal{S})$ is equal to l, we have $l \leq 2n - l$, which proves the result. □

Let $\mathcal{S}$ be a stabilizer on n qubits with $|\mathcal{S}| = 2^{n-k}$. It is standard[4] to present the corresponding binary space $\mathcal{B}(\mathcal{S})$ in terms of a *generator matrix*; this is a $2n \times (n-k)$ matrix S over $\mathbb{F}_2$, the columns of which form a basis of $\mathcal{B}(\mathcal{S})$, i.e.,

$$S = [\mathcal{B}(M_1) \mid \dots \mid \mathcal{B}(M_{n-k})] \in \mathbb{F}_2^{2n \times (n-k)} \tag{2.20}$$

[4]Regarding generator matrices, it is important to note that in this thesis we adopt a different notation from the one used in quantum coding theory. See also the last remark in section 2.6.2.

where $M_1, \ldots, M_{n-k}$ are generators of $\mathcal{S}$. This generator matrix satisfies $S^T P S = 0$ from the self-orthogonality of $\mathcal{B}(\mathcal{S})$. Note that this presentation of the space $\mathcal{B}(\mathcal{S})$ in terms of a generator matrix is non-unique. Indeed, for every $R \in GL(n-k, \mathbb{F}_2)$ the matrix SR is also a generator matrix of $\mathcal{B}(\mathcal{S})$, as a right multiplication of S with an invertible matrix R corresponds to a different choice of basis in $\mathcal{B}(\mathcal{S})$.

We now turn to the following question. Recalling that $V_{\mathcal{S}}$ is the linear space stabilized by $\mathcal{S}$ and that

$$\rho_{\mathcal{S}} = \frac{1}{2^n} \sum_{M \in \mathcal{S}} M \tag{2.21}$$

is (up to a multiplicative constant) the orthogonal projector on $V_{\mathcal{S}}$, we will investigate how the dimension of $V_{\mathcal{S}}$ or, equivalently, the rank of $\rho_{\mathcal{S}}$, is related to the structure of the stabilizer $\mathcal{S}$. In particular, we will show in proposition 2.11 that the rank of $\rho_{\mathcal{S}}$ is equal to 2^k if and only if $|\mathcal{S}| = 2^{n-k}$. In order to prove this proposition, we first gather some preliminary results.

Lemma 2.9 *Let $\mathcal{S}$ be a stabilizer on n qubits generated by $n-k$ independent elements $M_1, \ldots, M_{n-k}$. Let i be any fixed number in the range $1, \ldots, n-k$. Then there exists $M \in \mathcal{G}_n$ such that $MM_i = -M_iM$ and $MM_j = M_jM$ for every $j = 1, \ldots, n-k$, $j \neq i$.*

Proof: Let S be a $2n \times (n-k)$ generator matrix of $\mathcal{S}$. We have to prove that there exists $v \in \mathbb{F}_2^{2n}$ such that $S^T P v = e_i$, where e_i is the ith canonical base vector of $\mathbb{F}_2^{n-k}$. Indeed, then $M = \sigma_v$ satisfies the conditions in the lemma. But the existence of such a vector v is guaranteed, since the $(n-k) \times 2n$ matrix $S^T P$ has rank $n-k$ (over $\mathbb{F}_2$) and therefore its column space is equal to the whole space $\mathbb{F}_2^{n-k}$. □

Lemma 2.9 leads to the following interesting corollary:

Corollary 2.10 *Let $\mathcal{S}$, $\mathcal{S}'$ be two stabilizers on n qubits satisfying $\mathcal{B}(\mathcal{S}) = \mathcal{B}(\mathcal{S}')$. Then there exists $M \in \mathcal{G}_n$ such that $M\rho_{\mathcal{S}}M^\dagger = \rho_{\mathcal{S}'}$.*

Proof: Let $\mathcal{S}$ be generated by $n-k$ independent elements $M_1, \ldots, M_{n-k}$. Then there exist $f_1, \ldots, f_{n-k} \in \mathbb{F}_2$ such that $\mathcal{S}'$ is generated by

$$M_1' = (-1)^{f_1} M_1, \ \ldots, \ M_{n-k}' = (-1)^{f_{n-k}} M_{n-k}. \tag{2.22}$$

A successive application of lemma 2.9 then yields the result. □

We are now ready to prove the following proposition:

Proposition 2.11 *Let $\mathcal{S}$ be a stabilizer on n qubits with $|\mathcal{S}| = 2^{n-k}$. Then the rank of $\rho_{\mathcal{S}}$ is equal to $2^k = 2^n|\mathcal{S}|^{-1}$.*

Proof: We first introduce some notation. Let $\mathcal{S}$ be generated by $n-k$ independent elements $M_1, \dots, M_{n-k}$. For every $x = (x_1, \dots, x_{n-k}) \in \mathbb{F}_2^{n-k}$, let $\mathcal{S}^x$ be the stabilizer generated by the operators

$$(-1)^{x_1} M_1, \dots, (-1)^{x_{n-k}} M_{n-k}. \tag{2.23}$$

Note that $\mathcal{S} = \mathcal{S}^0$. Moreover, one has $\rho(\mathcal{S}^x)\rho(\mathcal{S}^{x'}) = 0$ for every $x, x' \in \mathbb{F}_2^{n-k}$ with $x \neq x'$: this follows from the identity

$$\rho(\mathcal{S}^x) = \frac{1}{2^n} \prod_{i=1}^{n-k} (I + (-1)^{x_i} M_i), \tag{2.24}$$

for every $x \in \mathbb{F}_2^{n-k}$, and the fact that

$$(I + (-1)^a M)\left(I + (-1)^b M\right) = 0 \tag{2.25}$$

for every Hermitian $M \in \mathcal{G}_n$ and for every $a, b \in \mathbb{F}_2$, $a \neq b$. This shows that the operators $\rho(\mathcal{S}^x)$ and $\rho(\mathcal{S}^{x'})$ project on orthogonal subspaces of $\mathbb{H}_n$ whenever $x \neq x'$. Finally, note that

$$\sum_{x \in \mathbb{F}_2^{n-k}} \rho(\mathcal{S}^x) \sim I. \tag{2.26}$$

It follows that the sum of all the ranks of the projectors $\rho(\mathcal{S}^x)$ must be equal to 2^n. But corollary 2.10 shows that the ranks of all projectors are the same, and we conclude these ranks are equal to 2^k. This ends the proof. □

Thus, we have shown that the dimension of the space $V_{\mathcal{S}}$ only depends on the cardinality of the stabilizer $\mathcal{S}$. A for our purposes important implication of proposition 2.11 is the following: if $\mathcal{S}$ is a stabilizer on n qubits with maximal cardinality $|\mathcal{S}| = 2^n$, then $\rho_{\mathcal{S}}$ has rank 1 and therefore projects on a one-dimensional subspace. This subspace contains essentially one pure state $|\psi\rangle$, which is called a *stabilizer state on n qubits*. The stabilizer $\mathcal{S} \equiv \mathcal{S}(\psi)$ is called the stabilizer of the state $|\psi\rangle$. Note that a stabilizer state is completely specified (up to an irrelevant overall phase factor) by its stabilizer. Stabilizer states will be the main subjects of interest in this dissertation and we discuss some of their properties in the next section.

2.4 Stabilizer states and graph states

In this section we consider the general properties of stabilizer states and give several examples. We also define *graph states*, which constitute a subclass of stabilizer states that will play a key role in our study of local equivalence.

2.4.1 Stabilizer states

In the previous section we have shown that a stabilizer state $|\psi\rangle$ on n qubits is the unique (modulo an overall phase factor) simultaneous eigenvector with eigenvalue 1 of all elements in a stabilizer of maximal cardinality 2^n. This stabilizer, denoted by $\mathcal{S}(\psi)$, is the group

$$\mathcal{S}(\psi) = \{M \in \mathcal{G}_n \mid M|\psi\rangle = |\psi\rangle\}. \tag{2.27}$$

Letting $M_1, \ldots, M_n$ be n independent generators of $\mathcal{S}(\psi)$, one can equivalently state that $|\psi\rangle$ is the unique (again, modulo a phase) normalized state satisfying the n equations

$$M_i|\psi\rangle = |\psi\rangle \qquad (i = 1, \ldots, n). \tag{2.28}$$

Indeed, $|\psi\rangle$ satisfies the above equations if and only if $M|\psi\rangle = |\psi\rangle$ for every $M \in \mathcal{S}(\psi)$, since $M = M_1^{x_1} \ldots M_n^{x_n}$ for some $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

In the binary framework, a stabilizer state is usually specified by a $2n \times n$ generator matrix S of its stabilizer; this generator matrix determines the state up to the overall phases of the elements in its stabilizer. In the following, we will denote

$$\rho_\psi := \rho_{\mathcal{S}(\psi)} = |\psi\rangle\langle\psi|. \tag{2.29}$$

Since $|\psi\rangle$ is mostly presented in terms of a generator matrix S, we will also use the notation

$$C_S := \mathcal{B}(\mathcal{S}(\psi)). \tag{2.30}$$

Note that, as $\dim(C_S) = n$, the space C_S is its own orthogonal complement in $\mathbb{F}_2^{2n}$ with respect to the symplectic inner product, and this space is therefore called *self-dual*. It follows that a vector $v \in \mathbb{F}_2^{2n}$ belongs to the space C_S if and only if $w^T P v = 0$ for every $w \in C_S$ or, equivalently, if and only if $S^T P v = 0$.

Example. A first trivial example of a stabilizer state is the computational basis state $|0 \ldots 0\rangle$ on n qubits. Indeed, one readily verifies that the n operators

$$\begin{aligned}
&\sigma_z \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, \\
&\sigma_0 \otimes \sigma_z \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, \\
&\ldots \\
&\sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_z
\end{aligned} \tag{2.31}$$

commute, are independent, and have the state $|0 \ldots 0\rangle$ as an eigenvector with eigenvalue 1. Therefore $|0 \ldots 0\rangle$ is a stabilizer state. The $2n \times n$ generator matrix associated with the operators (2.31) is $[I\ 0]^T$. In fact, a similar argument can be made to show that all computational basis states $|x_1 \ldots x_n\rangle$, where $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$, are stabilizer states with the same generator matrix. $\diamond$

Example. A second (and more important) example is the generalized GHZ state $|GHZ_n\rangle$ on n qubits, which has a stabilizer $\mathcal{S}(GHZ_n)$ generated by the n elements

$$\begin{aligned}
&\sigma_x \otimes \sigma_x \otimes \sigma_x \otimes \sigma_x \otimes \cdots \otimes \sigma_x, \\
&\sigma_z \otimes \sigma_z \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, \\
&\sigma_0 \otimes \sigma_z \otimes \sigma_z \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, \\
&\sigma_0 \otimes \sigma_0 \otimes \sigma_z \otimes \sigma_z \otimes \cdots \otimes \sigma_0. \\
&\cdots
\end{aligned} \tag{2.32}$$

One can again verify that the above operators commute and are independent. This shows that the state $|GHZ_n\rangle$ is a stabilizer states on n qubits. Considering e.g. the case $n = 5$, the generator matrix associated with the operators (2.32) is

$$\left[\begin{array}{ccccc|ccccc}
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot
\end{array}\right]^T, \tag{2.33}$$

where the empty entries "$\cdot$"in the above matrix are zero. Note that the EPR state (2.17) is a special case of this example for $n = 2$. ◇

2.4.2 Graph states

Next we introduce a subclass of stabilizer states that is of considerable interest in stabilizer theory, namely the *graph states*. Graph states on n qubits are stabilizer states for which the defining eigenvector equations (2.28) can be constructed on the basis of a graph on n vertices.

First we state some definitions concerning graphs. Formally, a *graph* is a pair $G = (V, E)$ of sets, where $V = \{1, \ldots, n\}$ is a finite subset of $\mathbb{N}$ and the elements of E are 2-element subsets of V. The elements of V are called the vertices of the graph G and the elements of E are its edges. Usually, a graph is pictured by drawing a (labelled) dot for each vertex and joining two dots i and j by a line if the corresponding pair of vertices $\{i, j\} \in E$. We will only consider *simple* graphs, which have no multiple edges and no loops (a loop is an edge of the form $\{i, i\}$, where $i \in V$). Two vertices $i, j \in V$ are called adjacent vertices, or neighbors, if $\{i, j\} \in E$. The *neighborhood* $N(i)$ of a vertex $i \in V$ is the set of all neighbors of i. The *adjacency matrix* $\theta(G) \equiv \theta$ of a simple graph G on $|V| = n$ vertices describes the adjacency relations between the n vertices of G. It is the symmetric binary $n \times n$ matrix defined by

$$\begin{cases} \theta_{ij} = 1 & \text{if } \{i, j\} \in E \\ \theta_{ij} = 0 & \text{otherwise.} \end{cases} \tag{2.34}$$

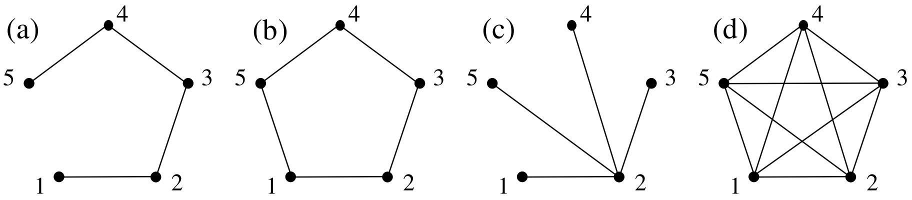

Figure 2.1: Graphs on $n = 5$ vertices: (a) The linear cluster graph LC_5. (b) The ring cluster graph RC_5. (c) The star graph SG_5. (d) The complete graph K_5. [23]

Note that the diagonal elements of θ are zero since G has no loops. In the following, we will denote by Θ_n the set of all adjacency matrices of simple graphs on n vertices, i.e., Θ_n consists of all $n \times n$ symmetric $(0,1)$-matrices with zero diagonal.

Remark. We will always consider the adjacency matrix of a graph as a matrix over $\mathbb{F}_2$, i.e., we consider Θ_n to be a subset of $\mathbb{F}_2^{n\times n}$ (this is in contrast with many texts on (algebraic) graph theory, where the adjacency matrix of a graph is considered as a real matrix). $\diamond$

Example. Some (simple) graphs on 5 vertices are depicted in Fig. 2.1. The adjacency matrix of e.g. the graph RC_5 is equal to

$$\begin{bmatrix} \cdot & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 \\ 1 & \cdot & \cdot & 1 & \cdot \end{bmatrix}. \tag{2.35}$$

$\diamond$

Given a graph G on n vertices with adjacency matrix θ, one defines n commuting Pauli operators

$$\begin{aligned} K_i &= \sigma_x^{(i)} \prod_{j\in N(i)} \sigma_z^{(j)} \\ &= \sigma_x^{(i)} \prod_{k=1}^{n} \left(\sigma_z^{(k)}\right)^{\theta_{ki}}, \end{aligned} \tag{2.36}$$

where $\sigma_x^{(i)}, \sigma_y^{(i)}, \sigma_z^{(i)} \in \mathcal{G}_n$ are those Pauli operators which have resp. $\sigma_x, \sigma_y, \sigma_z$ on the ith position in the tensor product and the identity elsewhere. The *graph state* $|G\rangle$ is the stabilizer state on n qubits with stabilizer generated by the operators $\{K_1, \ldots, K_n\}$. We will use the notation $\rho_G = |G\rangle\langle G|$. Note that the matrix $S = [\theta\ I]^T$ is a generator matrix of $|G\rangle$. This immediately follows from the definition of the generators K_i and corollary 2.7.

Example. The *linear cluster state* $|LC_n\rangle$ on n qubits has a stabilizer $\mathcal{S}(LC_n)$ generated by the n elements

$$\begin{aligned}
&\sigma_x \otimes \sigma_z \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \otimes \sigma_0,\\
&\sigma_z \otimes \sigma_x \otimes \sigma_z \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \otimes \sigma_0,\\
&\sigma_0 \otimes \sigma_z \otimes \sigma_x \otimes \sigma_z \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \otimes \sigma_0,\\
&\sigma_0 \otimes \sigma_0 \otimes \sigma_z \otimes \sigma_x \otimes \sigma_z \otimes \cdots \otimes \sigma_0 \otimes \sigma_0.\\
&\cdots && (2.37)\\
&\sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_z \otimes \sigma_x && (2.38)
\end{aligned}$$

The generator matrix associated with these operators in the case $n = 5$ is $[\theta(LC_5) \mid I]^T$, where

$$\theta(LC_5) = \begin{bmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot \end{bmatrix}^T. \tag{2.39}$$

The corresponding graph for $n = 5$ is depicted in Fig. 2.1(a). ◇

Graph states will play a central role in this dissertation, as it will be shown in corollary 3.16 that any stabilizer state is locally equivalent to a graph state. Therefore, in the study of local equivalence of stabilizer states, there will be no restriction in considering only graph states.

2.4.3 Basic properties

We now consider some general properties of stabilizer states and graph states.

2.4.3.1 Expansion in the Pauli basis

Firstly, recall that (the projector associated with) a stabilizer state $|\psi\rangle$ on n qubits can be written as

$$|\psi\rangle\langle\psi| = \frac{1}{2^n} \sum_{M \in \mathcal{S}(\psi)} M. \tag{2.40}$$

Note that any complex $2^n \times 2^n$ matrix ρ can be written as a linear combination of the Pauli operators $\{\sigma_v \mid v \in \mathbb{F}_2^{2n}\}$, as the latter form a basis of the vector space of complex $2^n \times 2^n$ matrices. More explicitly, one has

$$\rho = \frac{1}{2^n} \sum_{v \in \mathbb{F}_2^{2n}} \mathrm{Tr}(\rho\sigma_v)\ \sigma_v. \tag{2.41}$$

The identity (2.40) shows that $\mathrm{Tr}(|\psi\rangle\langle\psi|\sigma_v) = \langle\psi|\sigma_v|\psi\rangle \in \{0, \pm 1\}$, for every $v \in \mathbb{F}_2^{2n}$. In fact, any pure state that satisfies this property is a stabilizer state. This is proven in the next proposition:

Proposition 2.12 *A state $|\psi\rangle$ on n qubits is a stabilizer state if and only if $\langle\psi|\sigma_v|\psi\rangle \in \{0, \pm 1\}$ for every $v \in \mathbb{F}_2^{2n}$.*

Proof: We have already proven the forward implication. To prove the reverse implication, let $|\psi\rangle$ be a state on n qubits such that $\langle\psi|\sigma_v|\psi\rangle \in \{0, \pm 1\}$, for every $v \in \mathbb{F}_2^{2n}$. Denote by $\mathcal{S}$ the set of all Pauli operators of the form $M = \pm\sigma_v$ ($v \in \mathbb{F}_2^{2n}$) such that $\langle\psi|M|\psi\rangle = 1$. Firstly, every $M \in \mathcal{S}$ stabilizes $|\psi\rangle$ and therefore the set $\mathcal{S}$ is by definition a stabilizer. Moreover, we have

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\sum_{M\in\mathcal{S}} M \equiv \rho_{\mathcal{S}}, \tag{2.42}$$

showing that $\rho_{\mathcal{S}}$ is a one-dimensional projector. Using proposition 2.11 it then follows that $|\psi\rangle$ is a stabilizer state . $\square$

Of course, if $|\psi\rangle$ is a stabilizer state with generator matrix S, one has

$$\langle\psi|\sigma_v|\psi\rangle = \begin{cases} \pm 1 & \text{if } v \in C_S \\ 0 & \text{otherwise.} \end{cases} \tag{2.43}$$

Note that this shows that the vector $\sigma_w|\psi\rangle$ is perpendicular to $|\psi\rangle$ whenever $w \notin C_S$. If $|\psi\rangle \equiv |G\rangle$ is a graph state, the distribution of the signs $\langle\psi|\sigma_v|\psi\rangle = \pm 1$ (where $v \in C_S$) can easily be calculated. In the next proposition it is shown that the quadratic form

$$q_\theta : x \in \mathbb{F}_2^n \ \mapsto\ q_\theta(x) = \sum_{i<j} \theta_{ij} x_i x_j \in \mathbb{F}_2, \tag{2.44}$$

where θ is the adjacency matrix of G, plays a crucial role in determining this distribution of signs:

Proposition 2.13 *Let G be a graph on n vertices with adjacency matrix θ. Then the projector ρ_G can be parameterized as follows:*

$$\rho_G = \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n} (-1)^{q_\theta(x)}\ \tau_{(\theta x, x)}. \tag{2.45}$$

Proof: the state $|G\rangle$ is defined by the n relations $\tau_{(\theta_j, e_j)}|G\rangle = |G\rangle$, where θ_j is the jth column of θ and e_j is the jth canonical basis vector of $\mathbb{F}_2^n$. The stabilizer of $|G\rangle$ consists of all products

$$M_x = \prod_{j=1}^n {\tau_{(\theta_j, e_j)}}^{x_j},$$

where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. After a repeated application of the multiplication rule [10]

$$\tau_{(u,v)}\tau_{(u',v')} = (-1)^{v^T u'}\tau_{(u+u',v+v')},$$

where $u, u', v, v' \in \mathbb{F}_2^n$, we arrive at

$$M_x = (-1)^{q_\theta(x)}\ \tau_{(\theta x, x)}.$$

Since $\rho_G = \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n} M_x$, we obtain the result. □

Remark. It follows from the above result that graph states are *real* quantum states. ◇

This result makes the connection between the Hilbert space description of graph states and the binary stabilizer formalism explicit. It shows that the distribution of the coefficients $\langle G|\tau_v|G\rangle = \pm 1$ is determined by the quadratic form q_θ over $\mathbb{F}_2$ defined by the (adjacency matrix of the) graph G.

2.4.3.2 Expansion in the computational basis

A second manifestation of the connection between the Hilbert space description and the binary formalism is found when one considers the expansion of $|G\rangle$ in the standard basis $\{|x\rangle\}_{x\in\mathbb{F}_2^n}$, i.e., when one writes

$$|G\rangle = \frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n} f_x|x\rangle, \tag{2.46}$$

where the f_xs are complex coefficients. Interestingly, also in this expansion the quadratic form q_θ plays a central role:

Proposition 2.14 *Let G be a graph on n vertices with adjacency matrix $\theta \in \Theta_n$. Then*

$$|G\rangle = \frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n}(-1)^{q_\theta(x)}|x\rangle. \tag{2.47}$$

Proof: Using proposition 2.13, we will show that

$$|\langle G|\left\{\frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n}(-1)^{q_\theta(x)}|x\rangle\right\}|^2 = 1, \tag{2.48}$$

which will yield the result. To prove this, first note that the entries of the 1-qubit operators τ_{ab} can be parameterized as

$$\left(\tau_{ab}\right)_{c,d} = (-1)^{ac}\ \delta_{c+d,b}, \tag{2.49}$$

where $a, b, c, d \in \mathbb{F}_2$. Letting $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, one has

$$\begin{aligned}\langle u|\tau_{(\theta x, x)}|v\rangle &= \prod_{i=1}^{n} \left(\tau_{\theta_i^T x, x_i}\right)_{u_i, v_i} \\ &= \prod_{i=1}^{n} (-1)^{u_i \theta_i^T x}\ \delta_{u_i+v_i, x_i} \\ &= (-1)^{u^T \theta x}\ \delta_{u+v,x}, \end{aligned} \tag{2.50}$$

where θ_i^T denotes the ith row of θ, for every $i = 1, \ldots, n$. Computing the l.h.s of (2.48) then yields (up to a normalization)

$$\begin{aligned}&\sum_{u,v,x} (-1)^{q_\theta(u)+q_\theta(v)+q_\theta(x)+u^T\theta x}\ \delta_{u+v,x} \\ &= \sum_{u,x} (-1)^{q_\theta(u)+q_\theta(x+u)+q_\theta(x)+u^T\theta x}. \end{aligned} \tag{2.51}$$

Denoting by $\mathcal{P}_{\text{lows}}(\theta)$ the strictly lower triangular part of θ, we have $q_\theta(y) = y^T\mathcal{P}_{\text{lows}}(\theta)y$ for every $y \in \mathbb{F}_2^n$, and therefore

$$\begin{aligned}&q_\theta(u) + q_\theta(x+u) + q_\theta(x) + u^T\theta x \\ &= u^T\mathcal{P}_{\text{lows}}(\theta)u + (x+u)^T\mathcal{P}_{\text{lows}}(\theta)(x+u) + x^T\mathcal{P}_{\text{lows}}(\theta)x + u^T\theta x \\ &= 0 \end{aligned} \tag{2.52}$$

and the result follows. □

Thus, the coefficients f_x in the expansion $|G\rangle = (1/2^{n/2})\sum_x f_x|x\rangle$ are equal to ± 1 and again the distribution of the signs is governed by the quadratic form q_θ defined by the adjacency matrix of G. Note that this result can also be used to define graph states without any reference to the stabilizer formalism: given a graph with adjacency matrix θ, the corresponding graph state is (up to a normalization) simply the 2^n-dimensional real vector with components $(-1)^{q_\theta(x)}$, where $x \in \mathbb{F}_2^n$.

The above proposition is in fact a special case of a result in Ref. [10], where it is shown that an expansion similar to (2.47) can in fact be obtained for general stabilizer states. We will quote this result without proof, and the interested reader is referred to Ref. [10].

Proposition 2.15 *Let $|\psi\rangle$ be a stabilizer state on n qubits. Then there exist: $r_a, r_b \in \mathbb{N}$ such that $r_a + r_b \leq n$; an invertible symmetric matrix $Z \in \mathbb{F}_2^{r_a\times r_a}$; a vector $b \in \mathbb{F}_2^{r_a+r_b}$; a vector $c \in \mathbb{F}_2^{n-r_a-r_b}$; and an invertible linear transformation T of $\mathbb{F}_2^n$ such that*

$$|\psi\rangle = \frac{1}{\sqrt{2^{r_a+r_b}}} \sum_{y\in\mathbb{F}_2^{r_a+r_b}} (-i)^{z^T y_a} (-1)^{y_a^T\mathcal{P}_{lows}(Z+zz^T)y_a+b^T y}\ |T\begin{bmatrix} y \\ c \end{bmatrix}\rangle, \tag{2.53}$$

where $z \in \mathbb{F}_2^{r_a}$ is defined by $z_i = Z_{ii}$ for every $i = 1, \ldots, r_a$ and $y = [y_a^T \ y_b^T]^T$, where $y_a \in \mathbb{F}_2^{r_a}$ and $y_b \in \mathbb{F}_2^{r_b}$.

2.4.3.3 Reduced density operators

Next we consider what happens when some of the qubits in a stabilizer state are traced out of the system, and link reduced density operators of stabilizer states to the binary formalism. The definitions and results produced in this subsection will frequently be used throughout this dissertation. They are of particular importance in chapter 5, where we study local invariants. We start with the following definitions: let $M = \alpha\sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n} \in \mathcal{G}_n$; the *support* of M is the set

$$\text{supp}(M) = \{j \in \{1, \ldots, n\} \mid \sigma_{a_j} \neq \sigma_0\}. \tag{2.54}$$

Thus, supp(M) is the set of all i such that the ith tensor factor of M is not equal to the identity. Secondly, for any $\omega \subseteq \{1, \ldots, n\}$ the Pauli operator $M_\omega \in \mathcal{G}_{|\omega|}$ is defined by

$$M_\omega = \alpha \otimes_{j\in\omega} \ \sigma_{a_j}. \tag{2.55}$$

Let $|\psi\rangle$ be a stabilizer state on n qubits, let ω be a subset of $\{1, \ldots, n\}$ and let $\bar{\omega}$ be the complement of ω in $\{1, \ldots, n\}$. Tracing out all qubits of $|\psi\rangle$ outside ω yields a (generally mixed) state $\rho_\omega(\psi)$, which is equal to

$$\rho_\omega(\psi) = \frac{1}{2^{|\omega|}} \sum_{M\in\mathcal{S}(\psi),\ \text{supp}(M)\subseteq\omega} M_\omega. \tag{2.56}$$

This can easily be verified using the identity (2.40). Note that the set

$$\mathcal{S}_\omega(\psi) := \{M \in \mathcal{S}(\psi) \mid \ \text{supp}(M) \subseteq \omega\} \tag{2.57}$$

is a subgroup of $\mathcal{S}(\psi)$ and it is therefore a stabilizer as well. Consequently, proposition 2.11 relates the rank of $\rho_\omega(\psi)$ to the cardinality of $\mathcal{S}_\omega(\psi)$, yielding

$$\text{rank } \{\rho_\omega(\psi)\} = 2^{|\omega|}|\mathcal{S}_\omega(\psi)|^{-1}. \tag{2.58}$$

In chapter 5 we will be particularly interested in the numbers $B_\omega(\psi) := |\mathcal{S}_\omega(\psi)|$. Let us therefore examine how these quantities translate into the binary formalism. Letting S be a generator matrix for $\mathcal{S}$, any element of $\mathcal{S}(\psi)$ has the form $\alpha\sigma_{Sx}$, for some $\alpha = \pm 1$ and $x \in \mathbb{F}_2^n$. Defining the set $n + \omega \subseteq \{n + 1, \ldots, 2n\}$ by

$$j \in n + \omega \text{ if and only if } j - n \in \omega, \tag{2.59}$$

we denote by $S\langle\bar{\omega}\rangle$ the $2(n - |\omega|) \times n$ submatrix of S obtained by removing the rows on positions $j \in \omega \cup (n + \omega)$. It is then easy to verify that

$$\pm\sigma_{Sx} \in \mathcal{S}_\omega(\psi) \text{ if and only if } x \in \ \ker S\langle\bar{\omega}\rangle. \tag{2.60}$$

Therefore, one has

$$\log_2 B_\omega(\psi) = n - \mathrm{rank}_{\mathbb{F}_2}\ S\langle\bar{\omega}\rangle. \tag{2.61}$$

It is interesting to elaborate on the above identity in the case where $|\psi\rangle \equiv |G\rangle$ is a graph state, such that $S = [\theta\ I]^T$, with $\theta \in \Theta_n$ the adjacency matrix of G. Defining the $|\omega| \times (n - |\omega|)$ off-diagonal submatrix $\theta\langle\omega\rangle$ of θ by

$$\theta\langle\omega\rangle = (\theta_{ij})_{i\in\omega, j\in\bar{\omega}}\,, \tag{2.62}$$

one obtains

$$\begin{aligned} \log_2 B_\omega(G) &= |\omega| - \mathrm{rank}_{\mathbb{F}_2}\ \theta\langle\bar{\omega}\rangle \\ &= |\omega| - \mathrm{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle, \end{aligned} \tag{2.63}$$

where in the second equality we have used that $\theta\langle\omega\rangle^T = \theta\langle\bar{\omega}\rangle$ and therefore $\mathrm{rank}_{\mathbb{F}_2}\ \theta\langle\bar{\omega}\rangle = \mathrm{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle$. Using (3.6), we arrive at

$$\log_2 \mathrm{rank}\ \{\rho_\omega(G)\} = |\omega| - \log_2 B_\omega(G) = \mathrm{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle. \tag{2.64}$$

Let us illustrate the above notions with an example.

Example. Consider the graph SG_5 in Fig. 2.1 and denote $S = [\theta(SG_5)\ I]^T$, where

$$\theta(SG_5) = \begin{bmatrix} \cdot & 1 & 1 & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \tag{2.65}$$

is the adjacency matrix of the star graph on 5 vertices. Then e.g.

$$\theta\langle\{1,2,3\}\rangle = \begin{bmatrix} 1 & 1 \\ \cdot & \cdot \\ \cdot & \cdot \end{bmatrix}, \tag{2.66}$$

which has rank one over $\mathbb{F}_2$ and consequently the matrix $\rho_{\{1,2,3\}}(SG_5)$ has rank two. ◇

Eq. (2.64) shows in particular that $|G\rangle$ is a *fully entangled* state if and only if $\theta\langle\omega\rangle \neq 0$ for every $\omega \subseteq \{1, \dots, n\}$ [5]. Graphs that fulfill this property are called *connected graphs*. If a graph is not connected, it is called *disconnected*. The

[5] A state is called fully entangled if it cannot be written as a tensor product of two states on smaller Hilbert spaces. Therefore, a stabilizer state $|\psi\rangle$ is fully entangled if and only if $\rho_\omega(\psi)$ is not a pure state for every ω. This in turn is equivalent to stating that the rank of $\rho_\omega(\psi)$ must be strictly greater than 1. Using (2.64), this shows that $|G\rangle$ is fully entangled if and only if $\theta\langle\omega\rangle \neq 0$ for every ω.

motivation for this terminology is the following: by definition, a disconnected graph has an adjacency matrix of the form

$$\begin{bmatrix} \theta_1 & 0 \\ 0 & \theta_2 \end{bmatrix} \tag{2.67}$$

up to a simultaneous permutation of rows and columns, where $\theta_1 \in \Theta_{n_1}$ and $\theta_2 \in \Theta_{n_2}$ for some $n_1, n_2 \leq n$. Therefore, G consists of two smaller graphs G_1 and G_2, with adjacency matrices θ_1 and θ_2, respectively, such that no vertex from G_1 is adjacent to any vertex of G_2. This clearly motivates why such a graph is called "disconnected". We have therefore shown the following:

Proposition 2.16 *Let G be a graph. Then the corresponding graph state $|G\rangle$ is fully entangled if and only if G is connected.*

When asking questions concerning local equivalence there is of course no restriction in considering only fully entangled states. In the following, we will therefore only consider connected graphs.

2.4.3.4 GF(4) representation and linearity

Next to the binary stabilizer formalism that we have adopted in this dissertation, there is also a well known representation of stabilizers in terms of algebra over the field $\mathbb{F}_4 = \text{GF}(4)$. The latter is the finite field of 4 elements, which can be written as $\mathbb{F}_4 = \{0, 1, \xi, \xi^2\}$. Addition and multiplication in $\mathbb{F}_4$ satisfy the rules

$$\begin{aligned} 1+1 = \xi+\xi = \xi^2+\xi^2 &= 0 \\ 1+\xi &= \xi^2. \end{aligned} \tag{2.68}$$

Note that addition in $\mathbb{F}_4$ is performed modulo 2. Similar to (2.3), one now uses the encoding

$$\sigma_0 \mapsto 0,\ \sigma_z \mapsto 1,\ \sigma_x \mapsto \xi,\ \sigma_y \mapsto \xi^2, \tag{2.69}$$

and consequently Pauli operators on n qubits are represented as n-dimensional vectors with entries in $\mathbb{F}_4$. As in the binary description, the multiplicative structure of $\mathcal{G}_n$ becomes the additive structure of $\mathbb{F}_4^n$. Therefore, every stabilizer $\mathcal{S}(\psi)$ on n qubits corresponds to an *additive* subset (or *code*) of $\mathbb{F}_4^n$, i.e., the sum of any two vectors in this set again belongs to this set. Analogous to the binary case, this additive code is presented in terms of a generator matrix, which now has dimensions $n \times n$. Moreover, the property that a stabilizer is an Abelian group can again be translated into a self-duality property of the corresponding additive code over $\mathbb{F}_4$ with respect to a certain inner product (the *trace inner product*). As the details of this inner product are irrelevant in the following, we will omit them and the interested reader is referred to Ref. [7].

We will occasionally be interested in those specific stabilizer states with stabilizers corresponding to codes over $\mathbb{F}_4$ that are closed under scalar multiplication with ξ. Such codes are genuine linear subspaces of $\mathbb{F}_4^n$, as they are closed under taking linear combinations with coefficients in $\mathbb{F}_4$. They are therefore called $\mathbb{F}_4$-linear codes. Interestingly, $\mathbb{F}_4$-linearity of a stabilizer can be characterized elegantly in terms of a quadratic constraint on its generator matrix:

Theorem 2.17 *Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix $S = [S_z^T\ S_x^T]^T$, where S_z and S_x are $n \times n$ blocks. Then C_S is $\mathbb{F}_4$-linear if and only if*

$$S_z^T S_z + S_x^T S_x + S_z^T S_x = 0. \tag{2.70}$$

Proof: Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix $S = [S_z^T\ S_x^T]^T$. Every element in $\mathbb{F}_4$ has the form $a1 + b\xi \equiv a + b\xi$, where $(a, b) \in \mathbb{F}_2^2$. Using the identity $\xi^2 = \xi + 1$, multiplication of $a + b\xi$ with a second element $a' + b'\xi$, where also $(a', b') \in \mathbb{F}_2^2$, yields

$$(a + b\xi)(a' + b'\xi) = aa' + bb' + (ab' + ba' + bb')\xi. \tag{2.71}$$

Consequently, the set $\mathbb{F}_2^2$ inherits a multiplication law $\odot$ from $\mathbb{F}_4$, defined by

$$(a, b) \odot (a', b') = (aa' + bb', ab' + ba' + bb'), \tag{2.72}$$

and $\mathbb{F}_2^2$, with the multiplication $\odot$ and the standard addition modulo 2, is a field isomorphic to $\mathbb{F}_4$. It follows that the set $\mathbb{F}_2^{2n}$ with the standard addition of vectors modulo 2 and the scalar multiplication $\odot$, is an n-dimensional vector space over $\mathbb{F}_4$; here, the scalar multiplication is defined as follows: letting $v \in \mathbb{F}_2^{2n}$ and $(a, b) \in \mathbb{F}_2^2$, the vector $w := (a, b) \odot v$ is defined by

$$(w_i, w_{n+i}) = (a, b) \odot (v_i, v_{n+i}), \tag{2.73}$$

for every $i = 1, \ldots, n$. With these definitions, it follows that the binary space C_S is $\mathbb{F}_4$-linear if and only if $(0, 1) \odot v \in \mathcal{C}_S$ for every $v \in C_S$. Note that the action $(a, b) \to (0, 1) \odot (a, b)$ is linear transformation on the vector $(a, b) \in \mathbb{F}_2^2$. Indeed, one has

$$(0, 1) \odot (a, b) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \tag{2.74}$$

Consequently, if $v \in \mathbb{F}_2^{2n}$ then $(0, 1) \odot v$ corresponds to

$$\begin{bmatrix} 0 & I \\ I & I \end{bmatrix} v, \tag{2.75}$$

where I is the $n \times n$ identity matrix and 0 is here the $n \times n$ zero matrix. Denoting the columns of S by S_j $(j = 1, \ldots, n)$, this shows that C_S is $\mathbb{F}_4$-linear if and only if

$$(0, 1) \odot S_j \in \mathcal{C}_S \tag{2.76}$$

for every $j = 1, \ldots, n$, as the columns of S form a basis of C_S (regarded as a vector space over $\mathbb{F}_2$). Using (2.75) and the fact that any vector $v \in \mathbb{F}_2^{2n}$ belongs to C_S if and only if $S^T P v = 0$, we find that $\mathcal{C}_S$ is $\mathbb{F}_4$-linear if and only if

$$S^T P \begin{bmatrix} 0 & I \\ I & I \end{bmatrix} S = 0. \tag{2.77}$$

This is equivalent to

$$S_z^T S_z + S_x^T S_x + S_z^T S_x = 0, \tag{2.78}$$

which proves the result. □

A natural question is then, whether there exist graphs that define $\mathbb{F}_4$-linear codes. Following theorem 2.17, this is equivalent to finding solutions $\theta \in \Theta_n$ to the equation

$$\theta^2 + \theta + I = 0. \tag{2.79}$$

Unfortunately, solutions to this equation do not exist: (2.79) implies that

$$0 = (\theta^2)_{ii} + \theta_{ii} + 1 = (\theta^2)_{ii} + 1, \tag{2.80}$$

for every $i = 1, \ldots, n$, or, equivalently, $(\theta + I)e = 0$, where $e = (1, \ldots, 1) \in \mathbb{F}_2^n$. However, (2.79) is equivalent to $\theta(\theta + I) = I$ and therefore $\theta + I$ is nonsingular, such that the kernel of this matrix must be trivial. This leads to a contradiction, since we have just shown that the vector e must belong to this kernel. Therefore, there exists no graphs G such that $[\theta\ I]^T$ is the generator matrix of a $\mathbb{F}_4$-linear code. However, this problem can be overcome by allowing θ to have nonzero diagonal. Indeed, there do exist $n \times n$ matrices $\phi = \phi^T$ over $\mathbb{F}_2$, not having an all-zeros diagonal, such that $[\phi\ I]^T$ generates a $\mathbb{F}_4$-linear code. Consider e.g. the simple example

$$\phi = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \tag{2.81}$$

which indeed satisfies $\phi^2 + \phi + I = 0$.

Remark. Note that allowing ϕ to have nonzero diagonal entries corresponds to allowing the corresponding graph to have loops. ◇

In view of the above considerations, we define a simple graph G with adjacency matrix $\theta \in \Theta_n$ to be $\mathbb{F}_4$-*linear* if there exists an $n \times n$ diagonal matrix A such that

$$\begin{bmatrix} \theta + A \\ I \end{bmatrix} \tag{2.82}$$

generates a $\mathbb{F}_4$-linear space. Using theorem 2.17, G is $\mathbb{F}_4$-linear if and only if

$$I + (\theta + A)^2 + \theta + A = 0, \tag{2.83}$$

which is the same as

$$\theta^2 + A\theta + \theta A + \theta + I = 0. \tag{2.84}$$

We will denote the set of all $\mathbb{F}_4$-linear graphs on n vertices by $\mathcal{L}_n$. We will encounter $\mathbb{F}_4$-linear graphs in chapters 4 and 6.

2.5 Measurement-based quantum computation

We now consider a first application of stabilizer states in quantum information theory, viz. the model of the *one-way quantum computer*, denoted by $QC_{\mathcal{C}}$. The $QC_{\mathcal{C}}$ is a universal scheme of quantum computation where algorithms are implemented by performing one-qubit measurements on a cluster state, which is a graph state (see above). Thus, in this model the cluster state acts as a universal *resource state* for quantum computation. The $QC_{\mathcal{C}}$ model, also called the measurement-based model for quantum computation, has been developed quite recently and has already received a considerable amount of attention. In this section we outline the basic concepts underlying this model. We refer the interested reader to [38] and refs therein.

2.5.1 Quantum computation

Before introducing the model of the $QC_{\mathcal{C}}$, let us recall the very basics concerning quantum computation. The standard model of quantum computation is the model of a quantum logic network (QLN). In this QLN model, a quantum algorithm essentially consists of the following steps: first the system is prepared in an input state $|\psi_{\text{in}}\rangle \in \mathbb{H}_m$ (where $m \in \mathbb{N}_0$) in which the information one wants to process is encoded. Then a unitary operation $U \in U(2^m)$ is applied to $|\psi_{\text{in}}\rangle$, transforming this state into an output state $|\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle$. The unitary operation U constitutes the entire quantum computation. The output of the calculation is obtained by performing a sequence of measurements on $|\psi_{\text{out}}\rangle$. In the QLN model, the unitary operator U is implemented by decomposing it into a sequence of elementary unitary operators, which are called *quantum gates*. In other words, one writes U as a product

$$U = U_1 U_2 \dots U_N, \tag{2.85}$$

where the $U_i \in U(2^m)$ are chosen from a set of quantum gates. A set of quantum gates is called *universal* if every unitary operator can be approximated to an arbitrary degree of accuracy by products of gates from this set. For example, it is well known that a universal set of gates is obtained by considering arbitrary one-qubit unitary operations and CNOT-gates on arbitrary couples of qubits. By *one-qubit unitary* is meant a $2^m \times 2^m$ operator having the form $V \otimes I$ up to a permutation of the m qubits, where $V \in U(2)$. A *CNOT gate*,

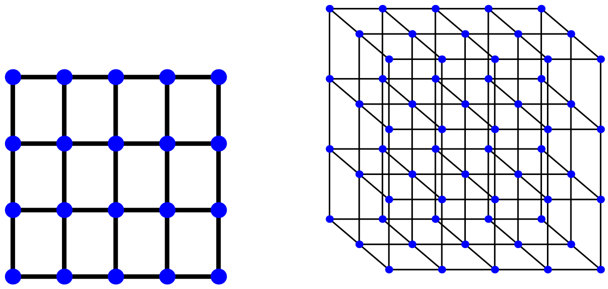

Figure 2.2: Cluster graphs in 2 and 3 dimensions. [24]

short for *controlled-not-gate*, is a $2^m \times 2^m$ operator of the form $U_{\mathrm{CNOT}} \otimes I$ up to a permutation of the qubits, where U_{CNOT} is the 2-qubit operator

$$U_{\mathrm{CNOT}} = \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{bmatrix} \in U(4). \tag{2.86}$$

The decomposition of an arbitrary unitary U into a sequence of elementary gates gives rise to a logical network of gates similar to logical networks in classical computation schemes, hence the term QLN.

2.5.2 Computational model of the $QC_{\mathcal{C}}$

Having established this more or less standard network picture of quantum computation, let us now explain the computational model of the $QC_{\mathcal{C}}$. We have already mentioned that a quantum computation in the $QC_{\mathcal{C}}$ model corresponds to a sequence of one-qubit measurements, i.e. one-qubit projections, on a cluster state. One therefore starts by preparing a cluster state on n qubits. There are in fact several types of cluster states used in the $QC_{\mathcal{C}}$ model, namely the one-dimensional cluster state or linear cluster state, depicted in Fig. 2.1, and the two- and three-dimensional cluster states, the graphs of which are depicted in Fig. 2.2.

The general procedure of a $QC_{\mathcal{C}}$ computation is then the following. The vertex set $V = \{1, \ldots, n\}$ of the cluster graph is partitioned into disjoint subsets

$$V = \omega_0 \cup \omega_1 \cup \cdots \cup \omega_{t_{\max}}, \tag{2.87}$$

where $t_{\max} \leq n$. The computation then consists of *measurement rounds* labelled by $0, 1, \ldots, t_{\max}$, where in each round t the qubits within the set ω_t are measured simultaneously (we note that also the input of the algorithm is incorporated in these measurement rounds). Thus, qubits in the sets ω_t are measured one after the other and therefore $t \in \{0, \ldots, t_{\max}\}$ can be regarded as a discrete time parameter underlying the computation. The set ω_0 consists of all qubits where one of the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ is measured (this is called the *Clifford part* of the computation.) In the subsequent measurement rounds only observables of the form $\cos\phi\ \sigma_x \pm \sin\phi\ \sigma_y$ are measured, where $0 \neq |\phi| < \pi/2$. In these rounds, the measurement bases are adaptive: the measurement outcomes from the qubits in ω_0 specify the measurement bases for the qubits in ω_1 in round 1, the measurement outcomes from the qubits in ω_0 and ω_1 specify the measurement bases for the qubits in ω_2 in round 2, etc. Finally, the result of the computation is calculated from the measurement outcomes obtained in all the rounds.

It is clear that the model of the one-way quantum computer makes no reference to the concept of unitary evolution or quantum gates, nor is there any specification of input and output states. However, it has been shown that any computation in the QLN model can be simulated within the $QC_{\mathcal{C}}$ model, which proves the universality of the $QC_{\mathcal{C}}$ model.

2.5.3 Clifford computations

In this thesis we will be interested in the *Clifford part* of a $QC_{\mathcal{C}}$ computation, or *Clifford computation* in short. Let us therefore examine in more detail how the measurement of a Pauli operator affects a stabilizer state. Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix S and suppose a Hermitian Pauli operator $M \in \mathcal{G}_n$ is measured (in the $QC_{\mathcal{C}}$ model we are in fact interested in the special case where $|\psi\rangle$ is a cluster state and $M = \sigma_a^{(i)}$, where $i \in \{1, \ldots, n\}$ and $a \in \{x, y, z\}$, is a one-qubit Pauli operator, but the argument below works for any stabilizer state and any Pauli operator). There are two possibilities:

(a) M commutes with every element in $\mathcal{S}(\psi)$

(b) M anti-commutes with some element M_1 in $\mathcal{S}(\psi)$

In case (a), it is easy to see that $\pm M \in \mathcal{S}(\psi)$. Indeed, letting $M \sim \sigma_v$ for some $v \in \mathbb{F}_2^{2n}$, it follows that $S^T P v = 0$ and therefore $v \in C_S$, showing that $\pm\sigma_v \in \mathcal{S}(\psi)$. Since $\pm M \in \mathcal{S}(\psi)$, it follows that $M|\psi\rangle = \pm|\psi\rangle$ and we see that $|\psi\rangle$ is an eigenstate of M. Therefore, measurement of M leaves the state $|\psi\rangle$ unchanged. On the other hand, suppose that case (b) occurs. One can then construct a generating set $\{M_1, M_2, \ldots, M_n\}$ of $\mathcal{S}(\psi)$. Without loss of generality, we can assume that M commutes with $M_2, \ldots M_n$ (to see this: suppose that M anticommutes with one of these generators, say M_2, then M_2 can be replaced by $M_2' = M_1 M_2$, yielding a new generating set where now $[M_2', M] = 0$). Now, measuring M is equivalent to applying the projector $(I + M)/2$ with probability p_+, yielding a measurement outcome 1, or the projector $(I - M)/2$ with probability p_-, yielding a measurement outcome -1; here, the measurement probabilities are given by

$$p_+ = \operatorname{Tr}\left(\frac{I+M}{2}\rho_\psi\right) \qquad p_- = \operatorname{Tr}\left(\frac{I-M}{2}\rho_\psi\right). \tag{2.88}$$

Using the properties $M_1\rho_\psi = \rho_\psi$ and $MM_1 = -M_1M$, we find

$$p_+ = \operatorname{Tr}\left(\frac{I+M}{2}M_1\rho_\psi\right) = \operatorname{Tr}\left(M_1\frac{I-M}{2}\rho_\psi\right) = \operatorname{Tr}\left(\frac{I-M}{2}\rho_\psi M_1\right) = p_-, \tag{2.89}$$

yielding $p_+ = p_- = 1/2$. If the result $+1$ occurs, the corresponding projection transforms the state $|\psi\rangle$ to $|\psi_+\rangle \equiv \frac{1}{2}(I+M)|\psi\rangle$, which satisfies

$$M|\psi_+\rangle = |\psi_+\rangle \quad \text{and} \quad M_i|\psi_+\rangle = |\psi_+\rangle \quad (i = 2, \ldots, n). \tag{2.90}$$

Therefore, $|\psi_+\rangle$ is again a stabilizer state, and the corresponding stabilizer $\mathcal{S}(\psi_+)$ is generated by $\{M, M_2, \ldots, M_n\}$. Note that these generators are indeed independent, since $M \notin \mathcal{S}(\psi)$ and $M_2, \ldots, M_n$ are independent from their definition. Analogously, $|\psi_-\rangle \equiv \frac{1}{2}(I-M)|\psi\rangle$ is a stabilizer state with stabilizer $\mathcal{S}(\psi_-)$ generated by the operators $\{-M, M_2, \ldots, M_n\}$. Note that $\mathcal{B}(\mathcal{S}(\psi_+)) = \mathcal{B}(\mathcal{S}(\psi_-))$ and therefore $|\psi_+\rangle$ and $|\psi_-\rangle$ have the same generator matrix

$$[\mathcal{B}(M)\ \mathcal{B}(M_2)\ \ldots\ \mathcal{B}(M_n)]. \tag{2.91}$$

Remark. Note that in the case where one qubit-measurements are performed, say $M = \sigma_a^{(1)}$, the state after the measurement has the form $|\psi_1\rangle|\psi_{\{2,\ldots,n\}}\rangle$, where $|\psi_1\rangle$ is a (stabilizer) state on the first qubit and $|\psi_{\{2,\ldots,n\}}\rangle$ is a stabilizer state on the $n-1$ qubits $\{2, \ldots, n\}$. Also note that Pauli measurements on different qubits can be performed simultaneously, since $\sigma_a^{(i)}$ commutes with $\sigma_b^{(j)}$ for every $a, b = x, y, z$ whenever $i \neq j$. $\diamond$

Example. Consider the linear cluster state $|LC_5\rangle$ and suppose the one-qubit Pauli operator $M = \sigma_z \otimes I \in \mathcal{G}_5$ is measured. Recall that a generator matrix of this graph state is given by $S = [\theta(LC_5) \mid I]$, where $\theta(LC_5)$ is given in (2.39). Note that

$$\mathcal{B}(M) = (1, 0, \ldots, 0) \equiv e_1 \in \mathbb{F}_2^{10}. \tag{2.92}$$

One can easily verify that $S_1^T P e_1 = 1$ and $S_i^T P e_1 = 0$ $(i = 2, \ldots, 5)$, where S_j is the jth column of S. Therefore, M anticommutes with the generator σ_{S_1} of $\mathcal{S}(LC_5)$ and commutes with $\sigma_{S_2}, \ldots, \sigma_{S_5}$. Using the same argument as above, it follows that the stabilizer state with stabilizer generated by $\{M, \sigma_{S_2}, \ldots, \sigma_{S_5}\}$ is obtained when the measurement outcome is $+1$; if -1 is measured then the resulting state has a stabilizer generated by $\{-M, \sigma_{S_2}, \ldots, \sigma_{S_5}\}$. In both cases, a generator matrix of the stabilizer is

$$S'^T = \begin{bmatrix} e_1^T \\ S_2^T \\ S_3^T \\ S_4^T \\ S_5^T \end{bmatrix}^T = \left[\begin{array}{ccccc|ccccc} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{array}\right]^T. \tag{2.93}$$

Using the theory developed in section 2.4.3, it is now an easy exercise to verify that the corresponding stabilizer states are $|f\rangle|LC_4\rangle$, where $f \in \mathbb{F}_2$. In other words, the σ_z measurement has removed the vertex 1 and its neighborhood (i.e., the vertex 2) from the graph LC_5, yielding the graph state $|LC_4\rangle$. $\diamond$

Thus, we have proven that measuring a Pauli operator when an n-qubit system is in a stabilizer state, yields another stabilizer state. This shows that a Clifford computation can entirely be described within the stabilizer formalism, hence our interest in this part of the $QC_\mathcal{C}$ model. An important consequence of this fact is that any Clifford computation can be efficiently simulated classically; this is (a version of) the Gottesman-Knill theorem, proven in [20].

Later in this thesis we will see that our study of local equivalence of stabilizer states has a natural relevance and interpretation within the framework of the one-way quantum computer. More particularly, we will see that LC equivalence of graph states corresponds to a natural equivalence relation between different Clifford computations. For this study we refer to chapters 3 and 4.

To conclude our discussion of the $QC_\mathcal{C}$, we next show how an arbitrary one-qubit unitary rotation $U \in SU(2)$, can be realized in the $QC_\mathcal{C}$ model. This serves as an example of how unitary gates are simulated in the $QC_\mathcal{C}$ model, and it also illustrates how a measurement sequence is typically implemented and which notions are relevant in the study of measurement-based computations. However, this example lies somewhat beyond the scope of this thesis and is written for the interested reader only; one can also directly move to section 2.6.

2.5.4 Illustration: simulation of a one-qubit gate in the $QC_\mathcal{C}$ model

Let $U \in SU(2)$ be a unitary operator mapping a one qubit input state $|\psi_{\text{in}}\rangle \in \mathbb{H}_1$ to the output state $|\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle$. We write U in its Euler representation

$$U \equiv U(\xi, \eta, \zeta) = U_x(\zeta)U_z(\eta)U_x(\xi), \tag{2.94}$$

where

$$U_x(\alpha) = \exp\left(-i\alpha\frac{\sigma_x}{2}\right), \quad U_z(\alpha) = \exp\left(-i\alpha\frac{\sigma_z}{2}\right) \tag{2.95}$$

In order to simulate the unitary gate U, the computational model of the $QC_\mathcal{C}$ as explained above needs to be somewhat adapted, since in the original formulation there is no mentioning of input or output states. In order to incorporate the notions of input and output, one starts the procedure with the preparation of the product state

$$|\psi_{\text{in}}\rangle \otimes (|0\rangle + |1\rangle)^{\otimes 4} \in \mathbb{H}_5 \tag{2.96}$$

rather then preparing a cluster state on 5 qubits; then one applies the operation

$$S = S^{12}S^{23}S^{34}S^{45} \in U(2^5), \tag{2.97}$$

where

$$S^{ab} = \frac{1}{2}(I + \sigma_z^{(a)} + \sigma_z^{(b)} - \sigma_z^{(a)}\sigma_z^{(b)}), \tag{2.98}$$

for $a, b \in \{1, \ldots, 5\}$. The operation S transforms the product state (2.96) into an entangled state. On this resulting state we will now perform a sequence of measurements; therefore, the state obtained after applying the entangling operation S to (2.96) plays the role of resource state as did the cluster state before.

In order to realize the transformation $|\psi_{\text{in}}\rangle \to |\psi_{\text{out}}\rangle$, a sequence of measurements on the qubits 1 to 4 is performed. This will produce the state $|\psi_{\text{out}}\rangle$ on the 5th qubit. In order to state this measurement pattern, we need some definitions: for every $\phi \in [0, 2\pi[$ define

$$B(\phi) = \left\{ \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\phi}|1\rangle}{\sqrt{2}} \right\}, \tag{2.99}$$

which is a basis of $\mathbb{H}_1$. The outcome of a measurement in a basis $B(\phi)$ will be denoted by a bit $s \in \mathbb{F}_2$, where $s = 0$ if and only if the state is projected on the first state of $B(\phi)$. We will denote the outcomes of the measurements on qubits 1 to 4 by $s_1, \ldots, s_4$, respectively. The following measurement procedure is implemented:

(1) measure qubit 1 in the basis $B(0)$;

(2) measure qubit 2 in the basis $B((-1)^{s_1+1}\xi)$;

(3) measure qubit 3 in the basis $B((-1)^{s_2+1}\eta)$;

(4) measure qubit 4 in the basis $B((-1)^{s_1+s_3+1}\zeta)$.

It can be shown (see e.g. [38]) that this sequence of measurements produces the state

$$\sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}U(\xi,\eta,\zeta)|\psi_{\text{in}}\rangle = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}|\psi_{\text{out}}\rangle \tag{2.100}$$

on the 5th qubit. Therefore, we have obtained the desired output state up to a multiplication with the operator $\sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}$, which is called a *byproduct operator*. Applying this operator to the state (2.100) then yields the desired output.

Note that during the sequence of measurements, the information propagates through the cluster. This is illustrated by the fact that in the above procedure the input state is located at the site of qubit 1, whereas the output state is produced on qubit 5.

This concludes our discussion of the one-way quantum computer. This was a first application illustrating the importance of the stabilizer formalism in quantum information theory. We will encounter a second example in the next section, where we discuss stabilizer codes and quantum error-correction.

2.6 Stabilizer codes and quantum error-correction

As a second application of the stabilizer formalism, we next introduce stabilizer codes and their role in the theory of quantum error-correction. Quantum error-correcting codes (QECCs) are constructions designed to protect the information stored in a quantum computer from unwanted interactions with its environment. From a mathematical point of view, a stabilizer code is no more than the stabilized subspace $V_{\mathcal{S}}$ of a stabilizer $\mathcal{S}$. Stabilizer states can therefore be regarded as special cases of stabilizer codes where the space $V_{\mathcal{S}}$ is one-dimensional (in this context, stabilizer states are called *self-dual* stabilizer codes). In the following we will first develop the basic notions of quantum error-correction and then consider stabilizer codes and the very basics concerning their error-correcting capabilities. The interested reader is referred to e.g. [8], [33], [5] and [19] for introductory and/or extensive accounts on QECCs.

2.6.1 Quantum error-correction

In this section we state the basic principles of the theory of quantum error-correction. We start with the following definition: a *quantum channel* $\mathcal{F}$ on the n-qubit Hilbert space $\mathbb{H}_n$ is a linear map of the form

$$\rho \mapsto \mathcal{F}(\rho) = \sum_{a=1}^{m} E_a \rho E_a^{\dagger}, \tag{2.101}$$

where ρ is an arbitrary $2^n \times 2^n$ density operator, $m \in \mathbb{N}_0$ and the E_as are $2^n \times 2^n$ matrices. Quantum channels model the most general evolution of a quantum system. In the following, the channel $\mathcal{F}$ represents an *unwanted* evolution of a quantum system − i.e., the map $\mathcal{F}$ represents noise operations or quantum *errors*. The operators E_a are therefore called the *error operators* of the channel. It is the goal of quantum coding theory to protect quantum systems from such errors. In particular, one wants to recover an initial state ρ after it has been affected by the channel $\mathcal{F}$. This process is called *error correction*. Note that it is of course not possible to correct arbitrary errors, since in general the map $\mathcal{F}$ is not invertible[6]. However, there may exist a subspace of $\mathbb{H}_n$ such that the restriction of $\mathcal{F}$ to this subspace is invertible. This leads to the following definition: a subspace V of $\mathbb{H}_n$ is called a *quantum error-correcting code* for the channel $\mathcal{F}$ if there exists a channel $\mathcal{D}$ such that $\mathcal{D}(\mathcal{F}(\rho)) \sim \rho$ for all density operators ρ on the subspace V. The channel $\mathcal{D}$ is called the *error-correction operator* of $\mathcal{F}$. It is to be a trace-preserving channel, i.e., it has error operators $\{D_l\}$ satisfying

$$\sum D_l^{\dagger} D_l = I. \tag{2.102}$$

[6] In fact, only channels which are unitary operations are invertible. [33]

This constraint is imposed to ensure that the recovery operation occurs with unit probability. As we will see below, the error-correction operation is typically implemented in two steps: first a sequence of measurements is performed and then a unitary operation (which depends on the measurement outcomes) is applied on the state obtained after these measurements.

Thus, a QECC for a given channel is a linear subspace of $\mathbb{H}_n$ such that the restriction of the channel to this subspace can be inverted by an error-correcting operator. While this definition of QECCs involves the error-correcting operator, the following characterization depends only on the error operators of the channel.

Theorem 2.18 *Let $\mathcal{F}$ be a quantum channel on $\mathbb{H}_n$ with error operators E_a $(a = 1, \ldots, m)$. A subspace V of $\mathbb{H}_n$ is a QECC for $\mathcal{F}$ if and only if*

$$PE_a^\dagger E_b P = c_{ab} P \tag{2.103}$$

for every $a, b = 1, \ldots, m$, where P is the orthogonal projector on the space V and c_{ab} are complex coefficients. Letting $\{|\psi_i\rangle\}_i$ be an orthogonal basis of V, this is equivalent to

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = c_{ab}\delta_{ij}, \tag{2.104}$$

for every $a, b,\ i,\ j$.

A proof of this theorem can be found in Ref. [5]. The conditions (2.104) are called the error-correcting conditions of a quantum code. If these conditions hold for a set of error operators $\{E_a\}$, this set is called a *correctable* set of errors of the code V. Interestingly, the following result shows that if the error operators $\{E_a\}$ are correctable, also a whole class of errors that can be obtained from $\{E_a\}$ are correctable errors for V:

Proposition 2.19 *If the conditions (2.104) hold for the set of error operators $\{E_a\}$, they also hold for the set of all linear combinations of these error operators.*

We refer to e.g. Ref. [5] for a proof of this proposition. This result is remarkable, as it allows for a *discretization* of the errors that are to be corrected: if a code can correct the errors in a finite set $\{E_a\}_{a=1}^m$, it can correct all errors in the linear space of operators

$$\{\sum_{a=1}^m c_a E_a \mid c_a \in \mathbb{C}\}. \tag{2.105}$$

Conversely, if one wants to design a code that is to correct all error operators in some linear subspace of $\mathbb{C}^{2^n \times 2^n}$, it is sufficient that a generating set of error operators in this space is correctable. Of course, one most efficiently chooses error operators that are linearly independent; this motivates the definition of *error bases* below.

So far we have made no restrictions on the error operators, nor have we made any specifications of "how many"or "what type"of errors a code can correct. In this context, a key parameter of an error operator is the number of qubits it affects. To this end we define the *weight* $\mathrm{wt}(E)$ of an operator E on n qubits to be the maximal number $w \in \{0, \ldots, n\}$ such that E can be written as $\sigma_0^{\otimes n-w} \otimes E'$ up to a permutation of the k qubits, for some matrix E'. By definition, the weight of the zero operator is 0. In other words, $\mathrm{wt}(E) = w$ if and only if E acts nontrivially on exactly w copies of $\mathbb{C}^2$. One subsequently defines a code $V \subseteq \mathbb{H}_n$ to be *t-error-correcting* if all error operators of weight up to and including t are correctable by V. A linearly independent set $\mathcal{E}$ of n-qubit operators is called a *t-error basis* if every n-qubit operator of weight no greater than t is a linear combination of elements of $\mathcal{E}$. Proposition 2.19 immediately yields the following result:

Proposition 2.20 *A quantum error-correcting code $V \subseteq \mathbb{H}_n$ is t-error-correcting if and only if all operators in a t-error basis are correctable.*

For qubits, the Pauli operators $\{\sigma_v \mid v \in \mathbb{F}_2^n\}$ of course form suitable candidates to construct error bases. Letting $t \in \mathbb{N}$, the set

$$\mathcal{E}_t := \{\sigma_v \mid v \in \mathbb{F}_2^n,\ \mathrm{wt}(\sigma_v) \leq t\} \tag{2.106}$$

is indeed a basis of the linear space of all operators on $\mathbb{H}_n$ of weight no greater than t. In the context of quantum coding theory, Pauli operators $E \in \mathcal{G}_n$ are referred to as *Pauli errors*.

Remark. In section 2.4.3.3 we have defined the support of a Pauli operator M on n qubits to be the subset of those $i \in \{1, \ldots, n\}$ such that the ith tensor factor of M is not equal to the identity. Note that the weight of a Pauli operator, as defined above, is equal to the cardinality of its support. ◇

Summarizing this section, we can conclude the following:

(i) QECCs are *subspaces* of $\mathbb{H}_n$, and

(ii) the error-correcting capabilities of a QECC can be exposed by investigating the effect of *Pauli errors* on the code.

In view of these results, it comes as no surprise that the stabilizer formalism offers a general framework to construct quantum error-correcting codes. In particular, we will see that the subspaces $V_{\mathcal{S}}$, defined in section 2.3, are good candidates for error-correcting codes. These codes are called *stabilizer codes*.

2.6.2 Stabilizer codes

As we already announced, a stabilizer code is a subspace $V_{\mathcal{S}} \subseteq \mathbb{H}_n$, where $\mathcal{S}$ is a stabilizer on n qubits. If $\mathcal{S}$ has cardinality 2^{n-k} then $V_{\mathcal{S}}$ is called an $[n, k]$ code. Note that an $[n, k]$ stabilizer code has dimension 2^k from proposition 2.11.

The main motivation to consider stabilizers in the context of quantum coding theory is that the stabilizer formalism exploits the group theoretic structure of the Pauli group $\mathcal{G}_n$, thereby allowing for an elegant construction of many QECCs. We will illustrate the power of this approach in this section.

Let us first investigate which conditions a stabilizer $\mathcal{S}$ has to satisfy in order for the error-correcting conditions (2.104) to be satisfied for a set of Pauli errors $\mathcal{E} \subseteq \mathcal{G}_n$. We need an additional definition. The *normalizer* $N(\mathcal{S})$ of $\mathcal{S}$ is the set of all $M \in \mathcal{G}$ satisfying $M\mathcal{S}M^\dagger = \mathcal{S}$. Note that $\mathcal{S} \subseteq N(\mathcal{S})$ trivially. We can now state the following result:

Theorem 2.21 *Let $\mathcal{S}$ be a stabilizer on n qubits. If $E_a^\dagger E_b \notin N(\mathcal{S})\setminus\mathcal{S}$ for every E_a, E_b in a set $\mathcal{E} \subseteq \mathcal{G}_n$ of Pauli errors, then $\mathcal{E}$ is a correctable set of errors for the code $V_\mathcal{S}$.*

Proof: Let $\mathcal{S}$ be a stabilizer on n qubits such that $E_a^\dagger E_b \notin N(\mathcal{S}) \setminus \mathcal{S}$ for every E_a, $E_b \in \mathcal{E}$. We have to prove that this implies that

$$\rho_\mathcal{S} E_a^\dagger E_b \rho_\mathcal{S} = c_{ab}\rho_\mathcal{S} \tag{2.107}$$

for some $c_{ab} \in \mathbb{C}$, since then $\mathcal{E}$ is a correctable set of errors due to theorem 2.18. Fix $E_a, E_b \in \mathcal{E}$ and denote $E \equiv E_a^\dagger E_b$. Then from our assumption there are two possibilities: either $E \in \mathcal{S}$ or $E \in \mathcal{G}_n \setminus N(\mathcal{S})$. In the former case it is clear that (2.107) holds, since $E\rho_\mathcal{S} = \rho_\mathcal{S}$ and therefore $\rho_\mathcal{S} E \rho_\mathcal{S} = \rho_\mathcal{S}^2 \sim \rho_\mathcal{S}$. On the other hand, suppose that $E \in \mathcal{G}_n \setminus N(\mathcal{S})$. Then there exists an element $M_1 \in \mathcal{S}$ that anticommutes with E from the definition of $N(\mathcal{S})$. Letting $M_1, \dots, M_k$ be an independent generating set for $\mathcal{S}$, we have

$$\rho_\mathcal{S} = \frac{1}{2^n}\prod_{i=1}^{k}(I + M_i). \tag{2.108}$$

Using the anti-commutativity of E and M_1 then gives

$$E\rho_\mathcal{S} = \frac{1}{2^n}(I - M_1)E\left\{\prod_{i=2}^{k}(I + M_i)\right\} \tag{2.109}$$

and consequently $\rho_\mathcal{S} E \rho_\mathcal{S} = 0$ since $(I + M_1)(I - M_1) = 0$. This shows that (2.107) also holds in this case. $\square$

Corollary 2.22 *If $E \notin N(\mathcal{S})\setminus\mathcal{S}$ for every $E \in \mathcal{E}_{2t}$ then the code $V_\mathcal{S}$ is t-error-correcting.*

Note that the normalizer $N(\mathcal{S})$ of the stabilizer $\mathcal{S}$ is equal to the *centralizer* $C(\mathcal{S})$ of $\mathcal{S}$, which is defined as the subset of all $M \in \mathcal{G}_n$ that commute with all elements in $\mathcal{S}$. This centralizer has a very simple interpretation in the binary framework: letting S be a generator matrix of $\mathcal{S}$, then $\alpha\sigma_v \in C(\mathcal{S})$ (where $\alpha \in \{\pm 1, \pm i\}$ and $v \in \mathbb{F}_2^{2n}$) if and only if $S^T P v = 0$. The binary encoding $\mathcal{B}(C(\mathcal{S}))$ of the centralizer is therefore no more then the orthogonal complement of C_S with respect to the symplectic inner product on $\mathbb{F}_2^{2n}$.

Theorem 2.21 motivates the definition of the *distance* of a stabilizer code, which is the minimal weight of an element of $N(\mathcal{S}) \setminus \mathcal{S}$. An $[n,k]$ stabilizer code with distance d is said to be a $[n,k,d]$ code. Corollary 2.22 shows that a code with distance $d = 2t+1$ is t-error-correcting.

Example. The *5-qubit code* is the code stabilized by the 4 independent 5-qubit operators

$$\begin{aligned} M_1 &= \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes \sigma_0 \\ M_2 &= \sigma_0 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \\ M_3 &= \sigma_x \otimes \sigma_0 \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \\ M_4 &= \sigma_z \otimes \sigma_x \otimes \sigma_0 \otimes \sigma_x \otimes \sigma_z, \end{aligned} \tag{2.110}$$

which give rise to the generator matrix

$$\left[\begin{array}{ccccc|ccccc} \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & \cdot \end{array}\right]^T. \tag{2.111}$$

The stabilizer $\mathcal{S}$ generated by these operators has cardinality $2^4 = 24$ and therefore $V_\mathcal{S}$ is a $[5,1]$ stabilizer code. Note that the generators M_2, M_3, M_4 can be obtained from M_1 by a cyclic permutation of the qubits. Therefore, the 5-qubit code is called a *cyclic* code. It is not hard to convince oneself that the set $C(\mathcal{S}) \setminus \mathcal{S} = N(\mathcal{S}) \setminus \mathcal{S}$ does not contain any element of weight 1 or 2. However, the operator

$$E = \sigma_z \otimes \sigma_x \otimes \sigma_z \otimes \sigma_0 \otimes \sigma_0 \tag{2.112}$$

does not belong to $\mathcal{S}$ and commutes with all four generators M_i. Therefore, $E \in N(\mathcal{S}) \setminus \mathcal{S}$ and the distance of $V_\mathcal{S}$ is 3. Thus, the 5-qubit code is a $[5,1,3]$ code, which can correct an arbitrary single-qubit error (i.e., it is 1-error-correcting). $\diamond$

Remark. It is important to note that in this thesis we adopt a different notation from the one used in quantum coding theory. Usually, the generator matrix of a $[n,k]$ stabilizer code is a $(n-k) \times 2n$ matrix, the *rows* of which generate the $(n-k)$-dimensional binary space $\mathcal{B}(\mathcal{S})$. Therefore, if S is a generator matrix in our notation, its transpose S^T is a generator matrix in the standard quantum coding literature. $\diamond$

Theorem 2.21 elegantly characterizes when a set of Pauli errors is correctable by a stabilizer code. However, this result does not tell us how to recover the original state when an error has occurred. To understand how this error-correction is performed, let $V_\mathcal{S}$ be an $[n,k]$ stabilizer code, let $\mathcal{E} \subseteq \mathcal{G}_n$ be a correctable set of errors and let $M_1, \ldots, M_{n-k}$ be $n-k$ independent generators of $\mathcal{S}$. Suppose our n-qubit system is originally in a state $|\psi_{\rm in}\rangle \in V_{\mathcal{S}}$ and that an error $E_a \in \mathcal{E}$ occurs, transforming $|\psi_{\rm in}\rangle$ into the state $E_a|\psi_{\rm in}\rangle \equiv |\psi_{\rm out}\rangle$. Note that the assumption that a mere Pauli error has occurred is quite unrealistic, but the techniques used to correct such Pauli errors will turn out to be also adequate to correct arbitrary errors; we will outline the procedure of correcting arbitrary errors below. Now, in a first step in the process of correcting the error E_a, one wants to *detect* that an error has occurred. This error-detection is obtained by measuring the generators M_i ($i = 1, \ldots, n-k$): defining $\beta_i = \pm 1$ by $E_a M_i = \beta_i M_i E_a$ for every $i = 1, \ldots, n-k$, we observe that

$$M_i|\psi_{\rm out}\rangle = M_i E_a|\psi_{\rm in}\rangle = \beta_i E_a M_i|\psi_{\rm in}\rangle = \beta_i E_a|\psi_{\rm in}\rangle = \beta_i|\psi_{\rm out}\rangle. \tag{2.113}$$

Therefore, measurement of M_i will yield an outcome β_i. The measurement results $\{\beta_i\}$ are called the *error-syndrome*. Note that the state $|\psi_{\rm out}\rangle$ is unaffected by measurement of the M_is, since it is an eigenstate of these operators. Having obtained the error-syndrome, one fixes any operator $E_b \in \mathcal{E}$ satisfying $E_b M_i = \beta_i M_i E_b$ for every $i = 1, \ldots, n-k$. Of course, the error E_a satisfies this property, but there may be more than one error operator with this property. We now claim that $E_b^\dagger|\psi_{\rm out}\rangle = |\psi_{\rm in}\rangle$. To see this, note that E_a and E_b have the same commutation relations with the generators M_i, and therefore

$$\begin{aligned} E_a\rho_{\mathcal{S}}E_a^\dagger &= \frac{1}{2^n}E_a\left\{\prod_{i=1}^k (I+M_i)\right\}E_a^\dagger \\ &= \frac{1}{2^n}\left\{\prod_{i=1}^k (I+E_aM_iE_a^\dagger)\right\} \\ &= \frac{1}{2^n}\prod_{i=1}^k (I+\beta_iM_i) \\ &= \frac{1}{2^n}\left\{\prod_{i=1}^k (I+E_bM_iE_b^\dagger)\right\} = E_b\rho_{\mathcal{S}}E_b^\dagger. \end{aligned} \tag{2.114}$$

The identity $E_a\rho_{\mathcal{S}}E_a^\dagger = E_b\rho_{\mathcal{S}}E_b^\dagger$ implies that $E_b^\dagger E_a \in N(\mathcal{S})$. Since $\mathcal{E}$ is a correctable set of errors, we know that $E_b^\dagger E_a \notin N(\mathcal{S}) \setminus \mathcal{S}$ and we conclude that $E_b^\dagger E_a \in \mathcal{S}$. This shows that $E_b^\dagger|\psi_{\rm out}\rangle = E_b^\dagger E_a|\psi_{\rm in}\rangle = |\psi_{\rm in}\rangle$ since $|\psi_{\rm in}\rangle \in V_{\mathcal{S}}$. Therefore, we have implemented a successful recovery of the initial state $|\psi_{\rm in}\rangle$.

We do not give a proof here, but the above procedure in fact works for general errors, i.e., also errors that do not belong to the Pauli group. Summarized, the strategy is the following: suppose that an initial state $|\psi_{\rm in}\rangle \in V_{\mathcal{S}}$ is subjected to errors, transforming it into a (generally mixed) final state

$$\sum_l A_l|\psi_{\rm in}\rangle\langle\psi_{\rm in}|A_l^\dagger \equiv \rho_{\rm out}, \tag{2.115}$$

where the error operators A_l belong to a correctable set $\mathcal{A}$ of the code. First a set of generators of the stabilizer is measured, yielding $n-k$ outcomes $\beta_i = \pm 1$ ($i = 1, \ldots, n-k$) constituting the error-syndrome. This sequence of measurements will induce a collapse of the state ρ_{out}, transforming it into a state of the form $E_a|\psi_{\text{in}}\rangle$, where $E_a \in \mathcal{G}_n$ is some correctable Pauli error of the code $V_{\mathcal{S}}$. Since this state is produced after measurement of the operators M_i, it satisfies

$$M_i \left(E_a|\psi_{\text{in}}\rangle\right) = \beta_i E_a|\psi_{\text{in}}\rangle \tag{2.116}$$

for every $i = 1, \ldots, n-k$. As above, one now fixes any correctable Pauli error E_b satisfying $E_b M_i = \beta_i M_i E_b$ for every $i = 1, \ldots, n-k$. Also as above, it follows that $E_b^\dagger E_a \in \mathcal{S}$. Applying $E_b^\dagger$ to $E_a|\psi_{\text{in}}\rangle$ then completes the error-correction, yielding $E_b^\dagger E_a|\psi_{\text{in}}\rangle = |\psi_{\text{in}}\rangle$.

To conclude our discussion of quantum error-correction and stabilizer codes, we state the following remark: in later chapters we will *not* be interested in research questions within the field of quantum error-correction regarding e.g. the construction of new codes, the rates of codes or the error-correcting capabilities of stabilizer codes altogether. Therefore our encounter with such topics in this section was brief and the interested reader is referred to the relevant literature (see the references section of this chapter). In this thesis, our interest lies in the problem of recognizing *local equivalence* of two given codes, a notion that will be introduced in chapter 3.

2.7 Conclusion

In this chapter we have considered stabilizer states and graph states as our main topic of interest. We introduced these states in the context of the stabilizer formalism, we gave several examples of such states and considered two important applications, viz. the measurement-based model of quantum computation and the theory of stabilizer codes within the context of quantum-error-correction.

The main conclusion to be drawn in this chapter is the use of algebra over the field $\mathbb{F}_2$ to describe stabilizer states and codes. This description constitutes a compact and transparent means of dealing with these states. It also announces that one mainly resorts to tools from discrete mathematics, such as e.g. graph theory, finite group theory and classical coding theory, in order to deal with problems in the context of the stabilizer formalism. This will become evident in the following chapters.

References

The basic theory of the stabilizer formalism that we outlined in sections 2.2 and 2.3 can be found in numerous standard texts on QIT, such as e.g. Nielsen and Chuang [8], Preskill [33] or the PhD thesis of Gottesman [19]. In recent years many authors have considered stabilizer states and graph states and even the very basic results concerning these states are scattered throughout the literature; see e.g. [13, 23, 15, 24, 14, 29, 10, 27, 20, 52] for various aspects of stabilizer states and graph states, but this is far from an exhaustive list. We refer to Hein et al. [25] for an extensive account on graph states. The graph theoretical definitions in this chapter are taken from Ref. [12]. Section 2.5 dealing with measurement-based computation is a summary of results of the work of Raussendorf et al., see [38] and refs therein. The theory of quantum error-correction and stabilizer codes appears as a chapter in many standard QIT textbooks; the material in section 2.6 has been gathered from [8], [33], [5] and [19]. We also refer to the standard paper by Calderbank et al. on stabilizer codes and their description in terms of algebra over $\mathbb{F}_4$ [7].

We note that there also appeared some (small) new results in this chapter, namely propositions 2.12, 2.13 and the results and definitions in section 2.4.3.4 on $\mathbb{F}_4$-linear codes; theorem 2.17 was published in our work Ref. [50].

Chapter 3

Local equivalence

3.1 Introduction

In this chapter we introduce the three notions of local equivalence of stabilizer states and codes that we will study in this dissertation. These different types of local equivalence all come about by fixing certain $2^n \times 2^n$ matrix groups, and consequently calling two n-qubit stabilizer states (codes) equivalent with respect to such a matrix group if there exists an operator in this group that maps the first state to the second. We are interested in *local* transformations, which act on each of the n qubits separately; these are transformations of the form $A_1 \otimes \cdots \otimes A_n$, where the A_is are (invertible) 2×2 matrices. In particular, we will consider the following groups of local transformations:

$$SL(2,\mathbb{C})^{\otimes n}, \quad U(2)^{\otimes n} \quad \text{and} \quad \mathcal{C}_n^l = \mathcal{C}_1^{\otimes n}. \tag{3.1}$$

We elaborate on the relevance of these groups in QIT one by one.

Firstly, $SL(2,\mathbb{C})$ is the group of 2×2 determinant 1 matrices. Mapping a one-qubit state ρ to $B\rho B^\dagger$, where $B \in SL(2,\mathbb{C})$ corresponds to selecting one outcome of a POVM measurement performed on the system in the state ρ (see also section 3.2 and appendix 1). The corresponding local equivalence relation is called equivalence under stochastic local operations assisted by classical communication, or simply *SLOCC equivalence*. This is regarded as the most general local equivalence relation. Two stabilizer states $|\psi\rangle$, $|\psi'\rangle$ are called SLOCC equivalent if there exists an operator $A \in SL(2,\mathbb{C})^{\otimes n}$ such that $A|\psi\rangle \sim |\psi'\rangle$. The set SLOCC($\psi$) is the set of all stabilizer states SLOCC equivalent to $|\psi\rangle$.

Secondly, $U(2)$ is the 2×2 unitary group, defining the "standard"unitary evolution of a one-qubit system. The corresponding local equivalence is called local unitary equivalence or *LU equivalence*. Two stabilizer states $|\psi\rangle$, $|\psi'\rangle$ are called LU equivalent if there exists an operator $U \in U(2)^{\otimes n}$ such that $U|\psi\rangle = |\psi'\rangle$. The set LU($\psi$) is the set of all stabilizer states LU equivalent to $|\psi\rangle$. Note that every two LU equivalent states are also SLOCC equivalent.

Thirdly, $\mathcal{C}_1$ is the Clifford group, which is a certain finite subgroup of $U(2)$ that arises naturally when dealing with stabilizers. The Clifford group is (a quotient group of) the group of all 2×2 unitary operators that map the Pauli group $\mathcal{G}_1$ to itself under conjugation. The group $\mathcal{C}_n^l = \mathcal{C}_1^{\otimes n}$ is the called the *local Clifford group* and defines local Clifford equivalence or *LC equivalence*: two stabilizer states $|\psi\rangle$, $|\psi'\rangle$ are called LC equivalent if there exists an operator $V \in \mathcal{C}_n^l$ such that $V|\psi\rangle \sim |\psi'\rangle$. Thus, LC equivalence is a restricted version of LU equivalence. The set LC(ψ) is the set of all stabilizer states LC equivalent to $|\psi\rangle$.

The general goal of this chapter is to introduce the basic definitions and results concerning SLOCC, LU and LC equivalence of stabilizer states and codes. A detailed investigation of these local equivalences will follow in the subsequent chapters of this dissertation. This chapter is structured as follows. In section 3.2 we prove that every two SLOCC equivalent stabilizer states are necessarily LU equivalent. This shows that we can in fact restrict our attention to LU and LC equivalence. In section 3.3 we state the basics concerning LU equivalence of stabilizer states and we define the related notion of local equivalence of stabilizer codes. In section 3.4, finally, we formally define the local Clifford group and LC equivalence of stabilizer states and codes. Due to its definition, LC equivalence of stabilizer states and codes can entirely be described within the binary formalism. We develop this general binary framework of LC equivalence and, using this framework, prove the well known result that every stabilizer state is LC equivalent to a graph state. Finally, we explain the relevance of LC equivalence of stabilizer states in the context of the measurement-based quantum computer.

3.2 SLOCC equivalence equals LU equivalence

In this section we show that SLOCC(ψ) = LU(ψ) for every stabilizer state $|\psi\rangle$. Recall that two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are called SLOCC equivalent if there exists an operator $A \in SL(2,\mathbb{C})^{\otimes n}$ such that $A\rho_\psi A^\dagger \sim \rho_{\psi'}$, where the group $SL(2,\mathbb{C})$ consists of all complex 2×2 matrices with determinant equal to 1 (see also appendix 1).

A central ingredient to the proof that SLOCC(ψ) = LU(ψ) for every stabilizer state $|\psi\rangle$, is the following theorem, which (is an adapted version of a theorem that) appeared in Ref. [53].

Theorem 3.1 *Let ρ be an n-qubit density operator such that all its 1-qubit density operators are nonsingular. Then there exists an element in the SLOCC orbit of ρ, the 1-party density operators of which are all maximally mixed, i.e. they are proportional to the identity. Moreover, this element is unique up to LU equivalence and is called an SLOCC normal form of ρ.*

Proof: Let ρ be an n-qubit density operator such that all its 1-qubit density operators are nonsingular. It will be convenient to let ρ be unnormalized. The idea behind the proof of the theorem is that the local operator $A = A_1 \otimes \cdots \otimes A_n \in SL(2,\mathbb{C})^{\otimes n}$ that brings ρ into its normal form can be constructed iteratively by a procedure where at every step the trace of ρ decreases. This procedure is the following: first, consider the partial trace $\rho_1 = \mathrm{Tr}_{\{2,\ldots,n\}}\rho$. Since ρ_1 is invertible, there exists an operator $X \in SL(2,\mathbb{C})$ such that $X\rho_1 X^\dagger \sim \sigma_0$. Indeed, the matrix $X = \det(\rho_1)^{1/4}\ \rho_1^{-1/2}$ does the job, and we have

$$\rho_1' := X\rho_1 X^\dagger = \det(\rho_1)^{1/2}\ \sigma_0. \tag{3.2}$$

Denoting

$$\rho' := (X \otimes \sigma_0 \otimes \cdots \otimes \sigma_0)\rho(X \otimes \sigma_0 \otimes \cdots \otimes \sigma_0)^\dagger, \tag{3.3}$$

we also have

$$\mathrm{Tr}(\rho') = \mathrm{Tr}(\rho_1') = 2\det(\rho_1)^{1/2} \leq \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\rho). \tag{3.4}$$

Denoting the eigenvalues of ρ_1 by λ and μ, the inequality in (3.4) is equivalent to

$$2\sqrt{\lambda\mu} \leq \lambda + \mu, \tag{3.5}$$

which can readily be verified. Moreover, note that equality in (3.4) occurs if and only if $\lambda = \mu$ or, equivalently, $\rho_1 \sim \sigma_0$. Therefore, the operation $\rho \mapsto \rho'$ is trace-decreasing. We can now repeat this procedure with the other parties, and then iteratively repeat everything. After each iteration, the trace of ρ will decrease, unless all partial traces are equal to the identity. Because the trace of a density operator is bounded from below (since this is a positive operator), the decrements become arbitrarily small and following equation (3.4), this implies that all 1-qubit density operators converge to a multiple of the identity σ_0.

The proof that the normal form is unique up to LU equivalence is beyond the scope of this dissertation and we refer the interested reader to Ref. [53]. This ends the proof. □

Thus, theorem 3.1 shows that, under some weak assumptions, every multipartite state can be brought in an SLOCC normal form which is unique up to LU equivalence. The following corollary immediately follows from the proof of this theorem:

Corollary 3.2 *Two states ρ and ρ' are SLOCC equivalent if and only if they have LU equivalent normal forms.*

Proof: This immediately follows from the fact that the normal form is unique up to LU equivalence. □

We will use corollary 3.2 to show that $\mathrm{SLOCC}(\psi) = \mathrm{LU}(\psi)$ for every stabilizer state $|\psi\rangle$. We need the following lemma:

Lemma 3.3 *Let $|\psi\rangle$ be a stabilizer state on n qubits which is not a tensor product of a 1-qubit state and a state on $n-1$ qubits. Then $\rho_{\{i\}}(\psi) \sim \sigma_0$ for every $i = 1, \dots, n$.*

proof: Let $|\psi\rangle$ be a fully entangled stabilizer state on $n \geq 2$ qubits and fix $i \in \{1, \dots, n\}$. It follows from identity (2.58) in section 2.4.3.3 that

$$\text{rank } \rho_{\{i\}}(\psi) = 2|\mathcal{S}_{\{i\}}(\psi)|^{-1}, \tag{3.6}$$

where we recall that

$$\mathcal{S}_{\{i\}}(\psi) = \{M \in \mathcal{S}(\psi) \mid \text{ supp}(M) \subseteq \{i\}\}. \tag{3.7}$$

Since $\rho_{\{i\}}(\psi)$ is a 1-qubit density operator, it has rank equal to one or two. If $\rho_{\{i\}}(\psi)$ has rank one, it is the projector associated with a pure 1-qubit stabilizer state, which is impossible from the given. This shows that $\rho_{\{i\}}(\psi)$ has rank two. It then follows from (3.6) that $|\mathcal{S}_{\{i\}}(\psi)| = 1$ and therefore $\rho_{\{i\}}(\psi) \sim \sigma_0$. This ends the proof. $\square$

Corollary 3.4 *SLOCC(ψ) = $LU(\psi)$ for every stabilizer state $|\psi\rangle$.*

Proof: It is sufficient to prove the result for fully entangled stabilizer states. If $|\psi\rangle$ is a fully entangled stabilizer state, it fulfills the requirements of lemma 3.3 and therefore all its 1-qubit density operators are maximally mixed. Now let $|\psi'\rangle \in$ SLOCC(ψ). Then $|\psi'\rangle$ is also fully entangled and therefore also has maximally mixed 1-qubit density operators. It follows that both $|\psi\rangle$ and $|\psi'\rangle$ are in SLOCC normal form. As these states are SLOCC equivalent, corollary 3.2 shows that they must also be LU equivalent. This ends the proof. $\square$

We now have completed the proof that SLOCC(ψ) = LU(ψ) for every stabilizer state $|\psi\rangle$. Therefore, in our study of local equivalence of stabilizer states, we can restrict our attention to LU and LC equivalence.

3.3 LU equivalence

Having reduced the problem of recognizing SLOCC equivalence to recognizing LU equivalence of stabilizer states, in this section we turn to the latter equivalence relation an define the basic notions. We also define LU equivalence of stabilizer codes and explain its relevance in quantum coding theory.

3.3.1 Stabilizer states

Regarding LU equivalence of stabilizer states we will, at this point, be very brief, and simply recall that two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ on n qubits are called LU equivalent if there exists a local unitary operator $U \in U(2)^{\otimes n}$ relating these two states, i.e., $U|\psi\rangle = |\psi'\rangle$. We will deal with LU equivalence of stabilizer states in detail in the following chapters.

3.3.2 Stabilizer codes

In quantum coding theory one defines two natural equivalence relations on the set of stabilizer codes. Formally, two n-qubit stabilizer codes $V_{\mathcal{S}}$ and $V_{\mathcal{S}'}$ are called *globally equivalent*, or simply *equivalent*, if $V_{\mathcal{S}'}$ can be obtained from $V_{\mathcal{S}}$ by applying a local unitary operation $U \in U(2)^{\otimes n}$ and a permutation of the n qubits. If $UV_{\mathcal{S}} = V_{\mathcal{S}'}$, without any additional permutation, then the codes are called *locally equivalent*. The motivations behind these definitions are the following. We have seen in section 2.6 that a stabilizer code is a subspace of an n-qubit Hilbert space $\mathbb{H}_n$. Moreover, all notions concerning the correction of errors are formulated with respect to the structure of this Hilbert space as consisting of n 1-qubit subsystems; indeed, the definitions of weight, distance, the notion of a t-error-correcting code etc. quantify the performance of a code in terms of the *number of qubits* it can protect. Therefore, any sensible "equivalence"of quantum error correcting codes should preserve the above structure. In view of these considerations, it is clear that a relabelling – or, equivalently, a permutation – of the n qubits cannot yield a fundamentally different stabilizer code, nor can a different choice of basis within the ith 1-qubit Hilbert space

$$\{|0\rangle, |1\rangle\}_i \quad \rightarrow \quad \{|\bar{0}\rangle \equiv U_i|0\rangle,\ |\bar{1}\rangle \equiv U_i|1\rangle\}_i\,, \tag{3.8}$$

where $U_i \in U(2)$, for every $i = 1, \ldots, n$. The natural definition of (global) equivalence of quantum codes is then obtained by combining the above two operations.

Note that two n-qubit stabilizer codes $V_{\mathcal{S}}$ and $V_{\mathcal{S}'}$ are locally equivalent if and only if $U\rho_{\mathcal{S}}U^\dagger = \rho_{\mathcal{S}'}$ for some $U \in U(2)^{\otimes n}$. Therefore, local equivalence of stabilizer codes corresponds to LU equivalence of the states $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ and is a natural extension of the definition of LU equivalence of stabilizer states. Although global equivalence is the true equivalence of stabilizer codes, the structure of local equivalence is simpler, and a lot of insight can be gained by studying local equivalence. Hence most authors tackle local equivalence, and we will do the same in this dissertation.

In the following, we will see that the majority of the results and proofs concerning LU equivalence that hold for stabilizer states, also hold for general stabilizer codes.

3.4 LC equivalence

In this section we consider a restricted version of LU equivalence, called *LC equivalence*. This local equivalence relation is obtained by only allowing local unitary operators belonging to a certain finite subgroup of $U(2)^{\otimes n}$, namely the local Clifford group. As we will see, local Clifford operations arise naturally in the context of the stabilizer formalism. Moreover, the action of local Clifford operations on stabilizer states and codes can elegantly be described within the binary description of the stabilizer formalism, which makes this group very manageable in this context. LC equivalence of stabilizer states plays an important role in the study of the entanglement properties and the coding theoretic aspect of stabilizer states, and in the development in the one-way quantum computer.

In the following we will first formally define the local Clifford group and LC equivalence. Secondly, we give a translation of LC equivalence of stabilizer states and codes in the binary stabilizer picture. We also show that every stabilizer state is LC equivalent to a graph state, thereby reducing the study of LC equivalence of stabilizer states to that of graph states. Finally, we elaborate on the relevance of LC equivalence of stabilizer states in the context of the one-way quantum computer.

3.4.1 Local Clifford group

The *Clifford group* $\mathcal{C}_1$ *on one qubit* is the subgroup of $U(2)$ generated by the matrices

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{3.9}$$

In quantum information terminology, the matrix H is called the Hadamard gate and P is called the phase gate. One can show (see e.g. [35]) that $\mathcal{C}_1$ consists of the following 192 matrices:

$$\eta^d \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & \alpha \\ \beta & -\alpha\beta \end{bmatrix}, \quad \eta^d \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix}, \quad \eta^d \begin{bmatrix} 0 & 1 \\ \alpha & 0 \end{bmatrix}, \tag{3.10}$$

where $\eta = (1+i)/\sqrt{2}$ (an 8th root of unity), $d \in \{0, \dots, 7\}$ and $\alpha, \beta \in \{\pm 1, \pm i\}$. Note that, in particular, $\mathcal{G}_1 \subseteq \mathcal{C}_1$. A key property of the Clifford group is the following:

Proposition 3.5 *Every $U \in \mathcal{C}_1$ maps the Pauli group $\mathcal{G}_1$ to itself under conjugation, i.e., $U\sigma U^\dagger \in \mathcal{G}_1$ for every $\sigma \in \mathcal{G}_1$.*

Proof: It is straightforward to verify that $H\sigma H^\dagger$ and $P\sigma P^\dagger$ belong to $\mathcal{G}_1$ for every $\sigma \in \mathcal{G}_1$. The result follows by noting that H and P generate the group $\mathcal{C}_1$. This ends the proof. □

The converse of proposition 3.5 is also true:

Proposition 3.6 *Let $U \in U(2)$ map the Pauli group $\mathcal{G}_1$ to itself under conjugation. Then there exists $\gamma \in \mathbb{C}$, $|\gamma| = 1$, such that $\gamma U \in \mathcal{C}_1$*

Proof: Since $U\mathcal{G}_1 U^\dagger = \mathcal{G}_1$, there exist phases $\alpha_x, \alpha_y, \alpha_z \in \{\pm 1, \pm i\}$ and a permutation π of the set $\{x, y, z\}$ such that

$$U\sigma_a U^\dagger = \alpha_a \sigma_{\pi(a)}, \tag{3.11}$$

for every $a \in \{x, y, z\}$. Moreover, these phases must be real, since $U\sigma_a U^\dagger$ is Hermitian and therefore $\alpha_a \sigma_{\pi(a)}$ must be Hermitian as well. This shows that $\alpha_x, \alpha_y, \alpha_z = \pm 1$. Also, knowledge of two of the phases, say α_x and α_z, fix the remaining one, since $\sigma_x \sigma_z \sim \sigma_y$. It is now straightforward to show (by a exhaustive distinction of cases) that one can always find a Clifford operation $V \in \mathcal{C}_1$ such that $V\sigma_a V^\dagger = \alpha_a \sigma_{\pi(a)}$, for every $a \in \{x, y, z\}$. As every 2×2 unitary operator is, up to a global phase factor, completely defined by its action on the Pauli matrices, it follows that U and V are equal up to a global phase factor. This ends the proof. □

Using group theory terminology, the *normalizer* $N(\mathcal{G}_1)$ of $\mathcal{G}_1$ in the unitary group $U(2)$ is defined by

$$N(\mathcal{G}_1) = \{U \in U(2) \mid U\mathcal{G}_1 U^\dagger = \mathcal{G}_1\}. \tag{3.12}$$

It follows from the above that

$$N(\mathcal{G}_1) = \{\gamma V \mid \gamma \in \mathbb{C},\ |\gamma| = 1,\ V \in \mathcal{C}_1\}. \tag{3.13}$$

Therefore, up to the overall phase factors γ, the Clifford group is simply the normalizer of $\mathcal{G}_1$ in $U(2)$.

We have shown that any Clifford operation on one qubit is, up to an overall phase factor, defined by a permutation π of $\{x, y, z\}$ and a couple of phases α_x and α_z. In the binary description (2.3), where Pauli matrices are described by pairs of bits, the permutation π in (3.11) corresponds to an invertible linear transformation Q of $\mathbb{F}_2^2$, yielding

$$U\sigma_u U^\dagger = \alpha_u \sigma_{Qu}, \tag{3.14}$$

for every $u \in \mathbb{F}_2^2 \setminus \{(0, 0)\}$, where $Q \in GL(2, \mathbb{F}_2)$. To see this, simply note that any permutation of the set $\{(1, 0), (0, 1), (1, 1)\}$ is an invertible linear transformation (and vice versa, trivially).

Example. The Hadamard gate H acts on the Pauli matrices as follows:

$$\begin{aligned} H\sigma_x H^\dagger &= \sigma_z \\ H\sigma_z H^\dagger &= \sigma_x \\ H\sigma_y H^\dagger &= -\sigma_y. \end{aligned} \tag{3.15}$$

Equivalently, we have $H\sigma_a H^\dagger = \alpha_a \sigma_{\pi(a)}$, for every $a = x, y, z$, where

$$\alpha_x = \alpha_z = -\alpha_y = 1, \tag{3.16}$$

and π permutes x and z and fixes y. Also, $H\sigma_u H^\dagger = \alpha_u \sigma_{Qu}$, for every $u \in \mathbb{F}_2^2 \setminus \{(0, 0)\}$, where $\alpha_{01} = \alpha_{10} = -\alpha_{11} = 1$ and

$$Q = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{3.17}$$

◇

Having introduced the Clifford group on one qubit, we now consider the local Clifford group. The *local Clifford group* $\mathcal{C}_n^l$ *on* n *qubits* is the n-fold tensor product of $\mathcal{C}_1$ with itself, i.e.

$$\begin{aligned} \mathcal{C}_n^l &= \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_1 \quad (n \text{ times}) \\ &= \{U_1 \otimes \cdots \otimes U_n \mid U_i \in \mathcal{C}_1, \text{ for every } i = 1, \dots, n\}. \end{aligned} \tag{3.18}$$

Analogous to the case of one qubit, the group $\mathcal{C}_n^l$ can be most easily described by its action on the Pauli group $\mathcal{G}_n$ on n qubits. Analogous to the single qubit case, we have the following:

Proposition 3.7 *The normalizer* $N(\mathcal{G}_n)$ *of the Pauli group* $\mathcal{G}_n$ *in the local unitary group* $U(2)^{\otimes n}$ *is equal to*

$$N(\mathcal{G}_n) = \{\gamma V \mid \gamma \in \mathbb{C},\ |\gamma| = 1,\ V \in \mathcal{C}_n^l\}. \tag{3.19}$$

Also analogous to the one qubit case, n-qubit local Clifford operations can be described in terms of linear operations over $\mathbb{F}_2$. We have the following result:

Proposition 3.8 *Every* $U \in \mathcal{C}_n^l$ *defines an invertible matrix* $Q \in GL(2n, \mathbb{F}_2)$ *of the block form*

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{3.20}$$

where the $n \times n$ *blocks* A, B, C, D *are diagonal, and a set of* $2n$ *phases* $\alpha_i = \pm 1$, *through the identities*

$$U \sigma_{e_i} U^\dagger = \alpha_i \sigma_{Q_i}, \tag{3.21}$$

where e_i *is the ith canonical basis vector in* $\mathbb{F}_2^{2n}$ *and* Q_i *is the ith column of* Q, *for every* $i = 1, \dots, 2n$. *Conversely, every such matrix* Q *and a set of* $2n$ *phases* $\{\alpha_i\}$ *define a unique local Clifford operation* U *up to a global phase through (3.21).*

Proof: The first part of the theorem is trivial, except for the block form of Q. Let $U \in \mathcal{C}_n^l$ and let $\{\alpha_i\}$ and $Q \in GL(n, \mathbb{F}_2)$ be such that (3.21) holds. Note that the Pauli operator σ_{e_i} acts nontrivially on exactly one qubit system (the one labelled i), since

$$\sigma_{e_i} = \begin{cases} \sigma_z^{(i)} & \text{if } i \in \{1, \dots, n\} \\ \sigma_x^{(i-n)} & \text{if } i \in \{n+1, \dots, 2n\}. \end{cases} \tag{3.22}$$

As U is a local Clifford operation, $U\sigma_{e_i}U^\dagger = \alpha_i \sigma_{Q_i}$ also acts nontrivially on the ith qubit system only, such that $(Q_i)_j = 0$ for every $j \in \{1, \dots, 2n\} \setminus \{i, i \pm n\}$.

Assembling the vectors Q_i as the columns of the matrix Q yields the desired block form (3.20).

To prove the second part of the proposition, consider a matrix $Q \in GL(n, \mathbb{F}_2)$ of the block form (3.20) and a set of phases $\{\alpha_i\}$. We will show that there exists a local Clifford operator U such that (3.21) holds and that U is uniquely defined up to a global phase. Denoting the ith diagonal entry of A, B, C, D by a_i, b_i, c_i, d_i, respectively, the submatrix

$$\begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \in GL(2, \mathbb{F}_2), \tag{3.23}$$

together with the couple of phases (α_i, α_{i+n}), defines (up to a global phase) a unique 1-qubit Clifford operator $U_i \in \mathcal{C}_1$ from proposition 3.6, for every $i = 1, \ldots, n$. It is now easy to verify that

$$U = U_1 \otimes \cdots \otimes U_n \in \mathcal{C}_n^l \tag{3.24}$$

satisfies (3.21). This ends the proof. □

Corollary 3.9 *Let $U \in \mathcal{C}_n^l$ and let the matrix Q be defined as in proposition 3.8. Then $U\sigma_v U^\dagger \sim \sigma_{Qv}$ for every $v \in \mathbb{F}_2^{2n}$.*

Proof: Every σ_v is equal to a product of σ_{e_i}s up to a global phase factor $\alpha \in \{\pm 1, \pm i\}$, i.e. $\sigma_v \sim \prod_{i\in\omega} \sigma_{e_i}$ for some set $\omega \subseteq \{1, \ldots, 2n\}$. In fact, one can easily verify that ω is exactly the set

$$\omega = \{i \in \{1, \ldots, 2n\} \mid v_i = 1\}. \tag{3.25}$$

Consequently, we have

$$U\sigma_v U^\dagger \sim \prod_{i\in\omega} U\sigma_{e_i} U^\dagger \sim \prod_{i\in\omega} \sigma_{Q_i} \sim \sigma_{(\sum_{i\in\omega} Q_i)} = \sigma_{Qv}. \tag{3.26}$$

This ends the proof. □

Corollary 3.9 shows that the action of a local Clifford operation U on a Pauli operator σ_v is translated into the binary formalism as a linear action of the corresponding matrix Q on the vector v. Note that the set of nonsingular matrices Q of the block form (3.20) is a subgroup of $GL(2n, \mathbb{F}_2)$. Needless to say that this subgroup will play a crucial role in many of our calculations on LC equivalence. Because of its connection with the local Clifford group $\mathcal{C}_n^l$, we denote this group by C_n^l.

Due to its special structure, the group C_n^l has a number of characterizations, stated in the following lemma.

Lemma 3.10 *Let $Q \in \mathbb{F}^{2n\times 2n}$ be a (not necessarily invertible) matrix of the block form*

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{3.27}$$

where the $n \times n$ blocks A, B, C, D are diagonal. Denote the ith diagonal entry of A, B, C, D by a_i, b_i, c_i, d_i, respectively, for every $i = 1, \ldots, n$. Then the following statements are equivalent:

(i) $Q \in C_n^l$;

(ii) $Q^T P Q = P$;

(iii) $a_i d_i + b_i c_i = \det \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} = 1$, *for every* $i = 1, \ldots, n$,

where P is the $2n \times 2n$ matrix defining the symplectic inner product on $\mathbb{F}_2^{2n}$, as before.

Verification of the lemma is trivial. Statement (ii) is interesting, as it implies that any $Q \in C_n^l$ preserves the symplectic inner product defined by the matrix P and is therefore a *symplectic transformation*. This is a reflection of the fact that the corresponding local Clifford operation U preserves the commutation relations of Pauli operators. Recall that two Pauli operators σ_v, $\sigma_w \in \mathcal{G}_n$ commute if and only if $v^T P w = 0$; moreover, these operators commute if and only if $U \sigma_v U^\dagger$ and $U \sigma_w U^\dagger$ do, which is in turn equivalent to $v^T Q^T P Q w = 0$ using corollary 3.9 and lemma 2.1(ii). Therefore, $v^T Q^T P Q w = v^T P w$ for every $v, w \in \mathbb{F}_2^{2n}$ and thus indeed $Q^T P Q = P$.

This concludes our study of the basic properties of the local Clifford group. In the next sections, we move to LC equivalence of stabilizer states and codes.

3.4.2 Stabilizer states

In this section we describe the basic notions of LC equivalence of stabilizer states. Recall that two stabilizer states $|\psi\rangle$, $|\psi'\rangle$ on n qubits are called LC equivalent if there exists an operator $V \in \mathcal{C}_n^l$ such that $V|\psi\rangle$ is equal to $|\psi'\rangle$ modulo an overall phase factor. Equivalently, one has $V \rho_\psi V^\dagger = \rho_{\psi'}$. The set of all stabilizer states that are LC equivalent to a given stabilizer state $|\psi\rangle$ will be denoted by LC(ψ).

3.4.2.1 Binary algebra

We have seen in the previous section that a local Clifford operation can be described elegantly in terms of a binary linear operation $Q \in C_n^l$ and a tuple of $2n$ phases. We will use this characterization of the local Clifford group to give a complete translation of LC equivalence of stabilizer states in the binary framework. Note that local Clifford operations map stabilizer states to stabilizer states. Indeed, if $|\psi\rangle$ is a stabilizer state and $V \in \mathcal{C}_n^l$, then $V|\psi\rangle$ is a stabilizer state with stabilizer equal to $V\mathcal{S}(\psi)V^\dagger$. Consequently, two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are LC equivalent if and only if $V\mathcal{S}(\psi)V^\dagger = \mathcal{S}(\psi')$ for some $V \in \mathcal{C}_n^l$.

First we state the following characterization of LC equivalence of stabilizer states in the binary stabilizer representation:

Proposition 3.11 *Let $|\psi\rangle$, $|\psi'\rangle$ be two stabilizer states on n qubits with generator matrices S, S', respectively. Then the following statements are equivalent:*

(i) $|\psi\rangle$ *and* $|\psi'\rangle$ *are LC equivalent;*

(ii) $QC_S = C_{S'}$ *for some* $Q \in C_n^l$*;*

(iii) $S'^T PQS = 0$ *for some* $Q \in C_n^l$*;*

(iv) $QSR = S'$ *for some* $Q \in C_n^l$ *and* $R \in GL(n, \mathbb{F}_2)$*.*

Proof: First we prove the implication (i) $\Rightarrow$ (ii). Suppose that $|\psi\rangle$ and $|\psi'\rangle$ are LC equivalent. Then $V\mathcal{S}(\psi)V^\dagger = \mathcal{S}(\psi')$ for some $V \in \mathcal{C}_n^l$. Using corollary 3.9, we then find that the spaces QC_S and $C_{S'}$ coincide. To prove (ii) $\Rightarrow$ (i), let $|\psi\rangle$, $|\psi'\rangle$ be two stabilizer states on n qubits with generator matrices S, S', respectively, such that $QC_S = C_{S'}$ for some $Q \in C_n^l$. Let $V \in \mathcal{C}_n^l$ be any local Clifford operation such that its corresponding operator in C_n^l equals Q. Then $|\psi''\rangle := V|\psi\rangle$ is a stabilizer state with $C(\mathcal{S}(\psi'')) = QC_S$. Since $QC_S = C_{S'}$, this shows that $C(\mathcal{S}(\psi'')) = C(\mathcal{S}(\psi'))$. But then there exists an $M \in \mathcal{G}_n$ such that $M\mathcal{S}(\psi'')M^\dagger = \mathcal{S}(\psi')$ from corollary 2.10. This shows that

$$MV\mathcal{S}(\psi)V^\dagger M^\dagger = M\mathcal{S}(\psi'')M^\dagger = \mathcal{S}(\psi'). \tag{3.28}$$

The result follows by noting that $MV \in \mathcal{C}_n^l$. To show (ii) $\Rightarrow$ (iv), note that (iv) expresses that the columns of the matrix QS generate the same vector space as the columns of the matrix S'. This is equivalent to (ii). The implication (iv) $\Rightarrow$ (iii) is trivial. Finally, we prove (iii) $\Rightarrow$ (ii). If $S'^T PQS = 0$ for some $Q \in C_n^l$ then every column $\tilde{S}_i$ of the matrix QS satisfies $S'^T P\tilde{S}_i = 0$, such that $\tilde{S}_i \in C_{S'}$ for every $i = 1, \ldots, n$. Therefore, the column space of QS is a subspace of $C_{S'}$. But the matrix QS has rank n and we conclude that $C_{QS} = QC_S = C_{S'}$. This completes the proof. $\square$

We have the following immediate corollary:

Corollary 3.12 *Let $|\psi\rangle$, $|\psi'\rangle$ be stabilizer states on n qubits with generator matrices S, S', respectively, such that $C_S = C_{S'}$. Then $|\psi\rangle$ and $|\psi'\rangle$ are LC equivalent.*

Note that this was already clear from corollary 2.10. Corollary 3.12 shows that all the information concerning the local equivalence class is contained in the generator matrix of a stabilizer state. In other words, the phases of the stabilizer elements of a stabilizer state do not play a role in determining its LC (or LU, SLOCC) equivalence class.

Proposition 3.11 shows that LC equivalence of stabilizer states can be described in a number of quite distinct ways. Indeed, in (iv) LC equivalence is stated as a type if equivalence transformation $S \mapsto QSR$ on the set of generator matrices S, whereas (iii) shows that LC equivalence of two states can be detected by solving the system of linear equations

$$S^{'T} P \begin{bmatrix} A & B \\ C & D \end{bmatrix} S = 0, \tag{3.29}$$

where A, B, C, D are diagonal $n \times n$ matrices, subject to the quadratic constraints

$$AD + BC = I. \tag{3.30}$$

Different descriptions of LC equivalence will be used according to the context at hand. E.g., the system of equations (iii) will be used in chapter 4 to construct an efficient algorithm to detect LC equivalence of two given stabilizer states, and we will employ the characterization (iv) to show that every stabilizer state is LC equivalent to a graph state. This last property will be proven in the next section.

3.4.2.2 Reduction to graph states

In this section we show that, under the transformations $S \to QSR$, each generator matrix S can be brought into a (nonunique) standard form which corresponds to the generator matrix of a graph state, i.e., a generator matrix of the form $[\theta\ I]^T$, where $\theta \in \Theta_n$ is the adjacency matrix of a simple graph on n vertices. First we need two lemmas:

Lemma 3.13 *Let $\theta \in \Theta_n$. For every diagonal $\Lambda \in \mathbb{F}_2^{n\times n}$, there exists an operation $Q \in C_n^l$ such that*

$$Q \begin{bmatrix} \theta + \Lambda \\ I \end{bmatrix} = \begin{bmatrix} \theta \\ I \end{bmatrix} \tag{3.31}$$

Proof: The operation

$$Q = \begin{bmatrix} I & \Lambda \\ 0 & I \end{bmatrix} \tag{3.32}$$

does the job. Note that $Q \in C_n^l$ since $I \cdot I + \Lambda \cdot 0 = I$. This ends the proof. □

Lemma 3.14 *Let $S \in \mathbb{F}_2^{2n\times n}$ be a matrix satisfying $S^T P S = 0$. Denote $S = [S_z^T \mid S_x^T]^T$, where S_z and S_x are $n \times n$ blocks. If S_x is nonsingular then there exists matrices $R \in GL(n, \mathbb{F}_2)$, $\theta \in \Theta_n$ and a diagonal matrix $\Lambda \in \mathbb{F}_2^{n\times n}$ such that*

$$SR = \begin{bmatrix} \theta + \Lambda \\ I \end{bmatrix}. \tag{3.33}$$

Proof: The matrix $S(S_x)^{-1}$ is equal to $[\phi^T \ I]^T$, where $\phi = S_z S_x^{-1}$. Moreover, it follows from

$$0 = S^T P S = (S_x)^{-T} S^T P S (S_x)^{-1} = \begin{bmatrix} \phi^T & I \end{bmatrix} P \begin{bmatrix} \phi \\ I \end{bmatrix} \tag{3.34}$$

that $\phi^T = \phi$. This ends the proof. □

We are now ready to state the following theorem:

Theorem 3.15 *Let $S \in \mathbb{F}_2^{2n\times n}$ be a full rank matrix satisfying $S^T P S = 0$. Then there exist matrices $Q \in C_n^l$, $R \in GL(n, \mathbb{F}_2)$ and $\theta \in \Theta_n$ such that*

$$QSR = \begin{bmatrix} \theta \\ I \end{bmatrix}. \tag{3.35}$$

Proof: Let $S \in \mathbb{F}_2^{2n\times n}$ be a matrix satisfying $S^T P S = 0$ and denote $S = [S_z^T \mid S_x^T]^T$, where S_z and S_x are $n \times n$ blocks. Using lemmas 3.13 and 3.14, it is sufficient to prove the existence of an operation $Q \in C_n^l$ such that $QS = [S_z'^T \mid S_x'^T]^T$ has a nonsingular lower block S_x'. We start by performing a basis change in C_S in order to bring S in the form

$$S \to \begin{bmatrix} R_z & S_z \\ R_x & 0 \end{bmatrix},$$

such that R_x is a full rank $n\times k$-matrix, where $k = \operatorname{rank}_{\mathbb{F}_2} S_x$; the blocks R_z, S_z have dimensions $n \times k$, $n \times (n-k)$, respectively. The symplectic self-duality of C_S implies that $S_z^T R_x = 0$. Furthermore, since S_z has full rank, it follows that the column space of S_z and the column space of R_x are each other's orthogonal complement (w.r.t. the standard inner product on $\mathbb{F}_2^n$).

As R_x has rank k, it has an invertible $k \times k$-submatrix. Without loss of generality, we assume that the matrix consisting of the first k rows of R_x is invertible, i.e.

$$R_x = \begin{bmatrix} R_x^1 \\ R_x^2 \end{bmatrix}, \tag{3.36}$$

where the upper $k\times k$-block R_x^1 is invertible and R_x^2 has dimensions $(n-k)\times k$. Partitioning S_z similarly in a $k\times(n-k)$-block S_z^1 and a $(n-k)\times(n-k)$-block S_z^2 , i.e. $S_z = [(S_z^1)^T \ (S_z^2)^T]^T$, the property $S_z^T R_x = 0$ then implies that S_z^2 is also invertible: for, suppose that there exist $x \in \mathbb{F}_2^{n-k}$ such that $(S_z^2)^T x = 0$; then the n-dimensional vector $v := (0, \ldots, 0, x)$ satisfies $S_z^T v = 0$ and therefore $v = R_x y$ for some $y \in \mathbb{F}_2^k$. This last equation reads

$$\begin{bmatrix} 0 \\ x \end{bmatrix} = \begin{bmatrix} R_x^1 \\ R_x^2 \end{bmatrix} y = \begin{bmatrix} R_x^1 y \\ R_x^2 y \end{bmatrix}.$$

Since R_x^1 is by construction invertible, $R_x^1 y = 0$ implies that $y = 0$, yielding $x = R_x^2 y = 0$. This proves the invertibility of S_z^2.

In a final step, we perform the transformation

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3.37}$$

on the qubits $k+1, \ldots, n$, i.e., we apply

$$\left[\begin{array}{cc|cc} I_k & & 0_k & \\ & 0_{n-k} & & I_{n-k} \\ \hline 0_k & & I_k & \\ & I_{n-k} & & 0_{n-k} \end{array}\right] \in C_n^l, \tag{3.38}$$

Where I_N, 0_N are the $N \times N$ identity and zero matrix, respectively, for $N \in \{k, n-k\}$. It is now easy to verify that this operation indeed yields an invertible lower $n \times n$-block in the resulting generator matrix. This ends the proof. □

Corollary 3.16 *Every stabilizer state is LC equivalent to a graph state.*

Proof: This immediately follows from the above theorem and proposition 3.11. □

Example. A stabilizer state with generator matrix S

$$S^T = \left[\begin{array}{cccc|cccc} 1 & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 \\ \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 \\ \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 \end{array}\right]^T, \tag{3.39}$$

is LC equivalent to the graph state defined by the adjacency matrix

$$\theta = \begin{bmatrix} \cdot & 1 & \cdot & 1 \\ 1 & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & 1 \\ 1 & \cdot & 1 & \cdot \end{bmatrix}. \tag{3.40}$$

Indeed, defining

$$Q = \left[\begin{array}{cccc|cccc} \cdot & & & & 1 & & & \\ & \cdot & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \\ \hline 1 & & & & \cdot & & & \\ & 1 & & & & 1 & & \\ & & \cdot & & & & 1 & \\ & & & 1 & & & & \cdot \end{array}\right], \quad R = \begin{bmatrix} \cdot & 1 & 1 & 1 \\ 1 & 1 & \cdot & \cdot \\ \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & 1 & 1 \end{bmatrix} \tag{3.41}$$

one can verify that $QSR^{-1} = [\theta \ I]^T$. □

Example. Similarly, it can be shown that the GHZ state $|GHZ_n\rangle$ is LC equivalent to the graph states $|SG_n\rangle$ and $|K_n\rangle$, where SG_n is the star graph and K_n is the complete graph (see Fig. 2.1). $\diamond$

The above result shows that in an investigation of LC equivalence of stabilizer states, it is no fundamental restriction to consider only graph states. We will dedicate an the whole of chapter 4 to the study of LC equivalence of graph states.

3.4.2.3 LC equivalence of graph states and the one-way QC

In this section we motivate the study of LC equivalence of graph states in the context of the measurement-based model of quantum computation. We first recall three facts regarding the $QC_{\mathcal{C}}$ model:

(i) a $QC_{\mathcal{C}}$ computation consists of a number of measurement rounds performed on a cluster state, which is regarded as a universal resource of quantum computation;

(ii) the first measurement round of a $QC_{\mathcal{C}}$ computation is a Clifford computation, consisting of a sequence of single-qubit Pauli measurements; after this measurement round, the cluster state has been transformed into a different stabilizer state $|\psi_0\rangle$ (on a smaller number of qubits); note that this state is LC equivalent to a graph state $|G_0\rangle$ from corollary 3.16;

(iii) a Clifford computation can efficiently be simulated on a classical computer.

Starting from the observations (i) and (ii), it is remarked in Ref. [38] that one can also model a $QC_{\mathcal{C}}$ computation as follows: rather than starting with a cluster state and then performing a series of measurement rounds consisting of a Clifford part and a non-Clifford part, one immediately specifies the graph state $|G_0\rangle$, which encodes the entire Clifford part of the computation; on this graph state one subsequently performs measurement rounds where only non-Pauli measurements are implemented. In this picture, the graph state $|G_0\rangle$ plays the role of an *algorithmic-specific resource* (as opposed to the cluster state, which is a universal resource). Note that in the original scheme measurements were performed on the stabilizer state $|\psi_0\rangle$ rather then on the LC equivalent graph state $|G_0\rangle$. Therefore, the one-qubit measurement bases of the first non-Clifford round have to be adjusted appropriately. To be more precise, take $U = U_1 \otimes \cdots \otimes U_n \in \mathcal{C}_n^l$ such that $U|\psi_0\rangle = |G_0\rangle$ and suppose that in the second measurement round the ith qubit was originally to be measured in some basis $\{|\alpha_i\rangle, |\beta_i\rangle\}$. In the modified scheme, where measurements are performed on $|G_0\rangle$ instead of $|\psi_0\rangle$, one simply measures the ith qubit in the basis $\{U_i^\dagger|\alpha_i\rangle, U_i^\dagger|\beta_i\rangle\}$ in order to obtain the same result.

Hence, in this alternative view, a $QC_{\mathcal{C}}$ computation is specified by on the one hand a graph G_0, comprising the Clifford part of the computation, and on the other hand a series of non-Pauli measurement rounds. The merit of this presentation is that it clearly separates the Clifford and non-Clifford parts of a $QC_{\mathcal{C}}$ computation.

It is now clear where LC equivalence of graph states enters the $QC_{\mathcal{C}}$ model. It follows from the above that the representation of a Clifford computation by a graph is non-unique; any graph state LC equivalent to $|\psi_0\rangle$, and hence also LC equivalent to $|G_0\rangle$, can be used to encode the corresponding Clifford computation. Therefore, in the framework of the one-way quantum computer, LC equivalent graph states correspond to the same Clifford computation.

3.4.3 Stabilizer codes

The notion of LC equivalence of stabilizer states can be extended naturally to stabilizer codes. We call two stabilizer codes $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ LC equivalent if there exists a local clifford operation $U \in \mathcal{C}_n^l$ such that $U\rho_{\mathcal{S}}U^\dagger = \rho_{\mathcal{S}'}$. It is clear that LC equivalence of stabilizer codes is a restrictive form of general local equivalence of stabilizer codes, which we described in section 3.3.2.

The following is a straightforward analogue of proposition 3.11:

Proposition 3.17 *Let $\rho_{\mathcal{S}}$, $\rho_{\mathcal{S}'}$ be two $[n, k]$ stabilizer codes with generator matrices S, S', respectively. Then the following statements are equivalent:*

(i') $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ are LC equivalent;

(ii') $QC_S = C_{S'}$ for some $Q \in C_n^l$;

(iv') $QSR = S'$ for some $Q \in C_n^l$ and $R \in GL(n-k, \mathbb{F}_2)$.

Proof: The proof is analogous to the proof of proposition 3.11. □

Remark. Proposition 3.11 (iii) has no counterpart in proposition 3.17. This is because arbitrary stabilizer codes C_S are not necessarily their own duals w.r.t. the symplectic inner product. ◇

We note that LC equivalence of stabilizer codes has a natural interpretation in terms of equivalence of classical codes. If $\rho_{\mathcal{S}}$ is a stabilizer code on n qubits with generator matrix S, the space C_S can be regarded as a classical linear code over the alphabet $\mathbb{F}_2^2$. Such codes are called codes over the Klein four group (see also Ref. [26]). The Klein four group K has four elements $0, x, y, z$ satisfying $x + y + z = 0$ and

$$x + x = y + y = z + z = 0. \tag{3.42}$$

One can easily see that K is isomorphic to $\mathbb{F}_2^2$, where the latter is regarded as an additive group. Therefore, a subspace $C_S \subseteq \mathbb{F}_2^{2n}$ can indeed be regarded as a subspace of $K^n = K \times \cdots \times K$. The classical notion of local equivalence of such codes is the following: two codes $C,\ C' \subseteq K^n$ are called locally[1] equivalent if there exist n permutations π_i of $\{0, x, y, z\}$ with $\pi_i(0) = 0$, such that

$$(\pi_1(v_1), \ldots, \pi_n(v_n)) \in C' \text{ if and only if } (v_1, \ldots, v_n) \in C. \tag{3.43}$$

The above component-wise permutations of x, y and z exactly correspond to performing an operation $Q \in C_n^l$ in the binary picture. Indeed, writing Q as

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{3.44}$$

where the $n \times n$ blocks A, B, C, D are diagonal, the 2×2 blocks

$$\begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \tag{3.45}$$

correspond to the permutations π_i, for every $i = 1, \ldots, n$ (where a_i, b_i, c_i, d_i is the ith diagonal entry of A, B, C, D, respectively). We have proven:

Proposition 3.18 *Let ρ_S, $\rho_{S'}$ be two stabilizer codes on n qubits with generator matrices S, S', respectively. Then ρ_S and $\rho_{S'}$ are LC equivalent if and only if the spaces C_S and $C_{S'}$ are locally equivalent as classical codes over the Klein four group.*

In a final remark, we point out that also theorem 3.15 and corollary 3.16 have analogues for stabilizer codes. One defines a *graph code*, which is the analogue of a graph state, as a stabilizer code having a $2n \times (n - k)$ generator matrix $S = [S_z^T\ S_x^T]^T$ such that the $n \times (n - k)$ block S_x has full rank (over GF(2), as always). A completely analogous proof to that of theorem 3.15 then yields the following:

Proposition 3.19 *Every stabilizer code is LC equivalent to a graph code.*

This proposition is a special case of a result [40], where it was shown, in a more general context of d-level systems rather then qubits, that each stabilizer code is equivalent to a graph code. This result was also proven in Ref. [21]. We are very brief on the topic of such graph codes, as we will not encounter them again in this dissertation. This concludes our first basic discussion of LC equivalence of stabilizer states and codes.

3.5 Conclusion

In this chapter we have introduced SLOCC, LU and LC equivalence of stabilizer states and codes. It was our aim to state the relevant definitions and to prove

[1] The codes are called *globally equivalent*, or simply *equivalent*, if also permutations of the coordinates v_i are allowed.

the basic results concerning these local equivalences so as to prepare us for a detailed study in the following chapters.

First we proved that there is in fact no distinction between the notions of SLOCC equivalence and LU equivalence of stabilizer states - that is, every two SLOCC equivalent stabilizer states are also LU equivalent and vice versa - thereby showing that we can restrict our attention to LU equivalence and LC equivalence. After having briefly defined LU equivalence of stabilizer states and codes, we moved to a formal definition of the local Clifford group. Up to overall phase factors of its elements, the local Clifford group $\mathcal{C}_n^l$ is simply the normalizer of the Pauli group $\mathcal{G}_n$ in the local unitary group $U(2)^{\otimes n}$. Due to this close connection between the local Clifford group and the Pauli group, and hence the stabilizer formalism, we are able to describe LC equivalence of stabilizer states and codes entirely within the binary stabilizer formalism. Using the binary picture, we could prove that every stabilizer state is LC equivalent to a graph state. This reduces our study to that of LC equivalence of graph states. The following chapter will be entirely dedicated to a study of this problem.

As far as the relevance of local equivalence of stabilizer states and codes is concerned, we showed that this problem is of interest in three different domains in quantum information theory; firstly, the study of local equivalence of stabilizer states arises naturally in an investigation of the entanglement properties of stabilizer states. Secondly, local equivalence of stabilizer codes is a natural equivalence relation to describe quantum codes that have the same error-correcting capabilities. Finally, LC equivalence of graph states naturally arises within the framework of the one-way quantum computer, corresponding to an equivalence relation between quantum algorithms.

A natural question that will be posed throughout this dissertation, is whether, like in the SLOCC-versus-LU case, there is in fact a difference between the notions of LU and LC equivalence of stabilizer states (codes). In other words, one asks whether $\text{LC}(\psi) = \text{LU}(\psi)$ for every stabilizer state $|\psi\rangle$. Note that $\text{LC}(\psi) \subseteq \text{LU}(\psi)$ by definition, so the question is whether the reverse inclusion also holds. A positive answer to this question would imply that there is in fact one single notion of "local"equivalence of stabilizer states. We will address this question in detail in chapter 6. However, similarities between LU and LC equivalence of stabilizer states will be present and pointed out throughout the entire text.

References

In section 3.2. we refer to Verstraete et al. [53] for the result on SLOCC normal forms. The definitions of LU equivalence of states and codes, the discussion of the local Clifford group and LC equivalence are all standard, see e.g. Preskill [33] and Nielsen and Chuang [8]. The (local) Clifford group has been studied extensively in QIT in both theoretical accounts as articles dedicated to applications; see [20, 4, 10, 11, 41] to name but a few. Interestingly, the Clifford group is also important in classical coding theory, see. e.g. the standard reference

[16] and more recent accounts [39, 30, 31] and references therein. Theorem 3.15, proving that every stabilizer state is LC equivalent to a graph state, is due to Schlingemann [40] and also Grassl et al. [21]. In section 3.4.3 we briefly mention classical codes over the Klein four group and we refer to Höhn [26] for further reading.

Corollary 3.4, proving that every two SLOCC stabilizer states are also LU equivalent, is a new result and was published in our work Ref. [48].

Chapter 4

LC equivalence of graph states

4.1 Introduction

In the previous chapter we have seen that every stabilizer state is LC equivalent to a graph state. Therefore, graph states can in fact be considered as some kind of "normal forms" of stabilizer states under LC equivalence. However, one quickly observes that these normal forms are by no means unique and therefore a study of LC equivalence within the set of graph states is called for $-$ this study will hence be the topic of research of this chapter.

It turns out that the problem of LC equivalence of graph states has a very rich and beautiful structure and is, moreover, far from trivial. First we will see that LC equivalence of n-qubit graph states naturally induces an equivalence relation on the set Θ_n of $n\times n$ adjacency matrices, such that two graph states are LC equivalent if and only if their corresponding adjacency matrices θ, $\theta' \in \Theta_n$ are related by a fractional linear transformation over $\mathbb{F}_2$ of the form

$$(A\theta + B)(C\theta + D)^{-1} = \theta', \tag{4.1}$$

where the $n\times n$ matrices A, B, C, D are diagonal and satisfy $AD{+}BC = I$. Such transformations can be regarded as discrete analogues annex generalizations of *Möbius transformations* (also known as *Cayley transformations*), which are defined by

$$x \mapsto \frac{ax + b}{cx + d}, \tag{4.2}$$

where $x, a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$; Möbius transformations are well known objects in complex analysis. In this chapter we study the transformations (4.1) in some detail and use them to gain insight in the number of graph states in an LC equivalence class and the number of distinct LC equivalence classes. After this we ask the question whether the transformations (4.1) have a clearcut combinatorial interpretation in terms graph transformations. In other words, we investigate how the transformations (4.1) affect the topology of a graph. We subsequently show that one basic graph transformation rule, called *local complementation*, suffices to generate the entire LC equivalence class of any graph. This yields an entire translation of the matrix transformations (4.1) into simple graph transformations.

It turns out that local complementation has been studied in graph theory by several authors, most importantly by Bouchet (see [3] and refs therein). Therefore, interesting insights can be obtained by studying the results in these references and interpreting them from our QIT point of view. Although there are many interesting such results, in this chapter we single out the most important one for our purposes, which is an efficient algorithm to detect whether two graphs are related by a sequence of local complementations. This result was proven in Ref. [2]. The connection between LC equivalence, fractional linear transformations and local complementation then allows us to quickly draw the conclusion that this algorithm can be used to efficiently recognize LC equivalence between two arbitrary stabilizer states. This last result will conclude the present chapter.

This chapter is organized as follows: in section 4.2 we relate LC equivalence of graph states to equivalence under fractional linear transformations of the corresponding adjacency matrices and study some basic properties of these transformations. We then use this formulation of LC equivalence to give a formula for the number of graph states in an LC equivalence class. This study is performed in section 4.3. We also briefly touch the problem of counting the number of LC equivalence classes in section 4.4. In section 4.5 we move to the definition of local complementation of graphs and show that two adjacency matrices are related by a transformation (4.1) if and only if their corresponding graphs are related by a sequence of local complementations. In section 4.6 we use this result to obtain an efficient algorithm to recognize LC equivalence of stabilizer states. In section 4.7 we consider the effect of local Pauli measurements on graph states. Finally, we conclude this chapter in section 4.8.

4.2 Fractional linear transformations

In this section we describe LC equivalence of graph states in terms of an equivalence relation on the corresponding set of adjacency matrices w.r.t a certain type of (nonlinear) transformations over $\mathbb{F}_2$. These transformations will be called fractional linear transformations (for reasons that will be clear from the definition of the transformations). We also discuss some basic properties of these fractional linear transformations.

Let G, G' be two graphs on n vertices with adjacency matrices θ, $\theta' \in \Theta_n$. We have seen in the previous chapter that the graph states $|G\rangle$ and $|G'\rangle$ are

LC equivalent if and only if

$$Q\begin{bmatrix}\theta\\ I\end{bmatrix}=\begin{bmatrix}\theta'\\ I\end{bmatrix}R \tag{4.3}$$

for some $Q \in C_n^l$ and $R \in GL(n, \mathbb{F}_2)$. Writing Q as

$$Q=\begin{bmatrix}A & B\\ C & D\end{bmatrix}, \tag{4.4}$$

where the $n \times n$ matrices A, B, C, D are diagonal, we obtain

$$\begin{bmatrix}A\theta+B\\ C\theta+D\end{bmatrix}=\begin{bmatrix}\theta' R\\ R\end{bmatrix}, \tag{4.5}$$

and therefore $R = C\theta + D$. Consequently, $|G\rangle$ and $|G'\rangle$ are LC equivalent if and only if there exists an operator (4.4) in C_n^l such that $C\theta + D$ is nonsingular and

$$(A\theta + B)(C\theta + D)^{-1} = \theta'. \tag{4.6}$$

This yields the following:

Proposition 4.1 *Let G, G' be two graphs with adjacency matrices θ, $\theta' \in \Theta_n$, respectively. Then the graph states $|G\rangle$ and $|G'\rangle$ are LC equivalent if and only if θ and θ' are related by a fractional linear transformation (4.6).*

Note that in general the image of a graph state under a local Clifford operation need not again yield another graph state. Indeed, an operation (4.4) in C_n^l maps the generator matrix $[\theta\ I]^T$ to the matrix on the l.h.s of (4.5). This matrix is the generator matrix of a graph state if and only if

(a) the matrix $C\theta + D$ is nonsingular, and

(b) the matrix $(A\theta + B)(C\theta + D)^{-1}$ has zeros on its diagonal.

This leads us to introduce, for each $Q \in C_n^l$, a domain of definition dom(Q), which is the set consisting of all $n \times n$ matrices $\theta \in \Theta_n$ which satisfy the conditions (a) and (b). If $\theta \in$ dom(Q), we will use the notation

$$Q(\theta) := (A\theta + B)(C\theta + D)^{-1}. \tag{4.7}$$

Note that, in the definition of the domain of Q, we need not impose the constraint that the matrix $Q(\theta)$ be symmetric, since this is automatically the case. This can be shown by noting that $Q(\theta)$ is symmetric if and only if the equality

$$(\theta C + D)(A\theta + B) = (\theta A + B)(C\theta + D) \tag{4.8}$$

holds. This last identity can readily be verified using the property $AD + BC = I$.

Let us consider some basic properties of the transformations $\theta \mapsto Q(\theta)$. We start with the following:

Proposition 4.2 *Let $\theta \in \Theta_n$ and let C, D be diagonal matrices such that $C\theta + D$ is invertible. Then there exists a unique*

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l \tag{4.9}$$

such that $\theta \in$ dom(Q).

Proof: Note that, since $C\theta + D$ is invertible, we only have to look for a Q such that $Q(\theta)$ has zero diagonal in order for θ to be in the domain of Q. First we will prove the uniqueness of A and B. Suppose there exist two pairs of diagonal matrices A, B and A', B' such that

$$Q := \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \; Q' := \begin{bmatrix} A' & B' \\ C & D \end{bmatrix} \in C_n^l$$

and $\theta \in \text{dom}(Q) \cap \text{dom}(Q')$. Denoting

$$\begin{aligned} \theta_z &:= A\theta + B \\ \theta'_z &:= A'\theta + B' \\ \theta_x &:= C\theta + D, \end{aligned} \tag{4.10}$$

we have $Q(\theta) = \theta_z \theta_x^{-1}$ and $Q'(\theta) = \theta'_z \theta_x^{-1}$. Denoting by $z_i^T, \bar{z}_i^T, x_i^T$ the rows of $\theta_z, \theta'_z, \theta_x$, respectively, the crucial observation is that either $\bar{z}_i^T = z_i^T$ or $\bar{z}_i^T = z_i^T + x_i^T$ for all $i = 1, \dots, n$; this is a direct consequence of the fact that Q, Q' are invertible and have the same lower blocks C, D. If the latter of the two possibilities is the case for some i_0, the i_0th diagonal entries of $Q(\theta)$ and $Q'(\theta)$ must be different, since

$$Q'(\theta)_{i_0 i_0} = \bar{z}_{i_0}^T (\theta_x^{-1})_{i_0} = z_{i_0}^T (\theta_x^{-1})_{i_0} + x_{i_0}^T (\theta_x^{-1})_{i_0} = Q(\theta)_{i_0 i_0} + 1, \tag{4.11}$$

where $(\theta_x^{-1})_{i_0}$ is the i_0th column of θ_x^{-1}. As both $Q(\theta)$ and $Q'(\theta)$ have zero diagonal, this yields a contradiction. We have therefore proven the uniqueness of A and B. To prove existence, note that for every $i \in \{1, \dots, n\}$ there are exactly two couples (a_i, b_i) such that

$$\begin{bmatrix} a_i & b_i \\ C_{ii} & D_{ii} \end{bmatrix} \tag{4.12}$$

is nonsingular. It follows from the above argument that we can always tune (a_i, b_i) such that $(A\theta + B)(C\theta + D)^{-1}$ has zero diagonal, where we take $A_{ii} = a_i$ and $B_{ii} = b_i$ for $i = 1, \dots, n$. Since each 2×2-matrix (4.12) is invertible, the matrix

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \tag{4.13}$$

is an element of C_n^l, which proves the result. $\square$

Next we state a criterion to verify whether $\theta \in \text{dom}(Q)$. To do this, we need some additional definitions. Let X be any $n \times n$ matrix. For every $\omega \subseteq \{1, \ldots, n\}$, define the $|\omega| \times |\omega|$ principal submatrix $X[\omega]$ of X by

$$X[\omega] = (X_{ij})_{i,j\in\omega}. \tag{4.14}$$

Secondly, for every $n \times n$ diagonal matrix Λ, denote $v_\Lambda := (\Lambda_{11}, \ldots, \Lambda_{nn})$. We can now state the following:

Proposition 4.3 *Let $n \in \mathbb{N}_0$ and*

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l. \tag{4.15}$$

Let $\omega \subseteq \{1, \ldots, n\}$ be the set defined by $\omega := \{i \mid C_{ii} = 1\}$ and let $\theta \in \Theta_n$. Then $\theta \in$ dom(Q) if and only if $\theta[\omega] + D[\omega]$ is nonsingular and $\theta v_{AC} = v_{BD}$.

Proof: First we show that $C\theta + D$ is invertible if and only if $\theta[\omega] + D[\omega]$ is invertible. It follows from the definition of ω and the fact that $Q \in C_n^l$ that $D[\bar{\omega}] = I$. Therefore, $C\theta + D$ has the form

$$\left[\begin{array}{c|c} I & 0 \\ \hline * & \theta[\omega] + D[\omega] \end{array}\right] \tag{4.16}$$

up to a simultaneous permutation of its rows and columns. It is now easy to see that $C\theta + D$ is nonsingular if and only $\theta[\omega] + D[\omega]$ is, which proves the first part of the theorem.

Secondly, we have to show that the matrix $(A\theta+B)(C\theta+D)^{-1}$ has zeros on its diagonal if and only if $\theta v_{AC} = v_{BD}$. To see this, note that for every $X \in \Theta_n$ and $R \in GL(n, \mathbb{F}_2)$ one has $R^T X R \in \Theta_n$. This follows from the observation that $(R^T X R)_{ii} = r_i^T X r_i = 0$, where r_i is the ith column of R (we have $r_i^T X r_i = 0$ because $X \in \Theta_n$). It follows from the above that $(A\theta + B)(C\theta + D)^{-1}$ has zero diagonal if and only if $(\theta C + D)(A\theta + B)$ has, which is equivalent to

$$(\theta AC\theta + AD\theta + \theta BC + BD)_{ii} = 0 \tag{4.17}$$

for every $i = 1, \ldots, n$. Since $\theta \in \Theta_n$ one has $(AD\theta)_{ii} = (\theta BC)_{ii} = 0$. Moreover,

$$\begin{aligned} (\theta AC\theta)_{ii} &= \sum_{k=1}^{n} \theta_{ik} A_k C_k \theta_{ki} \\ &= \sum_{k=1}^{n} \theta_{ik}^2 A_k C_k \\ &= \sum_{k=1}^{n} \theta_{ik} A_k C_k = (\theta v_{AC})_i . \end{aligned} \tag{4.18}$$

This shows that (4.17) is equivalent to $\theta v_{AC} = v_{BD}$. This proves the result. □

4.3 Number of graphs in an LC equivalence class

The translation of LC equivalence of graph states in terms of fractional linear transformations of the associated adjacency matrices will allow us to obtain a formula for the number of distinct graph states that are LC equivalent to a given graph state. For the remainder of this section, we will let G be a connected graph on n vertices with adjacency matrix $\theta \in \Theta_n$. Moreover, we let $\mathrm{LC}(G) \equiv \mathrm{LC}(\theta)$ be the set of all graphs corresponding to states LC equivalent to $|G\rangle$. Using proposition 4.1, this is equivalent to stating that

$$\mathrm{LC}(\theta) = \{Q(\theta) \mid Q \in C_n^l \text{ and } \theta \in \mathrm{dom}(Q)\}. \tag{4.19}$$

We start our analysis of $|\mathrm{LC}(G)|$ by defining the sets

$$\begin{aligned} \Delta(G) \equiv \Delta(\theta) &:= \{Q \in C_n^l \mid \theta \in \mathrm{dom}(Q)\} \\ \Sigma(G) \equiv \Sigma(\theta) &:= \{Q \in C_n^l \mid Q(\theta) = \theta\}. \end{aligned} \tag{4.20}$$

The set $\Delta(G)$ consists of all operations in C_n^l that have θ in their domain. The set $\Sigma(G)$, which is a subset of $\Delta(G)$, contains all operations in C_n^l that have θ as a fixed point. One has the following:

Proposition 4.4 *Let G be a graph with adjacency matrix θ. Then*

$$|LC(G)| = \frac{|\Delta(G)|}{|\Sigma(G)|}. \tag{4.21}$$

Proof: Let G be a graph with adjacency matrix $\theta \in \Theta_n$ and define the function

$$f_\theta : Q \in \Delta(\theta) \mapsto Q(\theta) \in LC(\theta). \tag{4.22}$$

It easy to see that

$$\Delta(\theta) = \bigcup_{\theta' \in \mathrm{LC}(\theta)} f_\theta^{-1}(\theta'), \tag{4.23}$$

where $f_\theta^{-1}(\theta')$ is the inverse image of θ' under the mapping f_θ, i.e.,

$$f_\theta^{-1}(\theta') = \{Q \in \Delta(\theta) \mid Q(\theta) = \theta'\}. \tag{4.24}$$

We first prove that $|f_\theta^{-1}(\theta')| = |\Sigma(\theta)|$ for every $\theta' \in \mathrm{LC}(\theta)$. To see this, fix an arbitrary $Q_0 \in f_\theta^{-1}(\theta')$. Then $Q_0 Q \in f_\theta^{-1}(\theta')$ for every $Q \in \Sigma(\theta)$. Conversely, take any $Q' \in f_\theta^{-1}(\theta')$. Then $Q' = Q_0(Q_0^{-1}Q')$, where $Q_0^{-1}Q' \in \Sigma(\theta)$ since $Q_0(\theta) = Q'(\theta)$. This shows that

$$f_\theta^{-1}(\theta') = \{Q_0 Q \mid Q \in \Sigma(\theta)\}, \tag{4.25}$$

which proves that $|f_\theta^{-1}(\theta')| = |\Sigma(\theta)|$. The result follows by noting that (4.23) is a disjoint union and therefore $|\Delta(\theta)| = |\mathrm{LC}(\theta)| \cdot |\Sigma(\theta)|$. This ends the proof. $\square$

It follows from proposition 4.4 that, in order to calculate $|\mathrm{LC}(G)|$, we have to gain insight in the cardinalities of the sets $\Delta(G)$ and $\Sigma(G)$. We will therefore split up our calculation, first considering $|\Delta(G)|$ and then $|\Sigma(G)|$.

4.3.1 Computing $|\Delta(G)|$

It follows from proposition 4.2 that $|\Delta(G)|$ is equal to the number of couples (C, D) of diagonal matrices such that $C\theta + D$ is nonsingular. To compute this number we let $d(\phi)$ be the number of $k \times k$ diagonal binary matrices Λ such that $\phi + \Lambda$ is nonsingular, for any $\phi \in \Theta_k$ ($k \in \mathbb{N}_0$). Then the proof of proposition 4.3 immediately yields the following result:

Proposition 4.5 *Let G be a graph on n vertices. Then*

$$|\Delta(G)| = \sum_{\omega \subseteq \{1,\dots,n\}} d\left(\theta[\omega]\right). \tag{4.26}$$

The formula (4.26) allows to compute $|\Delta(G)|$ easily for graphs with a sufficient degree of symmetry.

Example. Consider the complete graph K_n on n vertices, which has an adjacency matrix $\theta(K_n)$ satisfying $\theta(K_n)_{ij} = 1$ for every $i, j = 1, \dots, n$, $i \neq j$. Note that

$$\theta(K_n)[\omega] = \theta(K_{|\omega|}), \tag{4.27}$$

for every $\omega \subseteq \{1, \dots, n\}$. Moreover, it is easy to see that

$$d(\theta(K_k)) = \begin{cases} k+1 & \text{if } k \text{ is even} \\ k & \text{if } k \text{ is odd,} \end{cases} \tag{4.28}$$

for every $k \in \mathbb{N}_0$. A simple calculation then shows that

$$\begin{aligned} \Delta(K_n) &= 2^{n-1} + \sum_{k=1}^{n} \binom{n}{k} k \\ &= (n+1)2^{n-1}. \end{aligned} \tag{4.29}$$

◇

The formula in proposition 4.5 also leads to a lower bound for $|\Delta(G)|$. We need the following lemma [18]:

Lemma 4.6 *Let $k \in \mathbb{N}_0$ and let $\phi \in \Theta_k$ with $\mathrm{rank}_{\mathbb{F}_2}(\phi) = r$. Then there exist a permutation matrix $\Pi \in \mathbb{F}_2^{k \times k}$, a matrix $R \in \mathbb{F}_2^{(k-r)\times r}$ and a set $\omega \subseteq \{1, \dots, k\}$ with $|\omega| = r$ such that*

$$\Pi^T \phi \Pi = \begin{bmatrix} I \\ R \end{bmatrix} \phi[\omega] \begin{bmatrix} I & R^T \end{bmatrix}. \tag{4.30}$$

Proof: Since ϕ has rank r, this matrix has a linearly independent set ω of r rows. By symmetry, the corresponding set of columns is also linearly independent.

Therefore, there exists a permutation matrix Π, a matrix $N \in \mathbb{F}_2^{(k-r)\times r}$ and a matrix $H \in \mathbb{F}_2^{(k-r)\times(k-r)}$ such that

$$\Pi^T \phi \Pi = \begin{bmatrix} \phi[\omega] & N^T \\ N & H \end{bmatrix}. \tag{4.31}$$

Since the first r rows of this matrix generate the row space of $\Pi^T\phi\Pi$, one has $N = R\phi[\omega]$ for some $R \in \mathbb{F}_2^{(k-r)\times r}$, and hence $H = RN^T = R\phi[\omega]R^T$. Therefore

$$\Pi^T \phi \Pi = \begin{bmatrix} \phi[\omega] & \phi[\omega]R^T \\ R\phi[\omega] & R\phi[\omega]R^T \end{bmatrix}, \tag{4.32}$$

which yields the result. □

Remark. Note that the matrix $\phi[\omega]$ in the above lemma is nonsingular. ◇

Corollary 4.7 *Let G be a simple graph on n vertices with adjacency matrix $\theta \in \Theta_n$. Then $|\Delta(G)| \geq 2^n$.*

Proof: We claim that $d(\phi) \geq 1$ for every $\phi \in \Theta_k$. This will yield the desired result. To prove the claim, let $\phi \in \Theta_k$. We now use lemma 4.6, yielding Π, R and ω such that

$$\Pi^T \phi \Pi = \begin{bmatrix} \phi[\omega] & \phi[\omega]R^T \\ R\phi[\omega] & R\phi[\omega]R^T \end{bmatrix}. \tag{4.33}$$

Then the matrix

$$\begin{aligned} \Pi^T\phi\Pi + \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} &= \begin{bmatrix} \phi[\omega] & \phi[\omega]R^T \\ R\phi[\omega] & R\phi[\omega]R^T + I \end{bmatrix} \\ &= \begin{bmatrix} I & 0 \\ R & I \end{bmatrix} \begin{bmatrix} \phi[\omega] & \phi[\omega]R^T \\ 0 & I \end{bmatrix} \end{aligned} \tag{4.34}$$

is nonsingular, since it is a product of nonsingular matrices. Equivalently, the matrix

$$\phi + \Pi \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \Pi^T \tag{4.35}$$

is nonsingular. The result follows by noting that the matrix $\Pi \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \Pi^T$ is diagonal. This ends the proof. □

Note that the above bound is saturated by the empty graph. Indeed, $|\Delta(0)| = 2^n$, where 0 is the $n \times n$ zero matrix.

This ends our analysis of the cardinality of $\Delta(G)$. We now move to a study of the denominator of (4.21), i.e., the cardinality of $\Sigma(G)$.

4.3.2 Computing $|\Sigma(G)|$

We now consider the set $\Sigma(G)$. Using standard group theoretic terminology, we note that $\Sigma(\theta)$ is the stabilizer of θ under the action (4.7) of the group C_n^l on the set Θ_n. As a stabilizer is always a group, the set $\Sigma(\theta)$ is a subgroup of C_n^l and therefore $|\Sigma(\theta)|$ must divide $|C_n^l| = 6^n$. This leads to a first result:

Proposition 4.8 *Let G be a graph. Then $|\Sigma(G)| = 2^i 3^j$ for some $i, j \in \mathbb{N}$.*

Next, consider

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l. \tag{4.36}$$

It follows from proposition 3.11 that $Q \in \Sigma(G)$ if and only if

$$\begin{bmatrix} \theta & I \end{bmatrix} P\, Q \begin{bmatrix} \theta \\ I \end{bmatrix} = 0, \tag{4.37}$$

which is equivalent to

$$\theta C \theta + A\theta + \theta D + B = 0. \tag{4.38}$$

In other words, $|\Sigma(G)|$ is equal to the number of solutions (A, B, C, D) to the linear equation (4.38) that satisfy the additional constraint

$$AD + BC = I. \tag{4.39}$$

We observe that (4.38) implies that the matrix $A\theta+\theta D$ is symmetric or, equivalently, that $[A+D, \theta] = 0$. The next lemma shows that this last identity implies that either $A = D$ or $A = D + I$:

Lemma 4.9 *Let G be a connected graph with adjacency matrix θ and let Λ be a diagonal matrix satisfying $[\Lambda, \theta] = 0$. Then either $\Lambda = 0$ or $\Lambda = I$.*

Proof: Let $\omega \subseteq \{1, \ldots, n\}$ be the set of all j such that $\Lambda_{jj} = 0$ and suppose that $\emptyset \neq \omega \neq \{1, \ldots, n\}$, i.e., $0 \neq \Lambda \neq I$. We will show that this leads to a contradiction. Let $\theta\langle\omega\rangle$ be the off-diagonal $|\omega| \times (n - |\omega|)$ subblock of θ defined by

$$\theta\langle\omega\rangle = (\theta_{ij})_{i\in\omega, j\in\bar{\omega}}, \tag{4.40}$$

as before. Then $[\Lambda, \theta] = 0$ if and only if $\theta\langle\omega\rangle = 0$. But this cannot happen since G is connected. This proves the result. $\square$

Lemma 4.9 shows that any $Q \in \Sigma(G)$ must have one of the two forms

$$\begin{bmatrix} A & I \\ I & A+I \end{bmatrix} \text{ or } \begin{bmatrix} BC+I & B \\ C & BC+I \end{bmatrix}. \tag{4.41}$$

Consequently, $|\Sigma(G)|$ is sum of the cardinalities of the following two sets:

$$\Sigma_1(G) := \{A \mid \theta^2 + A\theta + \theta A + \theta + I = 0\} \tag{4.42}$$
$$\Sigma_2(G) := \{(B, C) \mid \theta C\theta + BC\theta + \theta BC + B = 0\}, \tag{4.43}$$

where A, B, C are diagonal $n \times n$ matrices. We will first consider $\Sigma_1(G)$ and then $\Sigma_2(G)$.

4.3.2.1 Computing $|\Sigma_1(G)|$

The cardinality of $\Sigma_1(G)$ is either equal to 0 or 2. To see this, firstly note that $A \in \Sigma_1(G)$ if and only $A + I \in \Sigma_1(G)$. Moreover, suppose that $A' \in \Sigma_1(G)$. Then the identities

$$\begin{aligned} \theta^2 + A\theta + \theta A + \theta + I &= 0 \\ \theta^2 + A'\theta + \theta A' + \theta + I &= 0 \end{aligned} \tag{4.44}$$

imply that $[A + A', \theta] = 0$, such that either $A' = A$ or $A' = A + I$ from lemma 4.9. This shows that $|\Sigma_1(G)|$ is either equal to 0 or 2. Note that $\Sigma_1(G)$ is an affine space, such that checking whether it is nonempty can be done efficiently. Also, note that the expression $\theta^2 + A\theta + \theta A + \theta + I = 0$ is exactly the one we encountered when defining $\mathbb{F}_4$-linear stabilizers in chapter 2. It follows that

$$|\Sigma_1(G)| = \begin{cases} 2 & \text{if } G \in \mathcal{L}_n \\ 0 & \text{otherwise.} \end{cases} \tag{4.45}$$

4.3.2.2 Computing $|\Sigma_2(\theta)|$

We now turn to the study of the set $\Sigma_2(\theta)$. Recall that this is the set consisting of all couples of diagonal matrices (B, C) such that

$$\theta C\theta + BC\theta + \theta BC + B = 0. \tag{4.46}$$

We are therefore faced with quadratic equations in the entries b_i, c_i ($i = 1, \dots, n$) of B, C, respectively. Firstly, equation (4.46) implies that

$$\sum_{j=1}^{n} \theta_{ij} c_j = (\theta C\theta)_{ii} = b_i. \tag{4.47}$$

Equivalently, we have $\theta v_C = v_B$, such that we can immediately eliminate B from equation (4.46), yielding quadratic equations in the c_is only. Performing this elimination of B, one readily obtains the equations

$$\sum_{k=1}^{n} \theta_{ik}\theta_{jk}c_k + (c_i\theta_i + c_j\theta_j)^T c = 0 \qquad \text{if } (i, j) \in E$$

$$\sum_{k=1}^{n} \theta_{ik}\theta_{jk}c_k = 0 \qquad \text{if } (i,j) \notin E, \tag{4.48}$$

where we have used the notation $c \equiv v_C = (c_1, \ldots, c_n)$. The set E is the edge set of G, as before. The above equations can be rewritten using the notation

$$\nu_{ij} := (\theta_{i1}\theta_{j1}, \ldots, \theta_{in}\theta_{jn}) \in \mathbb{F}_2^n, \tag{4.49}$$

for every $i, j \in \{1, \ldots, n\}$, yielding

$$\begin{aligned} \nu_{ij}^T\, c + (c_i\theta_i + c_j\theta_j)^T c = 0 \qquad & \text{if } (i,j) \in E \\ \nu_{ij}^T\, c = 0 \qquad & \text{if } (i,j) \notin E. \end{aligned} \tag{4.50}$$

Remark. Using the natural one-to-one correspondence between a vector $v \in \mathbb{F}_2^n$ and the set $\{i\ |v_i = 1\} \subseteq \{1, \ldots, n\}$, the vector ν_{ij} simply corresponds to the set $N(i) \cap N(j)$. ◇

An important notion in the solution of the equations (4.50) is that of the *bineighborhood space* of G, as defined in Ref. [2], which we introduce now. First, a *cycle* $\mathcal{C}$ of the graph G is a set of edges of the form

$$\{(i_1, i_2), (i_2, i_3), \ldots, (i_{N-1}, i_N), (i_N, i_1)\}, \tag{4.51}$$

where all $(i_\alpha, i_\beta) \in E$. The bineighborhood space $\nu(G) \equiv \nu(\theta)$ of G is then the subspace of $\mathbb{F}_2^n$ spanned by the sets of vectors

$$\{ \sum_{(i,j)\in\mathcal{C}} \nu_{ij} \mid \mathcal{C} \text{ is a cycle of } G\} \quad \text{and} \quad \{\nu_{ij} \mid (i,j) \notin E\}. \tag{4.52}$$

We have the following result:

Lemma 4.10 *Let G be a graph on n vertices. Then any solution $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$ to (4.50) belongs to $\nu(G)^\perp$. Here, the orthogonal complement is taken w.r.t. to the standard inner product in $\mathbb{F}_2^n$.*

Proof: Let $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$ be a solution to (4.50). The proof follows after noting that

$$\sum_{(i,j)\in\mathcal{C}} c_i\theta_i + c_j\theta_j = 0 \tag{4.53}$$

for every cycle $\mathcal{C}$ of G, since every term $c_i\theta_i$ occurs exactly twice in the above sum. This ends the proof. □

Corollary 4.11 *Let G be a graph. Then $|\Sigma_2(G)| \leq |\nu(G)^\perp|$.*

At the time of writing this dissertation, numerical experiments seemed to imply that the converse statement to lemma 4.10 is also true. That is, it appears that every element c in the orthogonal complement of the bineighborhood space of a graph satisfies (4.50). We therefore formulate the following conjecture:

Conjecture 4.12 *Let $G = (V, E)$ be a (connected) graph on n vertices. Then the quadratic forms*

$$x \in \mathbb{F}_2^n \mapsto \nu_{ij}^T\, x + (x_i\theta_i + x_j\theta_j)^T x, \quad \textit{for every } (i,j) \in E$$

are zero on the orthogonal complement of the bineighborhood space of the graph G.

Corollary 4.13 *Under the assumption of conjecture 4.12, one has $|\Sigma_2(G)| = |\nu(G)^\perp|$ for any graph G.*

Therefore (again, under the assumption of conj. 4.12), computing the cardinality of $\Sigma_2(G)$ can be done by calculating the number of elements of the bineighborhood space of G, which corresponds to finding the number of solutions to a system of linear equations over $\mathbb{F}_2$. This ends our analysis of the set $\Sigma_2(G)$.

4.3.2.3 Returning to $|\Sigma(G)|$

Having studied the sets $\Sigma_1(G)$ and $\Sigma_2(G)$, we can combine our results and come to a formula to compute $|\Sigma(G)| = |\Sigma_1(G)| + |\Sigma_2(G)|$. We obtain:

Corollary 4.14 *Under the assumption of conjecture 4.12, we have*

$$|\Sigma(G)| = \begin{cases} 2 + |\nu(G)^\perp| & \textit{if } G \in \mathcal{L}_n \\ |\nu(G)^\perp| & \textit{otherwise} \end{cases} \tag{4.54}$$

This result, together with proposition 4.5, ends our analysis of the number of graphs states in an LC equivalence class.

4.4 Number of LC equivalence classes

The above analysis of the set $\Sigma(G)$ is also very useful to gain insight in the number of LC equivalence classes, or, equivalently, the number of orbits under the action (4.7) of the group C_n^l on the set of graphs on n vertices. There is indeed a well known general formula to count the number of orbits of the action of an arbitrary finite group on an arbitrary set. This is the Cauchy-Frobenius lemma (a.k.a. Burnside's lemma), which states that the number of orbits of a finite group H acting on a set X is equal to

$$\frac{1}{|H|}\sum_{h\in H} |\mathrm{Fix}(h)|. \tag{4.55}$$

Here, $|\mathrm{Fix}(h)|$ is the number of fixed points in the set X of the group element h. Thus, (4.55) is equal to the average number of fixed points of H. The number λ_n of local equivalence classes of (connected) graphs on n vertices is then equal to

$$\lambda_n = \frac{1}{6^n} \sum_{Q \in C_n^l} |\mathrm{Fix}(Q)|, \tag{4.56}$$

where

$$\mathrm{Fix}(Q) = \{\theta \in \Theta_n^{\mathrm{conn}} \mid Q(\theta) = \theta\}. \tag{4.57}$$

Here, Θ_n^{conn} is the subset of Θ_n consisting of all adjacency matrices corresponding to connected graphs. It is easy to see that (4.56) is equal to

$$\begin{aligned} \lambda_n \quad &= \quad \frac{1}{6^n} \sum_{\theta \in \Theta_n^{\mathrm{conn}}} |\Sigma(\theta)| \\ &=^{[\text{conj } 4.12]} \quad \frac{1}{6^n} \left\{ 2 \cdot |\mathcal{L}_n| + \sum_{\theta \in \Theta_n^{\mathrm{conn}}} |\nu(\theta)^{\perp}| \right\}, \end{aligned} \tag{4.58}$$

where we have used corollary 4.14 . The equality $=^{[\text{conj } 4.12]}$ holds under the assumption of conjecture 4.12.

4.5 Local complementation

In the previous sections we have studied LC equivalence of graph states by considering the linear fractional transformations (4.7). A next question is then, how these transformations affect the topology of the corresponding graphs. That is, we ask whether one can translate the transformations $\theta \to Q(\theta)$, which are defined on the algebraic level of the adjacency matrix of a graph, into clearcut (combinatoric) graph transformation rules. We investigate this question in this section.

We start with some graph theoretical notions. Let $G = (V, E)$ be a graph on n vertices. A graph $G' = (V', E')$ which satisfies $V' \subseteq V$ and $E' \subseteq E$ is a *subgraph* of G and one writes $G' \subseteq G$. For a subset $\omega \subseteq V$ of vertices, the *induced subgraph* $G[\omega] \subseteq G$ is the graph with vertex set ω and edge set

$$\{\{i, j\} \in E \mid i, j \in \omega\}. \tag{4.59}$$

Note that the adjacency matrix of $G[\omega]$ is the matrix $\theta[\omega]$ as defined in section 4.2. If G has an adjacency matrix θ, its *complement* $\bar{G}$ is the graph with adjacency matrix $\theta + \mathbb{I}$, where $\mathbb{I}$ is the $n \times n$-matrix which has all ones, except for the diagonal entries, which are zero. In other words, the set $\{i, j\}$ is an edge of $\bar{G}$ whenever $\{i, j\}$ is not an edge of G and vice versa.

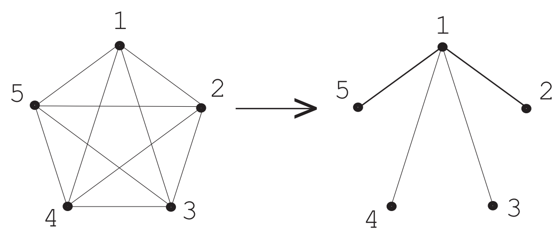

Figure 4.1: Local complementation of the complete graph K_5 at vertex 1.

With these definitions, one can define the following graph transformation rule: let $i \in V$ be an arbitrary vertex of G. Recall that the neighborhood $N(i) \subseteq V$ of a vertex $i \in V$ is the set of all neighbors of i. The *local complement of* G *at vertex* i, denoted by $G*i$, is obtained by replacing the subgraph $G[N(i)]$, i.e., the induced subgraph of the neighborhood of i in G, by its complement, and leaving the rest of the graph unchanged. The adjacency matrix $\theta * i$ of $G * i$ is equal to

$$\theta * i = \theta + \theta_i \theta_i^T + \text{ diag}(\theta_i), \tag{4.60}$$

where θ_i is the ith column of θ and $\text{diag}(\theta_i)$ is a diagonal matrix such that the kth diagonal entry is equal to θ_{ik}, for every $k = 1, \ldots, n$. Therefore, local complementation corresponds to a quadratic operation in the entries of θ.

Example. Consider the complete graph K_5 on 5 vertices. The local complement $K_5 * 1$ of K_5 at vertex 1 is shown in Fig. 4.1. $\diamond$

Local complementation of graphs has the following basic properties:

Proposition 4.15 *Let $G = (V, E)$ be a graph on n vertices. Let $i, j \in V$ be vertices of G. Then*

(i) $(G * i) * i = G$;

(ii) if $\{i, j\} \notin E$ *then* $(G * i) * j = (G * j) * i$

Proof: These are simple verifications. $\square$

Having defined local complementation, we now show that the transformation $\theta \mapsto \theta * i$ can be realized as a fractional linear transformation (4.7). This is stated in proposition 4.16.

Proposition 4.16 *Let $G = (V, E)$ be a graph on n vertices with adjacency matrix $\theta \in \Theta_n$ and let $i \in V$ be a vertex of G. Define*

$$Q_{\theta,i} = \left[\begin{array}{cc} I & diag(\theta_i) \\ \Lambda_i & I \end{array} \right] \in C_n^l, \tag{4.61}$$

where Λ_i is defined by $(\Lambda_i)_{ii} = 1$ and $\Lambda_{jk} = 0$ for every $(j,k) \neq (i,i)$. Then

$$\theta * i = Q_{\theta,i}(\theta). \tag{4.62}$$

Proof: The result can be shown straightforwardly by calculating $Q_{\theta,i}(\theta) = (\theta + \text{ diag}(\theta_i))(\Lambda_i\theta + I)^{-1}$ and noting that the matrix $\Lambda_i\theta + I$ is its own inverse. $\square$

We now introduce the necessary terminology needed to describe a successive application of the local complementation rule. A *word* m on the vertex set V is a sequence $m = i_1 i_2 \dots i_k$ with $i_j \in V$. We write

$$G * m = (((G * i_1) * i_2) \dots) * i_k. \tag{4.63}$$

Two graphs G and G' on the vertex set V are called *locally equivalent*[1] if there exists a word m on V such that $G * m = G'$.

Next we prove that the entire LC equivalence class of a graph is generated by successive application of the local complementation rule: we will show that two matrices θ, $\theta' \in \Theta_n$ are related by a transformation (4.7) if and only if their corresponding graphs are locally equivalent. First we prove the following proposition.

Theorem 4.17 *Define the matrix class $\mathbb{T} \subseteq \mathbb{F}_2^{n\times n}$ by*

$$\mathbb{T} = \quad \{C\theta + D| \ \theta \in \Theta_n \text{ and } C, D \text{ are diagonal and } C\theta + D \text{ is invertible}\}.$$

For every $i = 1, \dots, n$, define the transformation f_i of $\mathbb{T}$ by

$$f_i(X) = X(\Lambda_i X + X_{ii}\Lambda_i + I), \tag{4.64}$$

where $X \in \mathbb{T}$, and denote $f_{jk}(\cdot) := f_j f_k f_j(\cdot)$ for every $j, k = 1, \dots, n$. Consider an element $R \in \mathbb{T}$ and choose θ, C, D such that $R = C\theta + D$. Then

(i) there exists a finite sequence of f_is and f_{jk}s such that

$$f_{j_M k_M} \dots f_{j_1 k_1} f_{i_N} \dots f_{i_1}(R) = I, \tag{4.65}$$

where all the indices in the sequence are different;

(ii) define the word $m = i_1 \dots i_N \ j_1 k_1 j_1 \dots j_M k_M j_M$. Then there exists diagonal matrices A, B such that

$$Q := \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l \tag{4.66}$$

and $\theta \in$ dom(Q) and

$$\theta * m = Q(\theta). \tag{4.67}$$

[1]Here, the term *locally* equivalent, which is taken from the graph theoretic literature, refers to the fact that local complementation inverts the *neighborhood* of a vertex. It is a nice coincidence that we use the same terminology in our QIT problem of local equivalence.

Proof: First, straightforward calculation shows that f_i maps the class of matrices of the form $C\theta + D$ to itself. Furthermore, for each $X \in \mathbb{T}$ the matrix $\Lambda_i X + X_{ii}\Lambda_i + I$ is invertible, which implies that f_i maps invertible matrices to invertible matrices. Therefore each f_i is indeed a transformation of $\mathbb{T}$.

Statement (i) is proven by applying the algorithm below, where the idea is to successively make each ith row of R equal to the ith canonical basis vector $e_i^T = [0\dots 0\ 1\ 0\dots 0]$, by applying the correct f_js in each step. The image of R throughout the consecutive steps will be denoted by the same symbol $\bar{R} = (r_{ij})$. The algorithm consists of repeatedly performing one of the two following sequences of operations on $\bar{R}$:

Case 1: If $\bar{R}$ has a diagonal entry $r_{i_0 i_0} = 1$ (and the i_0th row of $\bar{R}$ is not yet equal to the basis vector $e_{i_0}^T$), apply f_{i_0}. It is easy to verify that, in this situation, f_{i_0} transforms the i_0th row of $\bar{R}$ into the basis vector $e_{i_0}^T$.

Case 2: If the conditions for case 1 are not fulfilled, apply the following sequence of three operations: firstly, fix a j_0 such that $r_{j_0 j_0} = 0$ and apply f_{j_0}. It can easily be seen that then $\text{diag}(\bar{R}) \to \text{diag}(\bar{R}) + \bar{R}_{j_0}$, where $\bar{R}_{j_0}$ is the j_0th column of $\bar{R}$ and $\text{diag}(\bar{R})$ is the diagonal of $\bar{R}$. Since $\bar{R}$ is invertible, $\bar{R}_{j_0}$ has some nonzero element, say on the k_0th position $r_{k_0 j_0} = 1$. Therefore, the application of f_{j_0} has put a 1 on the k_0th diagonal entry of the resulting $\bar{R}$. Now we apply f_{k_0}, turning the k_0th row into $e_{k_0}^T$ as in case 1. Furthermore, this second operation has put $r_{j_0 k_0}$ on the j_0th diagonal entry and, from the symmetry of $\bar{R}$, it holds that $r_{j_0 k_0} = r_{k_0 j_0} = 1$. Therefore, by again applying f_{j_0}, we obtain an $e_{j_0}^T$ on the j_0th row of the resulting $\bar{R}$. Finally, we note that after performing this sequence of operations, we end up with an $\bar{R}$ which will again satisfy the conditions for case 2.

Repetition of these elementary steps will eventually yield the identity matrix, which concludes the proof of statement (i).

Statement (ii) is proven by induction on the length of the sequence of f_is and f_{jk}s. We will consider the f_is and f_{jk}s as two different types of elementary blocks in the sequence (4.65). The proof will therefore consist of two parts A and B, part A dealing with the f_is and part B with the f_{jk}s.

<u>Part A:</u> in the basis step of the induction we have $f_i(R) = I$, where $R \in \mathbb{T}$. Any such R satisfies $R = \Lambda_i R + R_{ii}\Lambda_i + I$ and therefore must be of the form

$$R = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ x_1 & & x_{i-1} & 1 & x_{i+1} & & x_n \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{matrix}$$

for some x_j. Then any θ, C, D which satisfy $R = C\theta + D$ must satisfy $\theta_{ij} = x_j$ and $D = I$; moreover, if $C_{jj} = 1$ for $j \neq i$ then the jth row of θ must be equal to zero and if $C_{ii} = 0$ the ith row of θ must be to zero. It is now easy to see that $\theta * i = Q(\theta)$, with

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l, \tag{4.68}$$

for some A, B.

In the induction step, we assume that the statement holds for all sequences $f_{i_1}, \ldots, f_{i_N}$ of fixed length N and prove that this implies that the statement is true for sequences of length $N+1$. We start from the given that

$$f_{i_N} \ldots f_{i_1} f_i(R) = I$$

for some $f_i, f_{i_1}, \ldots, f_{i_N}$ and $R \in \mathbb{T}$ and we choose θ, C, D such that $C\theta + D = R$. Note that it follows from case 1 in the algorithm in part (i) of the theorem that we may take $C_{ii} = 1 = D_{ii}$, as a single f_i (as opposed to an f_{ij}) is only applied when $R_{ii} = 1$. Furthermore, we will denote by ω the set of all $j \in \{1, \ldots, n\}$ such that $C_{jj} = 1$. As R is invertible, this implies that $D_{kk} = 1$ for $k \in \bar{\omega}$. Now, denoting $R' := f_i(R)$, we have $f_{i_N} \ldots f_{i_1}(R') = I$, which allows us to use the result for length N: for any θ', C', D' that satisfy $C'\theta' + D' = R'$ there exists a $Q' \in C_n^l$ which has C', D' as its lower blocks such that $\theta' \in \operatorname{dom}(Q')$ and

$$\theta' * (i_1 \ldots i_N) = Q'(\theta'). \tag{4.69}$$

We make the following choices for θ', C', D':

$$\begin{aligned} \theta' &= \theta * i \\ C' &= C + \Lambda_i \\ D' &= D + \operatorname{diag}(\theta_i)_\omega \end{aligned}$$

where $\operatorname{diag}(\theta_i)_\omega$ is the diagonal matrix which has θ_{ij} on the jth diagonal entry if $j \in \omega$ and zeros elsewhere. This choice for θ', C', D' indeed yields $C'\theta' + D' = R'$; we will however omit the calculation since it is straightforward. Now, using the definition of θ' and proposition 4.16, equation (4.69) becomes

$$(\theta * i) * (i_1 \ldots i_N) = (Q' Q_{\theta,i})(\theta). \tag{4.70}$$

It is now again straightforward to show that $Q := Q' Q_{\theta,i}$ has C and D as its lower blocks. This proves the induction step, thereby concluding the proof of part A.

Part B: The proof of this part is analogous to part A, though a bit more involved. The basis step now reads $f_{jk}(R) = I$. Now case 2 in the algorithm in part (i) of the lemma implies that $R_{jj} = 0 = R_{kk}$ and $R_{jk} = 1$, as only if this is the case, f_{jk} is applied in the algorithm. For simplicity, but without losing generality, we take $i = 1, j = 2$. Then R must be of the form

$$R = \left[\begin{array}{cc|c} 0 & 1 & \theta_1^T \\ 1 & 0 & \theta_2^T \\ \hline 0 & 0 & I \end{array}\right],$$

where the θ_i are $(n-2)$-dimensional column vectors. Choosing θ, C, D s.t. $R = C\theta + D$, the matrix θ must satisfy

$$\theta = \left[\begin{array}{cc|c} 0 & 1 & \theta_1^T \\ 1 & 0 & \theta_2^T \\ \hline \theta_1 & \theta_2 & \phi \end{array}\right],$$

where ϕ is a symmetric $(n-2)\times(n-2)$-matrix with zero diagonal; furthermore $D_{11} = 0 = D_{22}$, $D_{jj} = 1$, $C_{11} = 1 = C_{22}$ and if $C_{j+2,j+2} = 1$ then $\theta_{1j} = \theta_{2j} = \phi_{kj} = 0$, for $j, k = 1, \ldots, n-2$. We will give the proof for $C_{j+2,j+2} = 0$, the other cases are similar. Thus, we have to show that there exists a $Q \in C^l$ with lower blocks C, D s.t. $g_{12}(\theta) = Q(\theta)$. To prove this, we use proposition 4.16, yielding

$$Q = \begin{bmatrix} \cdot & \cdot \\ \Lambda_1 & I \end{bmatrix} \begin{bmatrix} I & \mathrm{diag}((\theta * 1)_2) \\ \Lambda_2 & I \end{bmatrix} \begin{bmatrix} I & \mathrm{diag}(\theta_1) \\ \Lambda_1 & I \end{bmatrix},$$

where $(\theta * 1)_2 = (1, 0, \theta_{13} + \theta_{23}, \ldots, \theta_{1n} + \theta_{2n})$ is the second column of $(\theta * 1)$. A simple calculation reveals that

$$Q = \begin{bmatrix} \cdot & \cdot \\ \Lambda_1 + \Lambda_2 & I + \Lambda_1 + \Lambda_2 \end{bmatrix} = \begin{bmatrix} \cdot & \cdot \\ C & D \end{bmatrix},$$

which proves the basis of the induction.

In the induction step, we again follow an analogous reasoning to part A: we assume that the statement is true for sequences $f_{j_1k_1}, \ldots, f_{j_Nk_N}$ of length N and prove that this implies the statement for length $N+1$. Our starting point is now

$$f_{j_Nk_N} \ldots f_{j_1k_1} f_{jk}(R) = I$$

for some $f_{jk}, f_{j_1k_1}, \ldots, f_{j_Nk_N}$ and $R \in \mathbb{T}$. Note that again we have $R_{jj} = 0 = R_{kk}$ and $R_{jk} = 1$ as in the basis step. As from this point on the strategy is identical as in part A and all calculations are straightforward, we will only give a sketch: first we denote $R' = f_{jk}(R)$; for θ, C, D s.t. $R = C\theta + D$, we define

$$\begin{aligned} \theta' &= \theta * (jkj) \\ C' &= C + \Lambda_j + \Lambda_k \end{aligned}$$

$$D' \quad = \quad D + \Lambda_j + \Lambda_k$$

It is then straightforward to show that $R' = C'\theta' + D'$. The induction yields a $Q' \in C^l$ with lower blocks C', D' such that

$$\theta' * (j_1 k_1 j_1 \ldots j_N k_N j_N) = Q'(\theta').$$

Using proposition 4.16, we calculate Q_{jk} s.t. $g_{jk}(\theta) = Q_{jk}(\theta)$. Then

$$\theta' * (jkj\ j_1 k_1 j_1 \ldots j_N k_N j_N) = (Q' Q_{jk})(\theta)$$

and a last calculation shows that $Q = Q' Q_{jk}$ has lower blocks C and D. This proves part B of the theorem. □

The main result of this section is now an immediate corollary of theorem 4.17 and proposition 4.2:

Corollary 4.18 *Let $\theta \in \Theta$ and let $Q \in C_n^l$ such that $\theta \in$ dom(Q). Then there exists a word m on $\{1, \ldots, n\}$ such that $Q(\theta) = \theta * m$.*

Proof: Let

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l \tag{4.71}$$

such that $\theta \in$ dom(Q). As $C\theta + D$ is an invertible element of $\mathbb{T}$, theorem 4.17(ii) can be applied, yielding a $Q_0 \in C_n^l$ with lower blocks C and D, and a word m such that $\theta \in$ dom(Q_0) and

$$\theta * m = Q_0(\theta),$$

As Q and Q_0 have the same lower blocks C and D and θ is in both of their domains, it follows from proposition 4.16 that $Q_0 = Q$ and the result follows. □

Corollary 4.19 *Two graph states $|G\rangle$ and $|G'\rangle$ are LC equivalent if and only if the graphs G an G' are locally equivalent.*

This result concludes our translation of the fractional linear transformations (4.7) into graph transformation rules. Note that this result makes it possible to generate the entire LC equivalence class of a graph state by a successive application of the local complementation rule. An example of this is given in Fig. 4.2.

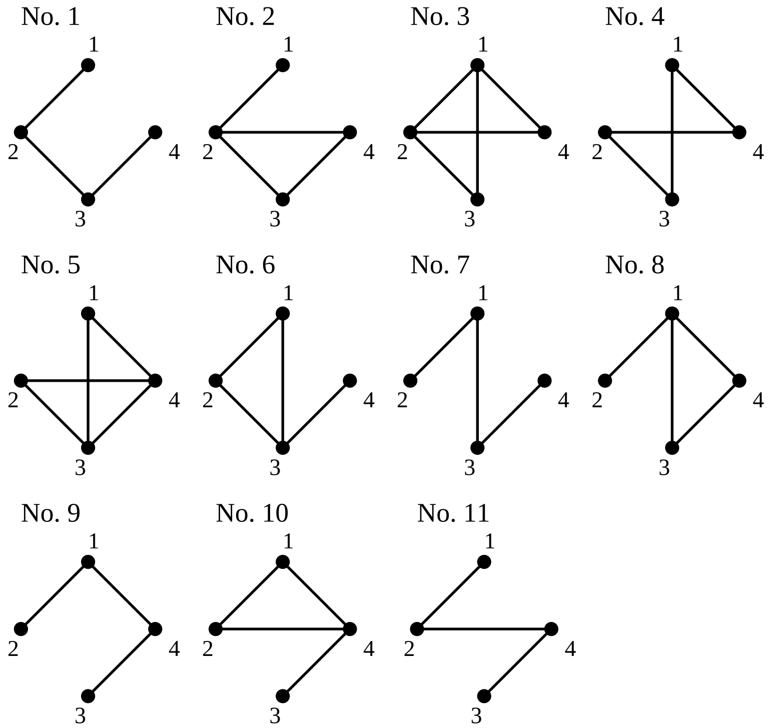

Figure 4.2: [25] Example of a successive application of local complementation, generating the entire local equivalence class of graph No. 1. Local complementation is performed w.r.t. that vertex of the predecessor which is written above the arrows in the following diagram:

$$\text{No. } 1 \xrightarrow{3} \text{No. } 2 \xrightarrow{2} \text{No. } 3 \xrightarrow{3} \text{No. } 4 \xrightarrow{1} \text{No. } 5 \xrightarrow{3} \text{No. } 6$$
$$\xrightarrow{1} \text{No. } 7 \xrightarrow{3} \text{No. } 8 \xrightarrow{4} \text{No. } 9 \xrightarrow{1} \text{No. } 10 \xrightarrow{2} \text{No. } 11$$

4.6 Efficient algorithm to recognize LC equivalence

Having obtained the above translation of LC equivalence of graph states in terms of local equivalence of the corresponding graphs, one can turn to the graph theory literature and look for results that are interesting from our QIT point of view. Local complementation of graphs has indeed been studied in quite some detail (see [3] and refs therein). One key result for our study is Ref. [2], where an efficient algorithm to recognize local equivalence of graphs is presented. We repeat this algorithm in this section.

Let G, G' be two graphs with adjacency matrices θ, $\theta' \in \Theta_n$, respectively. Recall that G and G' are locally equivalent if and only if there exists an operator

$$Q = \left[\begin{array}{cc} A & B \\ C & D \end{array} \right] \in C_n^l \tag{4.72}$$

such that

$$\left[\begin{array}{cc} \theta & I \end{array} \right] Q^T P \left[\begin{array}{c} \theta' \\ I \end{array} \right] = 0, \tag{4.73}$$

which is equivalent to

$$\theta' C \theta + A\theta + \theta' D + B = 0. \tag{4.74}$$

When θ and θ' are given, (4.74) is in fact a system of linear equations in the unknown matrices A, B, C, D, together with the additional quadratic constraints

$$AD + BC = I. \tag{4.75}$$

More explicitly, denoting the diagonal entries of A, B, C, D by a_i, b_i, c_i, d_i, respectively, (4.74) is the system of n^2 linear equations

$$\left(\sum_{i=1}^{n} \theta_{ij} \theta'_{ik} c_i \right) + \theta_{jk} a_k + \theta'_{jk} d_j + \delta_{jk} b_j = 0, \tag{4.76}$$

for all $j,\ k = 1, \ldots, n$, where the $4n$ unknowns a_i, b_i, c_i, d_i must satisfy the constraints

$$a_i d_i + b_i c_i = 1. \tag{4.77}$$

The set $\mathcal{V}$ of solutions to the linear equations (4.76), with disregard of the constraints, is a linear subspace of $\mathbb{F}_2^{4n}$. A basis $B = \{b_1, \ldots, b_d\}$ of $\mathcal{V}$ can be calculated efficiently in $\mathcal{O}(n^4)$ time by standard Gauss elimination over $\mathbb{F}_2$. Then we can search the space $\mathcal{V}$ for a vector which satisfies the constraints (4.77). As (4.76) is for large n a highly overdetermined system of equations, the space $\mathcal{V}$ is typically low-dimensional. Therefore, in the majority of cases this method gives a quick response. Nevertheless, in general one cannot exclude that the dimension of $\mathcal{V}$ is of order $\mathcal{O}(n)$ and therefore the overall complexity of this approach is nonpolynomial. However, it was shown in [2] that it is sufficient to enumerate a specified subset $\mathcal{V}' \subseteq \mathcal{V}$ with $|\mathcal{V}'| = \mathcal{O}(n^2)$ in order to find a solution which satisfies the constraints, if such a solution exists. Indeed, the following lemma holds:

Lemma 4.20 *[2] If dim($\mathcal{V}$) > 4, then the system (4.76)-(4.77) of linear equations plus constraints has a solution if and only if the set*

$$\mathcal{V}' := \{b + b' \mid b, b' \in B\} \subseteq \mathcal{V}$$

contains a vector which satisfies the constraints.

The proof of lemma 4.20 makes extensive use of local complementation. It is however quite involved and beyond the scope of this dissertation. The interested reader is referred to ref. [2] for the details.

Lemma 4.20 shows that, if a solution to (4.76)-(4.77) exists, this solution can be found by enumerating either all $|\mathcal{V}| \leq 16$ elements of $\mathcal{V}$ if $\dim(\mathcal{V}) \leq 4$ or the $\mathcal{O}(n^2)$ elements of $\mathcal{V}'$ if $\dim(\mathcal{V}) > 4$ and checking these vectors against the constraints (4.77). Hence, a polynomial time algorithm to check the solvability of (4.76)-(4.77) is obtained. The overall complexity of the algorithm is $\mathcal{O}(n^4)$. Note that, whenever LC equivalence occurs, the algorithm produces a solution

$$(a_1, b_1, c_1, d_1, \ \ldots, \ a_n, b_n, c_n, d_n) \tag{4.78}$$

to (4.76)-(4.77) which immediately yields an operator $Q \in C_n^l$ such that $Q(\theta) = \theta'$.

It is also important to remark that the above algorithm provides an efficient approach to recognize LC equivalence between two arbitrary stabilizer states (i.e., not necessarily graph states). Indeed, we have seen in chapter 3 that any stabilizer state is LC equivalent to a graph state. Moreover, such an LC equivalent graph state can be found in polynomial time; the proof of theorem 3.15 indeed yields a construction to transform any generator matrix into a generator matrix of the form $[\theta\ I]^T$ and this construction essentially depends on pivoting methods, which can be implemented efficiently. Hence an efficient algorithm to recognize LC equivalence of two arbitrary stabilizer states is obtained.

4.7 Pauli measurements as graph transformations

The notion of local complementation also allows us to elegantly describe how graph states are transformed under the action of local Pauli measurements; recall that this is of interest in the $QC_{\mathcal{C}}$ model.

First we need some notations. As before, let $G = (V, E)$ a graph on the vertex set $V = \{1, \ldots, n\}$ with adjacency matrix $\theta \in \Theta_n$. For any vertex $i \in V$, we define

$$G - i \equiv G[V \setminus \{i\}], \tag{4.79}$$

i.e., $G - i$ is the subgraph of G induced[2] by the $n-1$ vertices $V \setminus \{i\}$; hence, $\theta(G-i) \in \Theta_{n-1}$. We also refer to section 2.5 for a study of the effect of the measurement of a Pauli operator on a general stabilizer state.

Let $|G\rangle$ be the graph state on n qubits defined by G. Let us first consider the effect of a σ_z-measurement on the ith qubit, where $i \in \{1, \dots, n\}$. In complete analogy with (2.93), one can show the following:

Proposition 4.21 *Let G be a graph on n vertices. Measuring the operator $\sigma_z^{(i)}$, where $i = 1, \dots, n$, transforms $|G\rangle$ to a state of the form $|a\rangle \otimes M|G-i\rangle$, where $|a\rangle$ is a one-qubit stabilizer state and $M \in \mathcal{G}_{n-1}$.*

Proposition 4.21 show that performing a σ_z-measurement on the ith qubit of a graph state simply corresponds to deleting the vertex i in the corresponding graph. In order to obtain analogous results for σ_x- and σ_y-measurements, the notion of local complementation will prove very useful. Consider e.g. a σ_y-measurement on the first qubit, transforming $|G\rangle$ to $\frac{1}{2}(I \pm \sigma_y \otimes I)|G\rangle$. We now recall that the transformation $G \mapsto G * 1$ can be realized as a fractional linear transformation $\theta \mapsto \theta * 1 = Q_1(\theta)$, where

$$Q_1 = \begin{bmatrix} I & \mathrm{diag}(\theta_1) \\ \Lambda_1 & I \end{bmatrix} \in C_n^l, \tag{4.80}$$

where θ_1 is the first column of θ. Now, let $V \in \mathcal{C}_n^l$ be any local Clifford operation corresponding to Q_1 as defined in proposition 3.8. Observe that

$$Q_1 e_1 = e_1 + e_{n+1}, \quad Q_1(e_1 + e_{n+1}) = e_1 \tag{4.81}$$

and therefore

$$V\sigma_z^{(1)}V^\dagger = \pm\sigma_y^{(1)}, \quad V\sigma_y^{(1)}V^\dagger = \pm\sigma_z^{(1)} \tag{4.82}$$

and we see that V interchanges σ_z and σ_y on the first qubit. We now write $\frac{1}{2}(I \pm \sigma_y \otimes I)|G\rangle$ as follows:

$$\frac{1}{2}(I \pm \sigma_y \otimes I)|G\rangle = V^\dagger \left\{ \frac{1}{2}(I \pm \sigma_z \otimes I)V|G\rangle \right\}. \tag{4.83}$$

Note that $V|G\rangle$ is a graph state defined by the graph $G * 1$ from the definition of V. Using proposition 4.21, one then arrives at the following result:

Proposition 4.22 *Let G be a graph on n vertices. Measuring the operator $\sigma_y^{(i)}$, where $i = 1, \dots, n$, transforms $|G\rangle$ to a state of the form $|a\rangle \otimes U|(G*i)-i\rangle$, where $|a\rangle$ is a one-qubit stabilizer state and $U \in \mathcal{C}_{n-1}$.*

In a completely analogous way, one can also show:

[2] see section 4.5 for the definition of induced subgraph

Proposition 4.23 *Let G be a graph on n vertices. Let $i \in \{1, \ldots, n\}$ be a vertex of G and let $j \in N(i)$ be one of its neighbors. Measuring the operator $\sigma_x^{(i)}$ transforms $|G\rangle$ to a state of the form $|a\rangle \otimes U|(G * j * i) - i\rangle$, where $|a\rangle$ is a one-qubit stabilizer state and $U \in \mathcal{C}_{n-1}$.*

Propositions 4.21, 4.22 and 4.23 were proven in [25]. The above results show that local Pauli measurements on graph states can completely be described in terms of two elementary operations, namely the local complementation rule $G \mapsto G * i$ and the deletion of vertices $G \mapsto G - i$.

4.8 Conclusion

In this chapter we have studied LC equivalence of graph states in detail. Our research consisted of two main parts. In a first part we investigated LC equivalence of graphs states from an algebraic point of view, translating the problem in terms linear fractional transformations of adjacency matrices. This approach enabled us to obtain a formula for the number of graph states in an LC equivalence class. Secondly, we gave a translation of LC equivalence of graph states in terms of local complementation of graphs, thereby translating the problem in purely graph theoretical terms. This yielded an efficient algorithm to recognize LC equivalence of stabilizer states.

It should be noted that local equivalence of graphs has been studied by Bouchet in the context of certain algebraic and combinatorial structures called *isotropic systems*. Several remarks regarding these isotropic systems are in order. Firstly, there appears to be a very strong similarity between isotropic systems and the binary vector spaces that we have denoted by C_S. In fact, we strongly believe that our binary formulation of LC equivalence of stabilizer states, where spaces C_S and $C_{S'}$ are related by a linear transformation $Q \in C_n^l$, is completely equivalent to the theory of isotropic systems that is presented in the above references. However, at the time of writing this dissertation, our investigations on this probable equivalence of descriptions were only in a beginning stage and were not ready for publication. This research is however ongoing. What is more, it is not clear whether the description of local equivalence of graphs in terms of the fractional linear transformations (4.7) is known to graph theorists. Be this the case or not, this results enables one to calculate some interesting quantities related to local complementation, such as $|\mathrm{LC}(G)|$, in a quite straightforward manner − see section 4.3. We feel that the corresponding combinatorial calculations using only local complementation are much harder to complete and much less insightful. Therefore, it could be an interesting open subject to study the transformations (4.7) in more detail and look for results that are relevant from a purely graph theoretic point of view.

To conclude this chapter, we repeat the different characterizations of LC equivalence of graph states:

Theorem 4.24 *Let $G = (V, E)$, $G' = (V, E')$ be two graphs on n vertices with adjacency matrices θ, $\theta' \in \Theta_n$, respectively. Denote $S^T = [\theta\ I]^T$ and $S'^T = [\theta'\ I]^T$. Then the following are equivalent:*

(i) the states $|G\rangle$ and $|G'\rangle$ are LC equivalent;

(ii) there exist $Q \in C_n^l$ and $R \in GL(n, \mathbb{F}_2)$ such that $QSR = S'$;

(iii) there exists $Q \in C_n^l$ such that $S'^T PQS = 0$;

(iv) there exists $Q \in C_n^l$ such that $\theta \in$ dom(Q) and $Q(\theta) = \theta'$.

(v) the graphs G and G' are locally equivalent, i.e., there exists a word m on V such that $G * m = G'$.

References

Essentially all results in this chapter are our own work (sections 4.2 - 4.6). They are the subject of Refs. [47] and [45]. We note that we have not published the results in section 4.3 before.

After publishing Ref. [47], it came to our attention that Glynn has shown independently, in a paper preceding our work, that that two graph states are LC equivalent if and only if their corresponding graphs are locally equivalent [17]; the mathematical setting of his work is entirely different from ours and he makes no reference of fractional linear transformations of adjacency matrices. Finally, for a detailed study of local complementation of graphs and the related notion of isotropic systems we refer to the work of Bouchet, see [3, 2] and references therein.

Chapter 5

Local invariants

5.1 Introduction

This chapter is concerned with the characterization of the local equivalence class of a stabilizer state or code by means of local *invariants*. These are complex functions $F(\rho_{\mathcal{S}})$, where $\rho_{\mathcal{S}}$ is an arbitrary n-qubit stabilizer state or code, which remain invariant under the action of all elements in a group $\mathcal{L}$ of local operators, i.e.,

$$F(\rho_{\mathcal{S}}) = F(U\rho_{\mathcal{S}}U^{\dagger}) \tag{5.1}$$

for every $U \in \mathcal{L}$. As we are interested in LC operations on the one hand and general LU operations on the other hand, we will consider $\mathcal{L}$ to be either the local unitary group $U(2)^{\otimes n}$ or the local Clifford group $\mathcal{C}_n^l$. In studying local invariants, the general goal is to look for a *complete* set of invariants, i.e., a set of functions $\{F_1, F_2, \dots\}$ such that two stabilizer states or codes $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ are related by an operation in $\mathcal{L}$ if and only if $F_i(\rho_{\mathcal{S}}) = F_i(\rho_{\mathcal{S}'})$ for every i. Note that a complete set of invariants determines a given state or code up to an operation in $\mathcal{L}$. To obtain complete sets of invariants, we will use different techniques as we are dealing with either the local unitary or the local Clifford group. In the latter case we can work in the binary stabilizer formalism, and some ad hoc methods will in fact suffice to obtain a finite complete set of LC invariants of stabilizer states and codes. General local unitary operations, however, cannot be described within the binary stabilizer formalism, and we will therefore need more general techniques to study LU invariants. These techniques are found in a branch of mathematics called invariant theory. Our main goal will be to use the available general methods to construct LU invariants and see how these invariants translate into the binary stabilizer framework, when applied to the specific case of a stabilizer state or code.

A central notion in our study of both LC and LU invariants is that of *support* of a Pauli operator. Recall that the support $\text{supp}(\sigma_v)$ of a Pauli operator, where $v \in \mathbb{F}_2^{2n}$, is defined as the subset of those $i \in \{1, \dots, n\}$ such that

$(v_i, v_{n+i}) \neq (0,0)$. We will also transfer the notion of support to the binary formalism, employing the definition $\text{supp}(v) := \text{supp}(\sigma_v)$. As we will show in the following, both LU as LC invariants of stabilizer states and codes correspond to dimensions of certain subspaces of $C_S \times \cdots \times C_S$ that are defined in terms of constraints on the supports of their elements. Not only will this achieve a complete description of invariants within the binary stabilizer formalism, but this also shows a close relation between LU and LC invariants of stabilizer states and codes. We will elaborate on this this issue below.

This chapter is organized as follows: in section 5.2 we discuss LC invariants of stabilizer states and codes. Using the binary formalism, we give some examples of simple but important invariants and discuss their relevance from a QIT point of view. We then generalize this set of invariants and obtain a finite complete set of LC invariants of stabilizer states and codes. In section 5.3 we turn to LU invariants. We first state the relevant known results in invariant theory and then apply these results to the problem at hand. Eventually, we end up with a description of LU invariants within the binary stabilizer framework. We finally discuss the similarities between the obtained sets of LU and LC invariants.

5.2 LC invariants

In this section we study and characterize the LC equivalence class of an arbitrary stabilizer state using LC invariants.

5.2.1 Stabilizer states

A complex function F on the set of stabilizer states on n qubits is called an LC invariant function, or simply *LC invariant*, if

$$F(U\rho_\psi U^\dagger) = F(\rho_\psi) \tag{5.2}$$

for every stabilizer state $|\psi\rangle$ on n qubits and for every local Clifford operation $U \in \mathcal{C}_n^l$. Note that an LC invariant can only depend on the generator matrix of a stabilizer state. Indeed, a stabilizer state is, up to information concerning the overall phases of its stabilizer elements, completely determined by a generator matrix. Moreover, these phases do not play a role in determining the LC equivalence class of a stabilizer state, as was shown in corollary 3.12. Therefore, an LC invariant can be regarded as a complex function $\tilde{F}$ on the set of all $2n \times n$ generator matrices satisfying

$$\tilde{F}(QSR) = \tilde{F}(S) \tag{5.3}$$

for every $S \in \mathbb{F}_2^{2n\times n}$ satisfying $S^T PS = 0$, for every $Q \in C_n^l$ and $R \in GL(n, \mathbb{F}_2)$.

We start by considering some simple but important invariants. Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix S and let C_S be the n-dimensional column space of S as before. We have seen in chapter 2 that the number

$$B_\omega(\psi) \quad = \quad |\{v \in C_S \mid \text{supp}(v) \subseteq \omega\}| \tag{5.4}$$

is an LC invariant for every $\omega \subseteq \{1, \ldots, n\}$. Indeed, recall that

$$\text{rank } \rho_\omega(\psi) = 2^{|\omega|} B_\omega(\psi)^{-1}, \tag{5.5}$$

which shows that B_ω is invariant under all local unitary operations and it is therefore an LC invariant a fortiori. Of course, one can also directly see that B_ω is an LC invariant by simply noting that $\text{supp}(Qv) = \text{supp}(v)$ for every $v \in \mathbb{F}_2^{2n}$ and $Q \in C_n^l$, thereby showing that B_ω satisfies (5.3).

The invariants B_ω are related to a number of interesting physical quantities of the state $|\psi\rangle$. This is shown next:

Proposition 5.1 *Let $|\psi\rangle$ be a stabilizer state on n qubits and let $\omega \subseteq \{1, \ldots, n\}$. Then*

$$\begin{aligned} B_\omega(\psi) \quad &= \quad 2^{|\omega|} \; Tr\{\rho_\omega(\psi)^2\} && (5.6) \\ |\omega| - \log_2 B_\omega(\psi) \quad &= \quad - \; Tr\{\rho_\omega(\psi) \log_2 \rho_\omega(\psi)\} && (5.7) \end{aligned}$$

Proof: To show (5.6), note that

$$\rho_\omega(\psi)^2 = \frac{B_\omega(\psi)}{2^{|\omega|}} \rho_\omega(\psi) \tag{5.8}$$

from (2.15) and that $\text{Tr } \rho_\omega(\psi) = 1$. We now prove (5.7). Denoting by λ_i the nonzero eigenvalues of $\rho_\omega(\psi)$, we have

$$- \text{ Tr}\{\rho_\omega(\psi) \log_2 \rho_\omega(\psi)\} = - \sum_i \lambda_i \log_2 \lambda_i. \tag{5.9}$$

Since $\rho_\omega(\psi)$ is proportional to a projector and has rank $2^{|\omega|} B_\omega(\psi)^{-1}$, all nonzero eigenvalues are equal to $B_\omega(\psi)/2^{|\omega|}$ and we obtain

$$\begin{aligned} - \text{ Tr}\{\rho_\omega(\psi) \log_2 \rho_\omega(\psi)\} \quad &= \quad -\frac{2^{|\omega|}}{B_\omega} \frac{B_\omega}{2^{|\omega|}} \log_2 \frac{B_\omega}{2^{|\omega|}} \\ &= \quad - \log_2 B_\omega + |\omega|. && (5.10) \end{aligned}$$

□

The above proposition shows that the B_ωs are related to *bipartite* measures of entanglement, when partitioning the set $\{1, \ldots, n\}$ in two parties ω and $\bar{\omega}$: the number $B_\omega(\psi)$ is proportional to the *purity* $\text{Tr}\{\rho_\omega(\psi)^2\}$ of the subsystem $\rho_\omega(\psi)$; moreover, $- \log_2 B_\omega(\psi)$ is (up to an additive constant) the entropy of this subsystem, which is equal to the *entanglement* of the state $|\psi\rangle$ with respect to the bipartition $\{\omega, \bar{\omega}\}$.

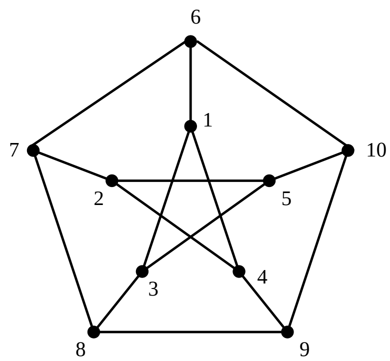

Figure 5.1: The Petersen graph. [24]

If $S = [\theta\ I]^T$ is the generator matrix of a graph state, recall that one can calculate $B_\omega(\psi)$ using the identity

$$\log_2 B_\omega(\psi) = |\omega| - \operatorname{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle \tag{5.11}$$

and therefore

$$-\operatorname{Tr}\{\rho_\omega(\psi)\log_2 \rho_\omega(\psi)\} = |\omega| - \log_2 B_\omega(\psi) = \operatorname{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle. \tag{5.12}$$

Expression (5.12) shows that the rank of the matrix $\theta\langle\omega\rangle$ measures the bipartite entanglement in the corresponding graph state according to the bipartition $\{\omega, \bar{\omega}\}$ of $\{1, \ldots, n\}$. Consequently, all information about the bipartite entanglement in a graph state (i.e., w.r.p. to all bipartitions) is contained in the function

$$c_G : \omega \subseteq \{1, \ldots, n\} \mapsto \operatorname{rank}_{\mathbb{F}_2}\ \theta\langle\omega\rangle. \tag{5.13}$$

Interestingly, the function c_G also appears in the work of Bouchet on locally equivalent graphs [3], where it is called the *connectivity function* of the graph G. Moreover, it was conjectured that the connectivity function constitutes a complete set of LC invariants, i.e., that the LC equivalence class of any graph state $|G\rangle$ is completely determined by the list of invariants $\{c_G(\omega)\}_\omega$. However, this has later been disproved by Fon-der-Flaas (see [3]), who showed that the Petersen Graph shown in Fig. 5.1, and the isomorphic graph obtained by exchanging the labels at each end of the five "spokes", no sequence of local complementations exists that transforms one graph into the other, although the connectivity functions of these graphs coincide.

In the following, we will study extensions of the set $\{c_G(\omega)\}_\omega$ to obtain a complete set of LC invariants.

Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix S. First we note that $B_\omega(\psi)$ is an invariant of the form

$$\sum_{v \in C_S} f(v), \tag{5.14}$$

where $f : \mathbb{F}_2^{2n} \to \mathbb{C}$ is a function satisfying

$$f(Qv) = f(v) \tag{5.15}$$

for every $v \in \mathbb{F}_2^{2n}$ and for every $Q \in C_n^l$. In the case of B_ω, f is equal to the function ϵ_ω, defined by

$$\epsilon_\omega(v) = \begin{cases} 1 & \text{if } \mathrm{supp}(v) \subseteq \omega \\ 0 & \text{otherwise.} \end{cases} \tag{5.16}$$

Note that any function f satisfying (5.15) takes on equal values on all elements in an orbit $\{Qv \mid Q \in C_n^l\}$, where $v \in \mathbb{F}_2^{2n}$. Since two vectors $v, v' \in \mathbb{F}_2^{2n}$ belong to the same orbit if and only if they have equal supports, $f(v)$ can only depend on $\mathrm{supp}(v)$. Defining the complex function δ_ω on $\mathbb{F}_2^{2n}$ by

$$\delta_\omega(v) = \begin{cases} 1 & \text{if } \mathrm{supp}(v) = \omega \\ 0 & \text{otherwise,} \end{cases} \tag{5.17}$$

it follows that $f(v) = \sum_\omega c_\omega\ \delta_\omega(v)$ for some coefficients $c_\omega \in \mathbb{C}$. Consequently, any LC invariant of the form (5.14) is a linear combination of the invariants $A_\omega(\psi)$, defined by

$$A_\omega(\psi) \quad = \quad |\{v \in C_S \mid \mathrm{supp}(v) = \omega\}|, \tag{5.18}$$

for every $\omega \subseteq \{1, \ldots, n\}$.

Remark. Note that the functions δ_ω are linearly independent. However, the corresponding functions A_ω are not. Indeed, one e.g. has the (trivial) identity $\sum_\omega A_\omega = 2^n$. We will encounter other linear dependencies between the A_ωs below. $\diamond$

Clearly, the invariants A_ω and B_ω have very similar definitions. Note that one trivially has

$$B_\omega = \sum_{\omega' \subseteq \omega} A_{\omega'}. \tag{5.19}$$

We will show that a converse relation, which writes the A_ωs as linear combinations of the B_ωs, also exists. This is done using the following lemma:

Lemma 5.2 *Let* $\omega \subseteq \{1, \ldots, n\}$. *Then*

$$\delta_\omega = \sum_{\omega' \subseteq \omega} (-1)^{|\omega| - |\omega'|} \epsilon_{\omega'}. \tag{5.20}$$

Proof: Firstly, note that $\delta_\omega = \epsilon_\omega \prod (1 - \epsilon_{\omega'})$, where the product has to be taken over all $\omega' \subseteq \omega$ satisfying $|\omega'| = |\omega| - 1$. Using the property $\epsilon_{\omega_1}\epsilon_{\omega_2} = \epsilon_{\omega_1 \cap \omega_2}$, we have

$$\epsilon_\omega \prod (1 - \ \epsilon_{\omega'}) \quad = \quad \epsilon_\omega \ - \sum_{\omega'} \ \epsilon_{\omega'}$$

$$+ \sum_{(\omega_1', \omega_2')} \epsilon_{\omega_1' \cap \omega_2'}$$
$$- \sum_{(\omega_1', \omega_2', \omega_3')} \epsilon_{\omega_1' \cap \omega_2' \cap \omega_3'} + \dots \tag{5.21}$$

where each sum $\sum_{(\omega_1', \dots, \omega_r')}$ runs over all r-tuples $(\omega_1', \dots, \omega_r')$ such that $\omega_i' \subseteq \omega$, $|\omega_i'| = |\omega| - 1$ and $\omega_i' \neq \omega_j'$, for every $i, j = 1, \dots, r$. A closer inspection reveals that

$$\sum_{(\omega_1', \dots, \omega_r')} \epsilon_{\omega_1' \cap \dots \cap \omega_r'} = \sum_{\substack{\omega' \subseteq \omega \\ |\omega'| = |\omega| - r}} \epsilon_{\omega'} \tag{5.22}$$

and the result follows. This ends the proof. □

Corollary 5.3 *Let $\omega \subseteq \{1, \dots, n\}$. Then*

$$A_\omega = \sum_{\omega' \subseteq \omega} (-1)^{|\omega| - |\omega'|} B_{\omega'}. \tag{5.23}$$

Corollary 5.4 *The functions ϵ_ω form a basis of the vector space of all functions $f : \mathbb{F}_2^{2n} \to \mathbb{C}$ satisfying (5.15).*

We have proven that the A_ωs are linear combinations of the B_ωs and vice versa. This shows that the sets of functions $\{A_\omega\}_\omega$ and $\{B_\omega\}_\omega$ span the same vector space and therefore these two lists of invariants contain the same nonlocal information.

Remark. Note that the $A_\omega(\psi)$s are much less manageable from a computational point of view than the $B_\omega(\psi)$s: the latter can efficiently be calculated through the identity (2.61), whereas an analogous expression for the A_ωs does not exist. ◇

Remark. The functions A_ω also play an important role in quantum coding theory, where one is interested in the quantities

$$A_d = \sum_{\omega,\ |\omega| = d} A_\omega, \tag{5.24}$$

for every $d = 1, \dots, n$. Recalling that the weight of a Pauli operator is the cardinality of its support, the number $A_d(\psi)$ counts the number of elements in the stabilizer $\mathcal{S}(\psi)$ with weight equal to d. The weight distribution $\{A_d\}_d$ is a central notion in coding theory, as it determines how many errors a code can correct. Moreover, it can be used to produce powerful bounds on how good codes can be. The interested reader is referred to Ref. [42] ◇

Remark. Using the identities

$$2^{n - |\omega|} B_{\bar{\omega}}(\psi)^{-1} = \text{rank } \rho_{\bar{\omega}}(\psi) = \text{rank } \rho_\omega(\psi) = 2^{|\omega|} B_\omega(\psi)^{-1}, \tag{5.25}$$

one arrives at the linear dependencies

$$2^{n-|\omega|}B_\omega - 2^{|\omega|}B_{\bar{\omega}} = 0 \tag{5.26}$$

$$2^{n-|\omega|}\sum_{\omega'\subseteq\omega} A_{\omega'} - 2^{|\omega|}\sum_{\omega\subseteq\omega'} A_{\omega'} = 0. \tag{5.27}$$

$\diamond$

Thus, we must conclude that our generalization of the LC invariants B_ω to the family (5.14) did not yield any essentially *new* invariants, since knowledge of the set $\{A_\omega(\psi)\}_\omega$ for any state $|\psi\rangle$ implies knowledge of the set $\{B_\omega(\psi)\}_\omega$ and vice versa. However, the form (5.14) allows for immediate generalizations, as one can now consider invariants of the form

$$F(\rho_\psi) = \sum_{v^1,\dots,v^r\in C_S} f(v^1,\dots,v^r), \tag{5.28}$$

where $r \in \mathbb{N}_0$ and $f : (\mathbb{F}_2^{2n})^{\times r} \to \mathbb{C}$ is a function satisfying

$$f(Qv^1,\dots,Qv^r) = f(v^1,\dots,v^r) \tag{5.29}$$

for every $v^1,\dots,v^r \in \mathbb{F}_2^{2n}$ and $Q \in C_n^l$. Note that the set of invariants (5.28) is a complex vector space for every r. Moreover, the set of all such invariants (i.e., for all r) is an algebra over $\mathbb{C}$, since this set is closed under taking products and linear combinations.

Analogous to the case $r = 1$ that we considered above, any function (5.29) takes on the same value within an orbit of the following action of C_n^l on $(\mathbb{F}_2^{2n})^{\times r}$:

$$Q \in C_n^l : (v^1,\dots,v^r) \mapsto (Qv^1,\dots,Qv^r). \tag{5.30}$$

Let $\{\gamma_1,\gamma_2,\dots\}$ denote the partition of $(\mathbb{F}_2^{2n})^{\times r}$ in these orbits and define the functions

$$\delta_{\gamma_i}(v^1,\dots,v^r) = \begin{cases} 1 & \text{if } (v^1,\dots,v^r)\in\gamma_i \\ 0 & \text{otherwise,}\end{cases} \tag{5.31}$$

for every $(v^1,\dots,v^r) \in (\mathbb{F}_2^{2n})^{\times r}$. It follows that $f = \sum_i c_{\gamma_i}\delta_{\gamma_i}$ for some complex coefficients c_i. Therefore, it is appropriate to investigate the structure of the orbits γ_i in more detail. We will do this next.

Let us first consider the case of one single qubit, i.e., $n = 1$. Noting that $C_1^l = GL(2,\mathbb{F}_2)$, we have the following action on $(\mathbb{F}_2^2)^{\times r}$:

$$Q \in GL(2,\mathbb{F}_2) : (a^1,\dots,a^r) \mapsto (Qa^1,\dots,Qa^r), \tag{5.32}$$

where $a^j = (a_1^j, a_2^j) \in \mathbb{F}_2^2$, for every $j = 1,\dots,r$. For each $a = (a^1,\dots,a^r) \in (\mathbb{F}_2^2)^{\times r}$, define the sets

$$\eta_0(a) \quad = \quad \{j|\ a^j = (0,0)\},$$

$$\begin{aligned}\eta_x(a) &= \{j|\ a^j = (0,1)\},\\ \eta_y(a) &= \{j|\ a^j = (1,1)\},\\ \eta_z(a) &= \{j|\ a^j = (1,0)\}.\end{aligned}$$

Then the following characterization is easily verified: two vectors $a, a' \in (\mathbb{F}_2^2)^{\times r}$ belong to the same orbit under the action (5.32) if and only if

(a) $\eta_0(a) = \eta_0(a')$ and

(b) there exists a permutation π of $\{x, y, z\}$ such that $\eta_x(a) = \eta_{\pi(x)}(a')$, $\eta_y(a) = \eta_{\pi(y)}(a')$, and $\eta_z(a) = \eta_{\pi(z)}(a')$.

This implies that any orbit Γ of the action (5.32) can completely be described by

(a') a set $\eta_0(\Gamma) \subseteq \{1, \ldots, r\}$ and

(b') a partition $\mathcal{P}(\Gamma) = \{\eta_1, \eta_2, \eta_3\}$ of $\{1, \ldots, r\} \setminus \eta_0(\Gamma)$ into three (possibly empty) subsets,

such that $a \in \Gamma$ if and only if $\eta_0(a) = \eta_0(\Gamma)$ and $\{\eta_x(a), \eta_y(a), \eta_z(a)\} = \mathcal{P}(\Gamma)$. Generalizing to multiple qubits, it follows that an orbit γ under the action (5.30) is characterized by an n-tuple $(\Gamma_1, \ldots, \Gamma_n)$ of orbits Γ_i of the action (5.32), such that $(v^1, \ldots, v^r) \in \gamma$ if and only if

$$(v_i^1, v_{n+i}^1, \ldots, v_i^r, v_{n+i}^r) \in \Gamma_i, \tag{5.33}$$

for every $i = 1, \ldots, n$. As every orbit Γ_i is characterized by a couple $(\eta_0(\Gamma_i), \mathcal{P}(\Gamma_i))$, we arrive at the following characterization of the orbits γ:

Proposition 5.5 *Let $n, r \in \mathbb{N}_0$. Let $\Gamma_1, \ldots, \Gamma_n$ be n orbits of the action (5.32) and let γ be the corresponding orbit of the action (5.30). For every $j, l \in \{1, \ldots, r\}$, $j < l$, define the sets ω^j and ω^{jl} by*

$$\begin{aligned}\omega^j &= \{i \in \{1, \ldots, n\} \mid j \in \eta_0(\Gamma_i)\}\\ \omega^{jl} &= \{i \in \{1, \ldots, n\} \mid j, l \in \eta_0(\Gamma_i) \textit{ or } j \textit{ and } l\\ &\qquad \textit{belong to the same element of } \mathcal{P}(\Gamma_i)\}.\end{aligned} \tag{5.34}$$

Let $(v^1, \ldots, v^r) \in (\mathbb{F}_2^{2n})^{\times r}$. Then $(v^1, \ldots, v^r) \in \gamma$ if and only if

$$supp(v^j) = \bar{\omega}^j, \qquad supp(v^j + v^l) = \bar{\omega}^{jl} \tag{5.35}$$

for every $j, l \in \{1, \ldots, r\}$, $j < l$, where $\bar{\omega}^j$, $\bar{\omega}^{jl}$ denote the complements of the sets ω^j, ω^{jl} in $\{1, \ldots, n\}$.

The proof of the above proposition is straightforward. It is also interesting to count the number of orbits γ of the action (5.30). In order to do so, we use the Cauchy-Frobenius orbit-counting lemma; recall that this states that the number of orbits of a finite group H acting on a set X is equal to the average number of fixed points, i.e., the number of orbits is equal to

$$\frac{1}{|H|}\sum_{h\in H}|\mathrm{Fix}(h)|, \tag{5.36}$$

where $|\mathrm{Fix}(h)|$ is the number of fixed points in the set X of the group element h. Let us first consider the case of one single qubit. We then have to calculate the number of fixed points of an arbitrary matrix $Q \in GL(2,\mathbb{F}_2)$ acting on $(\mathbb{F}_2^2)^{\times r}$. Firstly, it is trivial that the identity has $|(\mathbb{F}_2^2)^{\times r}| = 4^r$ fixed points. Secondly, there are three elements in $GL(2,\mathbb{F}_2)$ of order two. Consider e.g. the matrix

$$Q_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5.37}$$

When acting on $\mathbb{F}_2^2$, this operator fixes exactly two vectors, namely (0,0) and (1,1). Therefore, when Q_0 acts on $(\mathbb{F}_2^2)^{\times r}$, the set $\mathrm{Fix}(Q_0)$ consists of all vectors of the form

$$\alpha_1(1,1,0,0\ldots,0,0) \ + \ \alpha_2(0,0,1,1,\ldots,0,0) + \ \ldots \ + \ \alpha_r(0,0,0,0,\ldots,1,1), \tag{5.38}$$

where $\alpha_i \in \mathbb{F}_2$ for every $i = 1,\ldots,r$. Therefore, the cardinality of $\mathrm{Fix}(Q_0)$ is equal to 2^r. Note that an analogous argument holds for the other two matrices of order two. Finally, there are two elements in $GL(2,\mathbb{F}_2)$ of order three, which fix only the zero vector. Gathering these results in the formula (5.36), we find that the number of orbits under the action (5.32) is equal to $(4^r + 3\cdot 2^r + 2)/6$. Consequently, the number of orbits under the action (5.30) is equal to

$$\frac{1}{6^n}(4^r + 3\cdot 2^r + 2)^n. \tag{5.39}$$

Returning to our study of the functions (5.29) and the corresponding LC invariants (5.28), we have the following proposition:

Proposition 5.6 *Let $n, r \in \mathbb{N}_0$. Let $\Omega = (\omega^1, \omega^2, \ldots, \omega^{12}, \omega^{13,\cdots})$ be a tuple of sets $\omega^j, \omega^{jl} \subseteq \{1,\ldots,n\}$, for every $j, l = 1,\ldots,r$ with $j < l$. Define*

$$\delta^{\Omega}_{n,r} : (v^1,\ldots,v^r) \in (\mathbb{F}_2^{2n})^{\times r} \mapsto \left(\prod_{j=1}^{r}\delta_{\omega_j}(v^j)\right)\left(\prod_{j<l}\delta_{\omega_{jl}}(v^j+v^l)\right), \tag{5.40}$$

where $\omega^j, \omega^{jl} \subseteq \{1,\ldots,n\}$, for every $j,l \in \{1,\ldots,r\}$, $j<l$. Then any function $f : (\mathbb{F}_2^{2n})^{\times r} \to \mathbb{C}$ satisfying (5.29) is a linear combination of the functions $\{\delta^{\Omega}_{n,r}\}_{\Omega}$.

Proof: Let $\{\gamma_1, \gamma_2, \dots\}$ denote the partition of $(\mathbb{F}_2^{2n})^{\times r}$ in orbits and define the functions δ_{γ_i} as before. The result follows immediately by noting that for every γ_s ($s = 1, 2, \dots$) the function δ_{γ_s} can be written in the form (5.40) from proposition 5.5. This ends the proof. $\square$

Corollary 5.7 *Let $n, r \in \mathbb{N}_0$. Let $|\psi\rangle$ be a stabilizer state on n qubits and let Ω be a tuple of subsets of $\{1, \dots, n\}$ as in proposition 5.6. Let $A_{n,r}^{\Omega}(\psi)$ be the cardinality of the set*

$$\{(v^1, \dots, v^r) \in C_S^{\times r} |\ supp(v^i) = \omega^i,\ supp(v^i + v^j) = \omega^{ij},\ i, j = 1, \dots, r,\ i < j\}.$$

Then any invariant F of the form (5.28) is a linear combination of the invariants $\{A_{n,r}^{\Omega}\}_{\Omega}$.

Corollary 5.8 *Let $B_{n,r}^{\Omega}(\psi)$ be the cardinality of the set*

$$\{(v^1, \dots, v^r) \in C_S^{\times r} |\ supp(v^i) \subseteq \omega^i,\ supp(v^i + v^j) \subseteq \omega^{ij},\ i, j = 1, \dots, r,\ i < j\}.$$

Then any invariant F of the form (5.28) is a linear combination of the invariants $\{B_{n,r}^{\Omega}\}_{\Omega}$.

Proof: This immediately follows from the fact that every δ_ω can be written as a linear combination of the $\epsilon_{\omega'}$s. $\square$

Remark. Note that the nonzero[1] functions $\{\delta_{n,r}^{\Omega}\}_{\Omega}$ are linearly independent, as were the δ_ωs in the beginning of this section. Again, the corresponding LC invariants $A_{n,r}^{\Omega}$ are not linearly independent, since one e.g. has $\sum_{\Omega} A_{n,r}^{\Omega} = 2^{nr}$. $\diamond$

Thus, as in our study of the case $r = 1$ at the beginning of this section, we end up with two equivalent sets of LC invariants for every r. Both families of invariants correspond to cardinalities of subsets of the space $C_S^{\times r}$ and the notion of *support* is central in their definitions. As in the case $r = 1$, the $B_{n,r}^{\Omega}$s offer a computational advantage over the $A_{n,r}^{\Omega}$s, as every $B_{n,r}^{\Omega}(\psi)$ counts the number of elements in a *linear subspace* of $C_S^{\times r}$ – indeed, the sets (5.41) are vector spaces over $\mathbb{F}_2$. Consider e.g. the case $r = 2$: letting $\Omega = (\omega^1, \omega^2, \omega^{12})$ be a 3-tuple of subsets of $\{1, \dots, n\}$, one finds that $B_{n,2}^{\Omega}(\psi)$ is equal to the cardinality of the space of all couples $(x^1, x^2) \in (\mathbb{F}_2^n)^2$ satisfying

$$\begin{aligned} S\langle\bar{\omega}^1\rangle x^1 &= 0 \\ S\langle\bar{\omega}^2\rangle x^2 &= 0 \\ S\langle\bar{\omega}^{12}\rangle (x^1 + x^2) &= 0, \end{aligned} \tag{5.41}$$

[1]Note that not every tuple Ω can be obtained from an orbit γ as in proposition 5.5. For such Ω one has $\delta_{n,r}^{\Omega} \equiv 0$.

where $S\langle\cdot\rangle$ was defined in chapter 2.4.3.3. This cardinality is equal to that of the kernel of the matrix

$$\begin{bmatrix} S\langle\bar{\omega}^1\rangle & \cdot \\ \cdot & S\langle\bar{\omega}^2\rangle \\ S\langle\bar{\omega}^{12}\rangle & S\langle\bar{\omega}^{12}\rangle \end{bmatrix}, \tag{5.42}$$

which can be calculated efficiently.

Having obtained the above insights in the family (5.28) of LC invariants, it is natural to ask (i) whether this set is a complete family of LC invariants and (ii) if yes, whether one can provide upper bounds to how many invariants need to be considered in order to determine the LC equivalence class of an arbitrary stabilizer code. These questions are answered in the next proposition:

Proposition 5.9 *Let $|\psi\rangle$ be a stabilizer state on n qubits. Then the LC equivalence class of $|\psi\rangle$ is completely determined by the values of all invariants $\{A^{\Omega}_{n,n}(\psi)\}_{\Omega}$.*

Proof: To prove the result, let $|\psi\rangle$ and $|\psi'\rangle$ be two stabilizer states on n qubits such that $A^{\Omega}_{n,n}(\psi) = A^{\Omega}_{n,n}(\psi')$ for every tuple Ω as defined above. We will show that this implies that $|\psi\rangle$ and $|\psi'\rangle$ are LC equivalent. Let $|\psi\rangle$ and $|\psi'\rangle$ have generator matrices S, S', respectively. Fix a basis $\{v^1, \dots, v^n\}$ of C_S and define the tuple of sets $\Omega_* = (\omega^1_*, \dots, \omega^{12}_*, \dots)$ such that

$$\omega^j_* = \operatorname{supp}(v^j),\ \omega^{jl}_* = \operatorname{supp}(v^j + v^l), \tag{5.43}$$

for every $j, l = 1, \dots, n$ with $j < l$. It follows that $A^{\Omega_*}_{n,n}(\psi)$ is nonzero, and therefore $A^{\Omega_*}_{n,n}(\psi')$ is nonzero as well, since these numbers are equal by assumption. Therefore, there exist vectors $w^1, \dots, w^n \in C_{S'}$ such that

$$\operatorname{supp}(w^j) = \omega^j_*,\ \ \operatorname{supp}(w^j + w^l) = \omega^{jl}_*, \tag{5.44}$$

for every j, l. Expressions (5.43) and (5.44) show that the tuples $(v^1, \dots, v^n)$ and $(w^1, \dots, w^n)$ lie on the same orbit under the action of C^l_n on $(\mathbb{F}_2^{2n})^{\times n}$. Therefore, there is an operator $Q \in C^l_n$ such that $Qv^j = w^j$ for every $j = 1, \dots, n$. It follows that the space QC_S is spanned by the vectors $w^1, \dots, w^n$. Moreover, these vectors are linearly independent, as they are the images of a linearly independent set under an invertible linear transformation. Therefore, $\{w^1, \dots, w^n\}$ is a basis of $C_{S'}$ (since the latter is an n-dimensional vector space) and we obtain $QC_S = C_{S'}$. This proves the result. □

Corollary 5.10 *The LC equivalence class of $|\psi\rangle$ is completely determined by the values of all invariants $\{B^{\Omega}_{n,n}(\psi)\}_{\Omega}$.*

We have obtained a finite characterization of the LC equivalence class of an arbitrary stabilizer state. We note that the above result is to be regarded as an upper bound on the maximal r which needs to be considered in order to obtain a complete set of invariants. Indeed, it is likely that only invariants corresponding to (substantially) lower r need to be considered in order to recognize LC equivalence between two stabilizer states. One indication for this conjecture is the proof of proposition 5.9, which shows that all the information of the LC equivalence class of a given state $|\psi\rangle$ is in fact contained within a single invariant $A^{\Omega_*}_{n,n}(\psi)$. A second state $|\psi'\rangle$ is LC equivalent to $|\psi\rangle$ if and only if

$$A^{\Omega_*}_{n,n}(\psi') = A^{\Omega_*}_{n,n}(\psi), \tag{5.45}$$

(in fact, even $A^{\Omega_*}_{n,n}(\psi) > 0$ is sufficient) and the information in all other invariants is in fact redundant. It is not unlikely that there exist smaller complete lists of invariants (i.e. of smaller r) which exhibit less redundancies. We will continue this discussion in section 5.3.3.4.

5.2.2 Stabilizer codes

As for general stabilizer codes, we can be brief: essentially all definitions and results in this section have trivial generalizations to arbitrary stabilizer codes. The only difference between the stabilizer state case is that now the binary space C_S no longer has maximal dimension n. However, small changes in the relevant definitions and proofs suffice to incorporate this generalization. As an illustration, we state the generalization of proposition 5.9, and its proof, to the case of arbitrary stabilizer codes:

Proposition 5.11 *Let $\rho_{\mathcal{S}}$ be an $[n, k]$ stabilizer code. Then the LC equivalence class of $\rho_{\mathcal{S}}$ is completely determined by the values of all invariants $\{A^{\Omega}_{n,n-k}(\rho_{\mathcal{S}})\}_{\Omega}$.*

Proof: To prove the result, let $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ be two $[n, k]$ stabilizer codes such that $A^{\Omega}_{n,n-k}(\rho_{\mathcal{S}}) = A^{\Omega}_{n,n-k}(\rho_{\mathcal{S}'})$ for every tuple Ω as defined above. We will show that this implies that $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ are LC equivalent. Let $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ have generator matrices S, S', respectively. Fix a basis $\{v^1, \dots, v^{n-k}\}$ of C_S and define the tuple of sets $\Omega_* = (\omega^1_*, \dots, \omega^{12}_*, \dots)$ such that

$$\omega^j_* = \text{ supp}(v^j),\ \omega^{jl}_* = \text{ supp}(v^j + v^l), \tag{5.46}$$

for every $j, l = 1, \dots, n-k$ with $j < l$. It follows that $A^{\Omega *}_{n,n-k}(\rho_{\mathcal{S}})$ is nonzero, and therefore $A^{\Omega *}_{n,n-k}(\rho_{\mathcal{S}'})$ is nonzero as well, since these numbers are equal by assumption. Therefore, there exist vectors $w^1, \dots, w^{n-k} \in C_{S'}$ such that

$$\text{supp}(w^j) = \omega^j_*, \quad \text{supp}(w^j + w^l) = \omega^{jl}_*, \tag{5.47}$$

for every j, l. Expressions (5.46) and (5.47) show that the tuples $(v^1, \dots, v^{n-k})$ and $(w^1, \dots, w^{n-k})$ lie on the same orbit under the action of C^l_n on $(\mathbb{F}_2^{2n})^{\times(n-k)}$. Therefore, there is an operator $Q \in C^l_n$ such that $Qv^j = w^j$ for every $j =$

$1, \ldots, n-k$. It follows that the space QC_S is spanned by the vectors $w^1, \ldots, w^{n-k}$. Moreover, these vectors are linearly independent, as they are the images of a linearly independent set under an invertible linear transformation. Therefore, $\{w^1, \ldots, w^{n-k}\}$ is a basis of $C_{S'}$ (since the latter is an $n-k$-dimensional vector space) and we obtain $QC_S = C_{S'}$. This proves the result. □

5.3 LU invariants

We now move to the study of general LU invariants of stabilizer states. Recall that two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are called LU equivalent if there exists an operator $U \in U(2)^{\otimes n}$ such that $U\rho_\psi U^\dagger = \rho_{\psi'}$ for some $U \in U(2)^{\otimes n}$. A complex function F on the set of stabilizer states on n qubits is an LU invariant function, or simply *LU invariant*, if $F(U\rho_\psi U^\dagger) = F(\rho_\psi)$ for every $U \in U(2)^{\otimes n}$ and for every stabilizer state $|\psi\rangle$.

As was remarked before, LU operations on stabilizer states cannot be described within the binary stabilizer formalism and an approach to studying LU equivalence and LU invariants similar to the one we adopted in the previous section is not possible. Therefore, we will resort to general techniques for investigating LU invariants of arbitrary (pure or mixed) states, i.e., not necessarily stabilizer states or codes. We will repeat the known results concerning these general LU invariants and make the specification to the case where the states are stabilizer states (or codes).

Let us first recall the basic results concerning LU invariants of general states. It is well known that two arbitrary mixed states ρ and ρ' on n qubits are LU equivalent if and only if $F(\rho) = F(\rho')$ for every *polynomial* LU invariant F, which is a polynomial function in the entries of ρ [32]. Consequently, one studies the set of all complex polynomials $F(x) \equiv F(x_{11}, x_{12}, \ldots, x_{2^n 2^n})$, where x_{ij} are 2^{2n} variables which are assembled in a $2^n \times 2^n$ matrix $x = (x_{ij})$, such that $F(UxU^\dagger) = F(x)$ for every $U \in U(2)^{\otimes n}$. Such polynomials will also be called LU invariants. Note that the set of all LU invariants forms an algebra over $\mathbb{C}$, since linear combinations and products of invariants are again invariants. This algebra is called the invariant algebra[2] (or invariant ring) of $U(2)^{\otimes n}$. It is well known that the invariant algebra of $U(2)^{\otimes n}$ is finitely generated [43], i.e., a finite set of LU invariants $\{F_1, \ldots, F_m\}$ exists, such that any LU invariant F can be written as a polynomial in the invariants F_j ($j = 1, \ldots, m$). Consequently, two states ρ and ρ' are LU equivalent if and only if

$$F_j(\rho) = F_j(\rho'), \tag{5.48}$$

for every $j = 1, \ldots, m$, and knowledge of such a set of generators F_j constitutes a characterization of the LU equivalence class of any state. However, although

[2] In the literature the invariant algebra of a $N \times N$ matrix group G is usually defined as the set of all polynomials $p(x) = p(x_1, \ldots, x_N)$ in the variables x_i such that $p(Ax) = p(x)$ for every $A \in G$. Our definition is a variant of this.

the existence of such a finite generating set is guaranteed, an example is to date unknown. Since pinpointing a finite generating set of the invariant algebra of *any* matrix group is typically a hard problem, one generally relaxes the constraint that the generating set is to be finite. A standard approach is to study homogeneous polynomial invariants as follows: firstly, it is easy to see that any polynomial invariant is a sum of homogeneous invariants. Secondly, the set of all homogeneous invariants of a given degree is a finite-dimensional complex vector space. Therefore, an (infinite) generating set of the invariant algebra is obtained by constructing generating sets of each of these vector spaces of homogeneous invariants, and taking the union of these generating sets.

In the following, we repeat the known constructions of generating sets of homogeneous LU invariants (sections 5.3.1 - 5.3.2) and then evaluate the obtained set of polynomials in an arbitrary stabilizer state (or code). Our goal is to provide a translation of these invariants into the binary stabilizer formalism, with the aim of gaining insight in the structure of these invariants. We will conclude that these LU invariants bear great resemblance to the LC invariants that were considered in the previous section: the considered LU invariants also correspond to cardinalities of certain subsets (in fact: linear subspaces) of $C_S \times \cdots \times C_S$ that are defined through constraints on the supports of their elements (section 5.3.3). In some cases, the LU and LC invariants even coincide. This is discussed in section 5.3.4.

5.3.1 Invariant polynomials and matrix algebras

We first recall the basic background concerning (homogeneous) LU invariants. Let $x = (x_{ij})$ be a $2^n \times 2^n$ matrix of variables. Any homogeneous polynomial $F(x)$ of degree $r \in \mathbb{N}_0$ can be written as a trace

$$F(x) = \text{Tr}\ (A_F \cdot x^{\otimes r}) \tag{5.49}$$

for some complex $2^{nr} \times 2^{nr}$ matrix A_F. To see this, simply note that the tensor product $x^{\otimes r}$ contains all monomials of degree r in the entries x_{ij}. The coefficients of these monomials in the polynomial F are encoded in the entries of A_F (note, however, that the correspondence $F \leftrightarrow A_F$ is not one-to-one, i.e., the map $A_F \rightarrow F(\rho) = \text{Tr}(A_F \cdot \rho^{\otimes r})$ is not injective). One obtains the following characterization of LU invariants F in terms of the corresponding matrices A_F:

Proposition 5.12 *[22] Let $n, r \in \mathbb{N}_0$ and let $F(x)$ be a complex polynomial of degree r in 2^{2n} variables $x = (x_{ij})$. Then F is an LU invariant if and only if there exists a $2^{nr} \times 2^{nr}$ matrix A_F such that (5.49) holds and*

$$\left[U^{\otimes r}, A_F\right] = 0 \tag{5.50}$$

for every $U \in U(2)^{\otimes n}$.

Proof: The backward implication is trivial. We show the forward implication. Let $F(x)$ be a homogeneous invariant of $U(2)^{\otimes n}$ of degree r and let $\tilde{A}_F$ be a $2^{nr} \times 2^{nr}$ matrix such that $F(x) = \text{Tr}\ (\tilde{A}_F \cdot x^{\otimes r})$. As F is an LU invariant, we have

$$\begin{aligned} F(x) &= \int_{U(2)^{\otimes n}} dU\ F(UxU^\dagger) \\ &= \int_{U(2)^{\otimes n}} dU\ \ \text{Tr}(U^\dagger \tilde{A}_F U x^{\otimes r}) \\ &= \text{Tr}\ (A_F \cdot x^{\otimes r}), \end{aligned} \tag{5.51}$$

where dU is the normalized invariant integration measure of $U(2)^{\otimes n}$, and where we have used the definition

$$A_F := \int_{U(2)^{\otimes n}} dU\ U^\dagger \tilde{A}_F U. \tag{5.52}$$

The result follows by noting that A_F satisfies (5.50). This ends the proof. □

Proposition 5.12 shows that the study of homogeneous LU invariants of $U(2)^{\otimes n}$ of fixed degree r is transformed into the study of the algebra $\mathcal{A}_{n,r}$ of matrices A_F which satisfy (5.50). The general goal is now to construct, for every $r \in \mathbb{N}_0$, bases of matrices $\{A_1^r, \ldots, A_{m_r}^r\}$ (where $m_r \in \mathbb{N}_0$) that linearly generate $\mathcal{A}_{n,r}$. The corresponding polynomials $\text{Tr}(A_j^r \cdot \rho^{\otimes r})$ $(j = 1, \ldots, m_r)$ then linearly generate the space of homogeneous invariants of degree r. Note that these polynomials are generally *not* linearly independent. This is due to the fact that the correspondence $F \leftrightarrow A_F$ in (5.49) is not one-to-one.

Bases of the spaces $\mathcal{A}_{n,r}$ will be constructed in the next section.

5.3.2 Invariants, permutations and binary trees

In this section we repeat the construction of bases of the spaces $\mathcal{A}_{n,r}$ that was presented in Refs. [22] and [37].

Fix $r \in \mathbb{N}_0$. We first consider the case of one single qubit, i.e., we consider the algebra $\mathcal{A}_{1,r}$ of all $2^r \times 2^r$ matrices A satisfying

$$\left[U^{\otimes r}, A\right] = 0 \tag{5.53}$$

for every $U \in U(2)$. It was shown in Ref. [37] that a set of matrices that linearly generate this algebra can be obtained in a one-to-one correspondence with the permutation group S_r on r letters as follows: let $\pi \in S_r$ be a permutation of the set $\{1, \ldots, r\}$. The $2^r \times 2^r$ matrix T_r^π is defined as the permutation matrix which acts on $(\mathbb{C}^2)^{\otimes r}$ by permuting the r copies of $\mathbb{C}^2$ according to the permutation π, i.e., T_r^π is defined by

$$T_r^\pi |i_1 i_2 \ldots i_r\rangle = |i_{\pi(1)} i_{\pi(2)} \ldots i_{\pi(r)}\rangle, \tag{5.54}$$

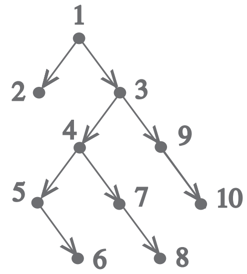

Figure 5.2: Binary tree on 10 nodes with maximal right paths $(1, 3, 9, 10)$, (2), $(4, 7, 8)$ and $(5, 6)$. Note the canonical way in which the nodes are labelled.

for every $i_1, \ldots, i_r \in \{0, 1\}$. The matrices $\{T_r^\pi\}_{\pi \in S_r}$ linearly generate $\mathcal{A}_{1,r}$. However, linear dependencies between the matrices T_r^π do exist and therefore this generating set is not minimal. In Ref. [22] a method was presented to pinpoint within the set $\{T_r^\pi\}_\pi$ a linearly independent subset, for every $r \in \mathbb{N}_0$. The approach was to consider *binary trees* and to associate with every binary tree B on r nodes a permutation $\pi_B \in S_r$. Enumeration of all possible permutations π_B, and hence permutation matrices $T_r^{\pi_B}$, yields a linearly independent subset of permutation matrices. We now repeat the details of this construction.

A (labelled, ordered and connected) binary tree B on r vertices is a special instance of a simple, oriented and connected graph, i.e. it consists of a set of vertices or nodes $V = \{1, \ldots, r\}$ which can be connected by arrows according to a number of prescriptions. If there is an arrow from a node $f \in V$ to a node $s \in V$ then f is called the father of s and, conversely, s is a son of f. In a binary tree, all nodes but one have exactly one father. The one node without father is called the root of the tree. Furthermore, every node has at most two sons (called left and right son, respectively). The labelling of the r nodes is obtained by traversing the tree in the order root - left subtree - right subtree. A *maximal right path* p in a binary tree B is an ordered tuple of nodes $p = (v_0, v_1, \ldots, v_s)$ such that v_0 is not the right son of any node of B, v_i is the right son of v_{i-1} for $i = 1, \ldots, s$ and v_s has no right son. An example of a labelled binary tree is given in Fig. 5.2.

Denoting by $\mathcal{R}(B)$ the set of all maximal right paths of B, the permutation π_B associated with the binary tree B is defined by the product of cycles

$$\pi_B = \prod_{(v_0, v_1, \ldots, v_s) \in \mathcal{R}(B)} (v_0 v_1 \ldots v_s).$$

Note that $\pi_B \in S_r$ whenever B has exactly r nodes and that there is a one-to-one correspondence between B and π_B. The set of all permutations obtained in this way is denoted by $\mathcal{P}_r$. According to the result in [22], the matrices $\{T_r^\pi\}_{\pi \in \mathcal{P}_r}$ form a vector space basis of the algebra $\mathcal{A}_{1,r}$.

For arbitrary n, the above result can immediately be used to construct a basis of $\mathcal{A}_{n,r}$. To see this, let us first consider the algebra of $2^{nr} \times 2^{nr}$ matrices

A that satisfy

$$U_1^{\otimes r} \otimes \cdots \otimes U_n^{\otimes r} A (U_1^{\otimes r} \otimes \cdots \otimes U_n^{\otimes r})^\dagger = A, \tag{5.55}$$

for every $U_1, \ldots, U_n \in U(2)^{\otimes n}$. It is straightforward to show that this algebra is the n-fold tensor product of $\mathcal{A}_{1,r}$ with itself. Therefore, a basis of this algebra is given by the matrices $T_r^{\pi_1} \otimes \cdots \otimes T_r^{\pi_n}$, where π_i ranges over permutations in $\mathcal{P}_r$, for every $i = 1, \ldots, n$. In order to obtain a basis of $\mathcal{A}_{n,r}$, one simply has to conjugate this basis with the permutation matrix $P_{n,r}$, defined by

$$\begin{aligned} &P_{n,r}\ |i_{11} \ldots i_{1r}; i_{21} \ldots i_{2r}; \ldots; i_{n1} \ldots i_{nr}\rangle \\ &= |i_{11} \ldots i_{n1}; i_{12} \ldots i_{n2}; \ldots; i_{1r} \ldots i_{nr}\rangle, \end{aligned} \tag{5.56}$$

where $i_{ab} \in \{0, 1\}$. Indeed, the matrix $P_{n,r}$ performs the appropriate permutation of tensor factors, mapping $U_1^{\otimes r} \otimes \cdots \otimes U_n^{\otimes r}$ to $(U_1 \otimes \cdots \otimes U_n)^{\otimes r}$ under conjugation. This leads to the following result:

Theorem 5.13 *Let $n, r \in \mathbb{N}_0$. Then the matrices*

$$T_{n,r}^{\Pi} := P_{n,r}\,(T_r^{\pi_1} \otimes \cdots \otimes T_r^{\pi_n})\,P_{n,r}^T, \tag{5.57}$$

where $\Pi = (\pi_1, \ldots, \pi_n)$ ranges over all n-tuples of permutations $\pi_i \in \mathcal{P}_r$, form a basis of the set $\mathcal{A}_{n,r}$.

Note that $T_{n,r}^{\Pi}$ is a $2^{nr} \times 2^{nr}$ permutation matrix which acts on $(\mathbb{C}^{2^n})^{\otimes r}$ by permuting the r copies of the ith qubit according to the ith permutation π_i, for every $i = 1, \ldots, n$.

Therefore, a generating set of basic invariants is obtained as follows:

Corollary 5.14 *The LU invariants*

$$I_{n,r}^{\Pi}(x) := Tr\ (T_{n,r}^{\Pi} \cdot x^{\otimes r}), \tag{5.58}$$

where $\Pi = (\pi_1, \ldots, \pi_n)$ ranges over all n-tuples of permutations $\pi_i \in \mathcal{P}_r$, form a generating set of the vector space of LU invariants of $U(2)^{\otimes n}$ of degree r.

To conclude this section, we state some definitions regarding binary trees that will be used below. Let B be a binary tree on r nodes. The *start* $\mathrm{st}(p)$ of a path $p = (v_0, v_1, \ldots, v_s) \in \mathcal{R}(B)$ is the element v_0 and the *finish* $\mathrm{fin}(p)$ is the element v_s. The *length* of p is the number $s + 1$. By an expression of the form "$i \in p$"is meant that the node i belongs to the set $\{v_0, v_1, \ldots, v_s\}$ (note that, due to the canonical labelling of the nodes, there is a one-to-one correspondence between p and the set $\{v_0, v_1, \ldots, v_s\}$). For every node i, the path $p(i) \in \mathcal{R}(B)$ is the unique maximal right path such that $i \in p(i)$.

5.3.3 Stabilizer states

We will now evaluate the basic invariants $I_{n,r}^{\Pi}$ in an arbitrary stabilizer state $|\psi\rangle$ on n qubits. Our objective is to give a translation of the invariant $I_{n,r}^{\Pi}\,(\rho_\psi)$ in the binary stabilizer formalism.

5.3.3.1 Main theorem

First we need an additional definition: let B be a binary tree on r nodes with $t := |\mathcal{R}(B)|$ maximal right paths $p_1, \ldots, p_t$, which we suppose to be ordered in such a way that $\mathrm{st}(p_1) < \mathrm{st}(p_2) < \cdots < \mathrm{st}(p_t)$. The $r \times t$ matrix R_B over $\mathbb{F}_2$ is defined through its columns $(R_B)_j$ as follows:

$$(R_B)_j = \sum_{i \in p_j} e_i, \tag{5.59}$$

for every $j \in \{1, \ldots, t\}$, where e_i is the ith canonical base vector in $\mathbb{F}_2^r$.

We are now ready to state the following theorem:

Theorem 5.15 *Let $|\psi\rangle$ be a stabilizer of state on n qubits with generator matrix S. Let S_i^T $(i = 1, \ldots, n)$ be the $2 \times n$ submatrix of S obtained by selecting the ith and the $(n+i)$th row of S. Fix $r \in \mathbb{N}_0$, let $B_1, \ldots, B_n$ be n binary trees on r nodes and let $\Pi \in \mathcal{P}_r^n$ be the associated n-tuple of permutations. Then*

$$log_2\ I_{n,r}^{\Pi}(\rho_\psi) = dim_{\mathbb{F}_2}\ ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix} + c, \tag{5.60}$$

where c is an additive constant independent of $|\psi\rangle$.

The proof of theorem 5.15 is now given in two main parts. We show in subsection 5.3.3.2 that it is sufficient to prove the theorem for graph states. The proof of theorem 5.15 for graph states is subsequently given in subsection 5.3.3.3. For the remainder of this section, we fix r and consider an n-tuple $\Pi = (\pi_1, \ldots, \pi_n)$ of permutations $\pi_i \in \mathcal{P}_r$ and n binary trees B_i on r vertices corresponding to the permutations π_i. We denote $\mathcal{B} := (B_1, \ldots, B_n)$.

5.3.3.2 Reduction to graph states

Suppose that theorem 5.15 holds for all graph states. Let $|\psi\rangle$ be a stabilizer state on n qubits with generator matrix S, and let $|G\rangle$ be an LC equivalent graph state with generator matrix S'. Then there exist $Q \in C_n^l$ and $R \in GL(n, \mathbb{F}_2)$ such that

$$QSR = S'. \tag{5.61}$$

Letting $Q^{(i)}$ be the 2×2 subblock of Q acting on the ith copy of $\mathbb{F}_2^2$, for every $i = 1, \ldots, n$, (5.61) is equivalent to

$$Q^{(i)} S_i^T R = S_i'^T, \tag{5.62}$$

for every $i = 1, \ldots, n$. Now, as $|\psi\rangle$ and $|G\rangle$ are LC equivalent, one has

$$I^{\Pi}_{n,r}(\rho_\psi) = I^{\Pi}_{n,r}(\rho_G). \tag{5.63}$$

Using theorem 5.15, this shows that $\log_2 \, I^{\Pi}_{n,r}(\rho_\psi)$ is, up to an additive constant, equal to

$$\begin{aligned}
& \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R^T_{B_1} \otimes S_1^{\prime T} \\ R^T_{B_2} \otimes S_2^{\prime T} \\ \cdots \\ R^T_{B_n} \otimes S_n^{\prime T} \end{bmatrix} \\
= \; & \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R^T_{B_1} \otimes Q^{(1)} S_1^T R \\ R^T_{B_2} \otimes Q^{(2)} S_2^T R \\ \cdots \\ R^T_{B_n} \otimes Q^{(n)} S_n^T R \end{bmatrix} \\
= \; & \dim_{\mathbb{F}_2} \ker \begin{bmatrix} I \otimes Q^{(1)} & \cdot & \cdots & \cdot \\ \cdot & I \otimes Q^{(2)} & \cdots & \cdot \\ & & \vdots & \\ \cdot & \cdot & \cdots & I \otimes Q^{(n)} \end{bmatrix} \begin{bmatrix} R^T_{B_1} \otimes S_1^T \\ R^T_{B_2} \otimes S_2^T \\ \cdots \\ R^T_{B_n} \otimes S_n^T \end{bmatrix} I \otimes R \\
= \; & \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R^T_{B_1} \otimes S_1^T \\ R^T_{B_2} \otimes S_2^T \\ \cdots \\ R^T_{B_n} \otimes S_n^T \end{bmatrix},
\end{aligned} \tag{5.64}$$

which proves the desired result.

5.3.3.3 Proof of main theorem for graph states

Fix a graph G on n vertices with adjacency matrix θ and the generator matrix

$$S = \begin{bmatrix} \theta \\ I \end{bmatrix},$$

which has $2 \times n$ subblocks S_i^T defined as in theorem 5.15 by

$$S_i^T = \begin{bmatrix} \theta_i^T \\ e_i^T \end{bmatrix}.$$

The proof of theorem 5.15 for the case where $\rho_\psi = \rho_G$ is structured as follows: in lemma 5.17 we show that the invariant $I^{\Pi}_{n,r}(\rho_G)$ is equal to a sum of the form

$$\frac{1}{N} \sum_{X \in \mathcal{V}} (-1)^{\mathcal{Q}(X)}, \tag{5.65}$$

where N is a normalization factor independent of G, $\mathcal{V}$ is a linear subspace of $\mathbb{F}_2^{n \times r}$ and $\mathcal{Q}$ is a quadratic form on $\mathbb{F}_2^{n \times r}$. In lemma 5.18, we subsequently show that the form $\mathcal{Q}$ is in fact identical zero on the space $\mathcal{V}$, which implies that the sum in (5.65) is (up to the normalization) equal to the cardinality of $\mathcal{V}$. Finally, this cardinality is related to the r.h.s of (5.60) and the proof of theorem 5.15 is completed.

To compute the invariant $I^{\Pi}_{n,r}(\rho_G)$, it will be useful to work with the expansion of ρ_G in terms of tau operators that we obtained in proposition 2.13 in chapter 2. After plugging (2.45) in (5.58), we will be dealing with expressions of the form

$$\mathrm{Tr}\ (T^{\Pi}_{n,r}\ \tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_r), \tag{5.66}$$

where the τ_is are themselves n-fold tensor products of tau matrices, i.e. $\tau_i \in \mathcal{G}_n$ for every $i = 1, \ldots, r$. A closer look at these expressions beforehand is appropriate. To this end, let $X, Y, \ldots$ be any r local operators of dimensions $2^n \times 2^n$ as follows:

$$\begin{aligned} X &= X_1 \otimes \cdots \otimes X_n, \\ Y &= Y_1 \otimes \cdots \otimes Y_n,\ \ldots, \end{aligned}$$

where $X_i, Y_i, \ldots$ are 2×2 matrices. Furthermore, for any $\pi \in \mathcal{P}_r$ we denote

$$A_{r,\pi}(U, V, \ldots) := \sum_{i_1,\ldots,i_r} U_{i_1 i_{\pi(1)}}\ V_{i_2 i_{\pi(2)}} \cdots,$$

where U, $V, \ldots$ are r arbitrary 2×2 matrices. Using the definition of $T^{\Pi}_{n,r}$, it is then easy to check that

$$\mathrm{Tr}\ (T^{\Pi}_{n,r}\ X \otimes Y \otimes \ldots) = \prod_{i=1}^{n} A_{r,\pi_i}(X_i, Y_i, \ldots). \tag{5.67}$$

It follows that (5.66) is a product of n factors of the form

$$A_{r,\pi}(\tau_{u_1 u'_1}, \ldots, \tau_{u_r u'_r}) =: A_{r,\pi}(u, u'),$$

where $u = (u_1, \ldots, u_r)$, $u' = (u'_1, \ldots, u'_r) \in \mathbb{F}_2^r$. Expressions of this type are calculated in the following lemma. First we need some additional definitions: let B be a binary tree on r nodes. The $r \times r$ matrix D_B over $\mathbb{F}_2$ is defined through its columns $(D_B)_j$ as follows:

$$(D_B)_j = \sum_{i \in p(j),\ i \leq j} e_i, \tag{5.68}$$

for every $j \in \{1, \ldots, r\}$. Secondly, the linear space V_B consists of all $x \in \mathbb{F}_2^r$ such that $\sum_{i \in p} x_i = 0$ for every $p \in \mathcal{R}(B)$ (i.e., V_B is the null space of the matrix R_B^T defined above).

With these definitions, we have the following result:

Lemma 5.16 *Let $\pi \in \mathcal{P}_r$ be a permutation corresponding to a binary tree B and let $(u,u') \in \mathbb{F}_2^{2r}$. Then*

$$A_{r,\pi}(u,u') = \begin{cases} 2^{r-dim\ V_B}(-1)^{u^T D_B^T u' + u^T u'} & \textit{if } u,u' \in V_B \\ 0 & \textit{otherwise} \end{cases} \tag{5.69}$$

Proof: First, note that the entries of the 1-qubit operators τ_{ab} can be parameterized as

$$(\tau_{ab})_{c,d} = (-1)^{ac}\delta_{c+d,b}, \tag{5.70}$$

where $a,b,c,d \in \mathbb{F}_2$. Using this formula in the definition of $A_{r,\pi}$, we obtain

$$A_{r,\pi}(u,u') = \sum_{x\in\mathbb{F}_2^r} (-1)^{u^T x}\delta_{x_1+x_{\pi(1)},u_1'} \dots \delta_{x_r+x_{\pi(r)},u_r'}. \tag{5.71}$$

Equivalently, the sum runs over all $x \in \mathbb{F}_2^r$ which lie in the affine subspace determined by the equations $x_i + x_{\pi(i)} = u_i'$ for all $i = 1,\dots,r$. However, this system of equations may not be consistent: indeed, one can easily show that a solution exists iff $u' \in V_B$. Whenever this is the case, the solutions are given by $x = x_0 + x'$, where $x_0 = D_B^T u' + u'$ and x' satisfies $x_i' + x_{\pi(i)}' = 0$ for every $i = 1,\dots,r$. Moreover, the space of all such x' is the orthogonal complement of V_B with respect to the standard inner product in $\mathbb{F}_2^r$ (or equivalently, the column space of R_B), as one can verify. Therefore, we have

$$A_{r,\pi}(u,u') = \begin{cases} \sum_{x'\in V_B^\perp} (-1)^{u^T(D_B^T u' + x' + u')} & \text{if } u' \in V_B \\ 0 & \text{otherwise} \end{cases} \tag{5.72}$$

Furthermore, the sum $\sum_{x'\in V_B^\perp}(-1)^{u^T x'}$ is equal to $2^{r-\dim V_B}$ if $u \in V_B$ and zero otherwise. This proves the result. $\square$

We now proceed in calculating the invariant $I_{n,r}^\Pi(\rho_G)$. Using lemma 5.16 in (5.58), we find that $I_{n,r}^\Pi(\rho_G)$ is equal to the sum

$$\frac{1}{2^{nr}} \sum_{x^1,\dots,x^r\in\ \mathbb{F}_2^n} \left\{(-1)^{\sum_{i=1}^r k_\theta(x^i)}\ \text{Tr}\ (T_{n,r}^\Pi\ \tau_{(\theta x^1,x^1)} \otimes \dots \otimes \tau_{(\theta x^r,x^r)})\right\} \tag{5.73}$$

First, denoting by $\mathcal{P}_{\text{lows}}(\theta)$ the strictly lower triangular part of θ and writing

$$X := [x^1|\dots|x^r] \in \mathbb{F}_2^{n\times r}, \tag{5.74}$$

we obtain the shorthand notation

$$\sum_{i=1}^r k_\theta(x^i) = \text{Tr}\ X^T\mathcal{P}_{\text{lows}}(\theta)X. \tag{5.75}$$

Secondly, the trace in (5.73) splits into a product of n factors as in (5.67), each of which can be calculated by employing lemma 5.16. The calculation is straightforward. Defining for every $X \in \mathbb{F}_2^{n\times r}$ the matrix $X_{\mathcal{B}} \in \mathbb{F}_2^{n\times r}$ by

$$(X_{\mathcal{B}})_{ij} = \sum_{k=1}^{r} X_{ik} \left(D_{B_i}\right)_{kj} ,$$

one finds that (5.73) is equal (up to a normalization independent of G) to

$$\sum (-1)^{\text{ Tr } X^T \mathcal{P}_{\text{lows}}(\theta) X + \text{ Tr } (X_{\mathcal{B}}+X)^T \theta X}, \tag{5.76}$$

where the sum runs over all X such that

$$S_i^T \left(\sum_{j\in p} x^j \right) = 0 \tag{5.77}$$

for every $i \in \{1, \ldots, n\}$ and $p \in \mathcal{R}(B_i)$. We will denote the space of all such X by $V_{\mathcal{B}}(G)$. Note that $\text{Tr}(X^T\theta X) = \sum_i (x^i)^T \theta x^i = 0$ since θ is symmetric and has zero diagonal. We have proven:

Lemma 5.17 *The invariant $I_{n,r}^{\Pi}(\rho_G)$ can be written as*

$$I_{n,r}^{\Pi}(\rho_G) = \frac{1}{N} \sum_{X \in V_{\mathcal{B}}(G)} (-1)^{\ Tr\ X^T \mathcal{P}_{lows}(\theta) X +\ Tr\ X_{\mathcal{B}}^T \theta X}, \tag{5.78}$$

where N is a normalization factor independent of G and the definitions of $V_{\mathcal{B}}(G)$ and $X_{\mathcal{B}}$ are as above.

The last part of our argument consists of showing that the quadratic form $\mathcal{Q}(X) := \text{ Tr } X^T \mathcal{P}_{\text{lows}}(\theta) X + \text{ Tr } X_{\mathcal{B}}^T\ \theta X$ is zero on the space $V_{\mathcal{B}}(G)$. Once this result is shown, the proof of theorem 5.15 is immediate: indeed, if $\mathcal{Q}(X) = 0$ for every $X \in V_{\mathcal{B}}(G)$ then $\log_2 I_{n,r}^{\Pi}(\rho_G) \sim \dim V_{\mathcal{B}}(G)$. Moreover, the matrices $X = [x^1| \ldots |x^r] \in V_{\mathcal{B}}(G)$ can be reshaped as vectors $\tilde{X} = (x^1, \ldots, x^r) \in (\mathbb{F}_2^n)^{\times r}$ which are exactly the elements in the null space of the matrix

$$\begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}. \tag{5.79}$$

Clearly, the spaces of the Xs and the $\tilde{X}$s have the same dimension and the proof of theorem 5.15 is thus completed. We now show that $\mathcal{Q} = 0$ on the space $V_{\mathcal{B}}(G)$:

Lemma 5.18 $\mathcal{Q}(X) = 0$ *for every $X \in V_{\mathcal{B}}(G)$.*

Proof: Let $X = [x^1|\dots|x^r]$ be an element of $V_{\mathcal{B}}(G)$. Recall that by definition (5.77) this entails that

$$\left[\begin{array}{c}\theta_i^T\\ e_i^T\end{array}\right]\left(\sum_{j\in p} x^j\right) = 0 \tag{5.80}$$

for every $i \in \{1,\dots,n\}$ and $p \in \mathcal{R}(B_i)$. In particular,

$$\sum_{j\in p} x_i^j = 0 \tag{5.81}$$

for every $i \in \{1,\dots,n\}$ and for every $p \in \mathcal{R}(B_i)$, where $x^j = (x_1^j,\dots,x_n^j)$. Consequently,

$$\sum_{j=1}^{r} x^j = 0. \tag{5.82}$$

Now, consider the first term of $\mathcal{Q}(X)$:

$$\begin{aligned}\mathcal{Q}_1 &:= \mathrm{Tr}\ X^T\mathcal{P}_{\mathrm{lows}}(\theta)X\\ &= \sum_{j=1}^{r}(x^j)^T\mathcal{P}_{\mathrm{lows}}(\theta)\ x^j.\end{aligned} \tag{5.83}$$

Substituting $x^r = \sum_{j=1}^{r-1} x^j$ (from (5.82)), an easy calculation shows that

$$\mathcal{Q}_1 = \sum_{j=1}^{r-1}\left(\sum_{k=1}^{j-1} x^k\right)^T \theta\ x^j.$$

Let $\omega_{ij} \subseteq \{1,\dots,n\}$ consist of all $k \in \{1,\dots,j-1\}$ which belong to a maximal right path p of B_i such that $\mathrm{fin}(p) \geq j$. Then, denoting $y^j := \sum_{k=1}^{j-1} x^k$, (5.81) implies that $y_i^j = \sum_{k\in\omega_{ij}} x_i^k$.

The second term of $\mathcal{Q}(X)$ is

$$\begin{aligned}\mathcal{Q}_2 &:= \mathrm{Tr}\ X_{\mathcal{B}}^T\ \theta X\\ &= \sum_{j=1}^{r}(z^j)^T\theta\ x^j,\end{aligned} \tag{5.84}$$

where z^j is the jth column of $X_{\mathcal{B}}$. Let η_{ij} consist of all $k \in \{1,\dots,j-1\}$ which belong to the unique maximal right path of B_i which contains j. It then follows from the definition of $X_{\mathcal{B}}$ that $z_i^j = \sum_{k\in\eta_{ij}\cup\{j\}} x_i^k$. Note that $\eta_{ir}\cup\{r\} \in \mathcal{R}(B_i)$ and therefore $z_i^r = 0$ for every $i = 1,\dots,n$ from (5.81). Thus, $z^r = 0$. Combining the above results, we obtain

$$\mathcal{Q}_1 + \mathcal{Q}_2 = \sum_{j=1}^{r-1}(y^j + z^j)^T\theta\ x^j, \tag{5.85}$$

where

$$y_i^j + z_i^j = \left(\sum_{k\in\omega_{ij}} x_i^k\right) + \left(\sum_{k\in\eta_{ij}} x_i^k\right) + x_i^j. \tag{5.86}$$

In the sum (5.86), every $k \in \omega_{ij} \cap \eta_{ij}$ gives rise to a double appearance of the term x_i^k and consequently all such terms vanish. As $\eta_{ij} \subseteq \omega_{ij}$, we obtain

$$y_i^j + z_i^j = \left(\sum_{k\in\omega_{ij}\setminus\eta_{ij}} x_i^k\right) + x_i^j. \tag{5.87}$$

When using (5.87) to calculate (5.85), the terms x_i^j in (5.87) do not contribute to the sum, as they give rise to terms $(x^j)^T\theta\, x^j$ in (5.85), which are equal to zero since θ is symmetric. Thus, defining the vectors u^j by

$$u_i^j := \left(\sum_{k\in\omega_{ij}\setminus\eta_{ij}} x_i^k\right),$$

(5.85) becomes

$$\mathcal{Q}(X) = \sum_{j=1}^{r-1} {u^j}^T \theta\, x^j. \tag{5.88}$$

Note that the set $\omega_{ij}\setminus\eta_{ij}$ consists of all $k \in \{1,\dots,j-1\}$ which belong to some path $p \neq p(j)$ in $\mathcal{R}(B_i)$ such that $\operatorname{fin}(p) \geq j$. We now show that whenever j and l belong to the same maximal right path of B_i, one has $\omega_{ij}\setminus\eta_{ij} = \omega_{il}\setminus\eta_{il}$ and consequently $u_i^j = u_i^l$. To see this, fix i and consider arbitrary nodes j and l which lie on the same maximal right path of B_i. Without loss of generality we can assume that $j < l$. Denoting by j' the right son of j, we prove that $\omega_{ij}\setminus\eta_{ij} = \omega_{ij'}\setminus\eta_{ij'}$: indeed, if $j' = j+1$ then j does not have a left son (due to the canonical labelling of the nodes) and the assertion follows trivially; if on the other hand $j' > j+1$ then j has a left subtree. However, the maximal right paths p in this subtree do not contribute to $\omega_{ij'}\setminus\eta_{ij'}$, as they all satisfy $\operatorname{fin}(p) < j'$ (which is again due to the canonical labelling of the nodes). Therefore $\omega_{ij}\setminus\eta_{ij} = \omega_{ij'}\setminus\eta_{ij'}$ and iteration of this argument shows that $\omega_{ij}\setminus\eta_{ij} = \omega_{il}\setminus\eta_{il}$.

We will now use the above property of the u^js to show that $\mathcal{Q}(X) = 0$. Let us consider the first binary tree B_1 and suppose that $(1,2,3)$ is a maximal right path of this tree. This example is chosen for notational convenience, but the argument will work for any maximal right path in any tree. Thus, we have $u_1^1 = u_1^2 = u_1^3 \equiv u$. Denoting $u^j = (u, v^j)$ for $j = 1,2,3$, the relevant terms in (5.88) are

$$\begin{aligned}&(u^1)^T\theta\, x^1 + (u^2)^T\theta\, x^2 + (u^3)^T\theta\, x^3\\ =\ &(u,v^1)^T\theta\, x^1 + (u,v^2)^T\theta\, x^2 + (u,v^3)^T\theta\, x^3\end{aligned}$$

$$= (u,\ 0\ )^T\theta(x^1 + x^2 + x^3)$$
$$+ (0, v^1)^T\theta\ x^1 + (0, v^2)^T\theta\ x^2 + (0, v^3)^T\theta\ x^3$$

In the r.h.s. of the last equality, the first term is equal to

$$u\ \theta_1^T(x^1 + x^2 + x^3), \tag{5.89}$$

which is equal to zero from (5.80), since $(1, 2, 3)$ is a maximal right path of B_1. Applying this argument to all maximal right paths of the trees in $\mathcal{B}$ shows that indeed $\mathcal{Q} = 0$ on the space $V_{\mathcal{B}}(G)$. This ends the proof. □

5.3.3.4 Discussion

Theorem 5.15 shows how the information contained in the invariants $I^{\Pi}_{n,r}(\rho_\psi)$ can entirely be recuperated within the binary representation of the stabilizer formalism. The fact that *a* translation into the binary framework is possible is of course not unexpected, as a stabilizer state is, up to information about the overall phases of its stabilizer elements, defined by its generator matrix. Moreover, we have seen in chapter 3 that these phases do not play a role in determining the local equivalence class of a state. However, the simple form of the result (5.60) is remarkable: an invariant $I^{\Pi}_{n,r}(\rho_\psi)$ is in a one-to-one correspondence with the dimension of a linear subspace of $C_S \times \cdots \times C_S$, which depends on the generator matrix S in a very transparent way. Additionally, it is interesting to notice the explicit way in which the n-tuple of binary trees appear in the result: every matrix R_{B_i}, corresponding to the ith binary tree, is coupled via a tensor product to the matrix S_i, which is the subblock of S containing the information about the ith qubit. Finally, we note that the r.h.s. of (5.60) can be computed efficiently via a calculation of the rank over $\mathbb{F}_2$ of the matrix

$$\begin{bmatrix} R^T_{B_1} \otimes S^T_1 \\ R^T_{B_2} \otimes S^T_2 \\ \cdots \\ R^T_{B_n} \otimes S^T_n \end{bmatrix}. \tag{5.90}$$

One can present the invariants (5.60) in an equivalent way. We start with the invariants of smallest nontrivial degree, i.e. $r = 2$. There are exactly two binary trees on 2 vertices, as node 2 can either be the right or the left son of node 1. Equivalently, there are two possible matrices R_B according to definition (5.59), namely

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad [1\ 1]^T, \tag{5.91}$$

where the identity matrix corresponds to the tree where 2 is the left son of 1. Now, consider an n-tuple $(B_1, \ldots, B_n)$ of binary trees and the corresponding n-tuple of permutations $\Pi \in \mathcal{P}^n_2$. Let $\omega \subseteq \{1, \ldots, n\}$ denote the set of all i

such that $R_{B_i} = [1\ 1]^T$ – note that every n-tuple of binary trees on 2 nodes corresponds uniquely to such a set ω. Using the notation S_i as before, this implies that

$$R_{B_i}^T \otimes S_i^T = [S_i^T\ S_i^T]$$

whenever $i \in \omega$ and

$$R_{B_i}^T \otimes S_i^T = \begin{bmatrix} S_i^T & 0 \\ 0 & S_i^T \end{bmatrix}$$

otherwise. Therefore, the null space of the matrix (5.90) consists of all vectors $(x, x') \in \mathbb{F}_2^{2k}$ such that

$$\begin{aligned} S_i(x + x') = 0 \qquad & \text{for every } i \in \omega \\ S_j x = S_j x' = 0 \qquad & \text{for every } j \in \bar{\omega}, \end{aligned} \tag{5.92}$$

where $\bar{\omega}$ is again the complement of ω in $\{1, \dots, n\}$. Note that (5.92) implies that $Sx = Sx'$ and therefore $x = x'$, since S has full rank. Thus, the solutions of (5.92) are in a one-to-one correspondence with the linear subspace of $\mathbb{F}_2^k$ of those x satisfying $S_j x = 0$ for every $j \in \bar{\omega}$ or, equivalently, $S_{\bar{\omega}} x = 0$. The linear mapping $\phi_S : \mathbb{F}_2^k \to \mathbb{F}_2^{2n}$ defined by the matrix S maps the space of such xs to the space of vectors $v = Sx$ which satisfy $v_j = v_{n+j} = 0$ for every $j \in \bar{\omega}$, or, equivalently, $\text{supp}(v) \subseteq \omega$. As S has full rank, the mapping ϕ_S is injective and the spaces of the xs and the vs have equal dimension. Thus, we have shown that

$$\log_2 I_{n,2}^{\Pi}(\psi) = \log_2 B_\omega(\psi) + c. \tag{5.93}$$

Therefore, we have shown that the LU invariants of degree two correspond to the LC invariants B_ω that we encountered in the first section of this chapter. This is clearly a more insightful presentation of the invariants $I_{n,2}^{\Pi}$ than (5.60). Moreover, a similar argument as above can be made to obtain an analogous presentation of the invariants of higher degree:

Theorem 5.19 *Let S be a $2n \times n$ generator matrix of a stabilizer state on n qubits and let the subblocks S_i^T be defined as in theorem 5.15. Fix $r \in \mathbb{N}_0$ and let $B_1, \dots, B_n$ be n binary trees on r vertices. Let $\mathcal{R} = \mathcal{R}(B_1) \cup \dots \cup \mathcal{R}(B_n)$ denote the set of all maximal right paths of these trees. For every $p \in \mathcal{R}$, let ω_p denote the subset of all $i \in \{1, \dots, n\}$ such that $p \notin \mathcal{R}(B_i)$. Then the dimension of the kernel of the matrix (5.90) is equal to the dimension of the space*

$$\{(v^1, \dots, v^r) \in\ C_S \times \dots \times\ C_S |\ supp\ (\sum_{j \in p} v^j) \subseteq \omega_p,\ for\ every\ p \in \mathcal{R}\}. \tag{5.94}$$

The proof of theorem 5.19 is omitted, as it is a straightforward generalization of the considerations made above for the invariants of degree 2. A number of properties of the invariants immediately follows from theorem 2: e.g., consider an invariant I_{r+1,Π_0} such that its n binary trees B_i have got a common maximal right path p_0 of exactly one element i_0, i.e. $p_0 = (i_0) \in \mathcal{R}(B_1) \cap \cdots \cap \mathcal{R}(B_n)$. Considering (5.94) for this invariant, it follows that $\omega_{p_0} = \emptyset$. Consequently, $\mathrm{supp}(v^{i_0}) \subseteq \emptyset$ and therefore $v^{i_0} = 0$ for every v^{i_0} in (5.94). Thus, the invariant I_{r+1,Π_0} is equal to an invariant of degree r corresponding to binary trees $\bar{B}_i$ which are obtained by deleting the node i_0 from the original trees B_i. Reversing the above argument shows that any invariant of degree r can be written as an invariant of degree $r+1$, thereby showing that

$$\{I_{n,r}^{\Pi}\}_{\Pi} \subset \{I_{n,r+1}^{\Pi'}\}_{\Pi'} \tag{5.95}$$

for every r, where Π (Π') ranges over all elements in $\mathcal{P}_r^n$ ($\mathcal{P}_{r+1}^n$). Moreover, this argument can be generalized to show that an invariant corresponding to a tuple of binary trees which have some subtree in common, can be written as the product of invariants of lower degree.

A second advantage of the presentation in theorem 5.19 is that it exposes the analogy between the above LU invariants and the LC invariants that we considered in section 5.2: also the LU invariants $I_{n,r}^{\Pi}(\rho_\psi)$ correspond to cardinalities of certain subspaces of $C_S \times \cdots \times C_S$ that are defined in terms of constraints on their supports. What is more, we have seen above that for degree $r = 2$ one even obtains equality of LU and LC invariants, as every invariant $I_{n,2}^{\Pi}(\rho_\psi)$ is equal (up to a normalization) to $B_\omega(\psi)$, for some ω. Interestingly, an analogous statement can be done for the LU invariants of degree 3:

Proposition 5.20 *Let $|\psi\rangle$ be a stabilizer state on n qubits. Let $\Omega = (\omega^1, \omega^2, \omega^{12})$ be a 3-tuple of subsets of $\{1, \ldots, n\}$. Then there exists an n-tuple $\Pi = (\pi_1, \ldots, \pi_n) \in \mathcal{P}_3^n$ such that $B_{n,2}^{\Omega}(\psi)$ is equal to $I_{n,3}^{\Pi}(\psi)$ up to an additive constant independent of $|\psi\rangle$.*

Proof: Recall that $B_{n,2}^{\Omega}(\psi)$ is equal to

$$|\{(v^1, v^2) \in C_S^{\times 2} |\ \mathrm{supp}(v^j) \subseteq \omega^j\ (j = 1, 2),\ \mathrm{supp}(v^1 + v^2) \subseteq \omega^{12}\}|,$$

which is equal to

$$|\{(v^1, v^2, v^3) \in C_S^{\times 3} |\ \mathrm{supp}(v^j) = \omega^j\ (j = 1, 2),\ \mathrm{supp}(v^3) = \omega^{12}, \sum_{j=1}^{3} v^j = 0\}|. \tag{5.96}$$

We now construct an n-tuple $\Pi = (\pi_1, \ldots, \pi_n) \in \mathcal{P}_3^n$ such as to yield the desired result. This construction goes as follows: let $i \in \{1, \ldots, n\}$;

- if i belongs to *at least two* of the sets $\bar{\omega}^1$, $\bar{\omega}^2$, $\bar{\omega}^{12}$, then $\pi_i = (1)(2)(3)$;
- if $i \in \bar{\omega}^1 \setminus (\bar{\omega}^2 \cup \bar{\omega}^{12})$ then $\pi_i = (1)(23)$;
  if $i \in \bar{\omega}^2 \setminus (\bar{\omega}^1 \cup \bar{\omega}^{12})$ then $\pi_i = (2)(13)$;
  if $i \in \bar{\omega}^{12} \setminus (\bar{\omega}^1 \cup \bar{\omega}^2)$ then $\pi_i = (3)(12)$;

- if $i \in \omega^1 \cap \omega^2 \cap \omega^{12}$ then $\pi_i = (123)$.

Note that indeed $\pi_i \in \mathcal{P}_3$ for every $i = 1, \ldots, n$. Letting $(B_1, \ldots, B_n)$ be the corresponding tuple of binary trees and defining the set $\mathcal{R}$ as in theorem 5.19, it is straightforward to verify that (5.96) is equal to

$$|\{(v^1, v^2, v^3) \in \ C_S^{\times 3}| \text{ supp } (\sum_{j \in p} v^j) \subseteq \omega_p, \text{ for every } p \in \mathcal{R}\}|. \tag{5.97}$$

This proves the result. □

The main merit of the above result is that the LC invariant $B^{\Omega}_{n,2}(\psi)$ is in fact also a general LU invariant. Note that this was not at all clear from its definition. As an immediate corollary, also the $A^{\Omega}_{n,2}(\psi)$s are LU invariants, as they can be written as linear combinations of the $B^{\Omega}_{n,2}(\psi)$s with constant coefficients.

Despite the interesting similarity between the LU invariants and the LC invariants we considered before, any bounds on the maximal degree r that needs to be considered in order to obtain a complete set of LU invariants, are to date unknown. Of course, the above problem is completely resolved should one be able to prove that every two LU equivalent stabilizer states are necessarily LC equivalent: then it is sufficient to consider LC invariants, for which we do have such bounds. This problem whether LU equivalence and LC equivalence of stabilizer states are essentially the same notions, and the possible role of invariant theory in this research, will be discussed in more detail in chapter 6.

5.3.4 Stabilizer codes

As in the section concerning LC invariants, also here essentially all results − and, in particular: theorem 5.15 − can be generalized to arbitrary stabilizer codes. However, the generalization of theorem 5.15 is not entirely trivial and is worth presenting.

Let $\rho_{\mathcal{S}}$ be an $[n, k]$ stabilizer code with generator matrix S. For large enough $m > n$, there exists a stabilizer state $|\psi\rangle$ on m qubits with generator matrix S' such that $\rho_{\mathcal{S}}$ can be obtained from $|\psi\rangle$ by tracing out the qubits $n+1, \ldots, m$, i.e.

$$\rho_{\mathcal{S}} = \rho_{\omega}(\psi), \tag{5.98}$$

where we have denoted $\omega = \{1, \ldots, n\}$. Now, let $\Pi' \in \mathcal{P}_r^m$ be the m-tuple of permutations which is obtained by appending to Π $m - n$ times the identity permutation (which belongs to $\mathcal{P}_r$) and let $\mathcal{B}' = (B_1, \ldots, B_n, B_0, \ldots, B_0)$ be the associated m-tuple of binary trees; here B_0 is the binary tree with r maximal right paths (i), corresponding to the identity permutation. The crucial observation is now that

$$I^{\Pi}_{n,r}(\rho_{\mathcal{S}}) = I^{\Pi'}_{n,r}(\rho_{\psi}). \tag{5.99}$$

This identity can easily be verified by using the definition of $I_{n,r}^{\Pi'}$. We can then apply theorem 5.15 and find

$$\begin{aligned}\log_2 I_{n,r}^{\Pi}(\rho_{\mathcal{S}}) &= \log_2 I_{r,\Pi'}(\rho_\psi) \\ &= \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R_{B_1}^T \otimes S_1'^T \\ \cdots \\ R_{B_n}^T \otimes S_n'^T \\ R_{B_0}^T \otimes S_{n+1}'^T \\ \cdots \\ R_{B_0}^T \otimes S_m'^T \end{bmatrix} + c \qquad (5.100)\end{aligned}$$

Applying theorem 5.19 to the generator matrix S' and the binary trees $\mathcal{B}'$, (5.100) is equal to the dimension of

$$\{(v^1, \ldots, v^r) \in\ C_{S'} \times \cdots \times\ C_{S'} |\ \text{supp}\ (\sum_{j\in p} v^j) \subseteq \omega_p,\ \text{for every}\ p \in \mathcal{R}'\} \qquad (5.101)$$

where $\mathcal{R}' = \mathcal{R}(B_1) \cup \cdots \cup \mathcal{R}(B_n) \cup \mathcal{R}(B_0)$. As the last $m-n$ trees in the m-tuple $\mathcal{B}'$ are equal to B_0, every v^j in (5.101) satisfies $\text{supp}(v^j) \subseteq \omega$. Therefore, the dimension of (5.101) is equal to the dimension of

$$\{(w^1, \ldots, w^r) \in\ C_S \times \cdots \times\ C_S |\ \text{supp}\ (\sum_{j\in p} w^j) \subseteq \omega_p,\ \text{for every}\ p \in \mathcal{R}\} \qquad (5.102)$$

where now $\mathcal{R} = \mathcal{R}(B_1) \cup \cdots \cup \mathcal{R}(B_n)$. A last application of theorem 5.19 yields

$$\log_2 I_{n,r}^{\Pi}(\rho_{\mathcal{S}}) = \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix} + c, \qquad (5.103)$$

which is the desired result. We have proven:

Theorem 5.21 *Let $\rho_{\mathcal{S}}$ be an $[n,k]$ stabilizer code with generator matrix S. Let S_i^T ($i = 1, \ldots, n$) be the $2 \times (n-k)$ submatrix of S obtained by selecting the ith and the $(n+i)$th row of S. Fix $r \in \mathbb{N}_0$, let $B_1, B_2, \ \ldots, B_n$ be n binary trees on r nodes and let $\Pi \in \mathcal{P}_r^n$ be the associated n-tuple of permutations. Then*

$$log_2\ I_{r,\Pi}(\rho_{\mathcal{S}}) = dim_{\mathbb{F}_2}\ ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix} + c, \qquad (5.104)$$

where c is an additive constant independent of $\rho_{\mathcal{S}}$.

The analogue of theorem 5.19 is straightforward to state and prove:

Theorem 5.22 *Let S be a $2n \times (n-k)$ generator matrix of a stabilizer code on n qubits and let the subblocks S_i^T be defined as before. Fix $r \in \mathbb{N}_0$ and let $B_1, \ldots, B_n$ be n binary trees on r vertices. Let $\mathcal{R}$ be defined as before and consider, for every $p \in \mathcal{R}$, the set ω_p as before. Then the dimension of the kernel of the matrix in (5.104) is equal to the dimension of the space*

$$\{(v^1, \ldots, v^r) \in\ C_S \times \cdots \times\ C_S|\ supp\ (\sum_{j\in p} v^j) \subseteq \omega_p,\ for\ every\ p \in \mathcal{R}\}. \tag{5.105}$$

5.4 Conclusion

In this chapter we performed a detailed study of local unitary and local Clifford invariants of stabilizer states and codes. We started with an analysis of LC invariants. As a main result, we obtained two closely related finite sets of invariants which both completely characterize the LC equivalence class of any stabilizer state or code. These invariants are entirely formulated within the binary stabilizer formalism. A crucial notion in the construction of these invariants was that of the support of a vector in $\mathbb{F}_2^{2n}$.

In the second part of this chapter we moved to the study of LU invariants. This problem is considerably harder, since LU operations cannot be described within the binary framework. We started our study of LU invariants by considering known results on the invariant algebra of the local unitary group, where a generating set of LU invariant polynomials is obtained on the basis of combinatorial structures known as binary trees; afterwards we specified these general results to the problem at hand, thereby obtaining a complete set of LU invariants of stabilizer states and codes. Our main result in this part of the chapter was a translation of the known family of LU invariants in terms of the binary stabilizer language. We noticed that the notion of support also plays a crucial role in this translation.

Although the families of LC and LU invariants are obtained through considerably different methods, there is a striking resemblance between them. In particular, we showed that the LU invariants of degrees 2 and 3 coincide with our LC invariants. These similarities suggest that it is worthwhile to investigate the relation between LU and LC equivalence of stabilizer states and codes in more detail. This is done in chapter 6.

References

The main results in this chapter are the subject of our work [46] (section 5.2, prop. 5.5, prop. 5.6, cor. 5.7, cor. 5.8, prop. 5.9, cor. 5.10) and [49] (section 5.3, thm. 5.15, thm. 5.19, prop. 5.20, thm. 5.21).

In section 5.2 we refer to Rains [36] for a study of the invariants A_ω and B_ω for general codes (i.e., not necessarily stabilizer codes), which he calls *quantum weight enumerators*. Hein et al. [25] also mention the B_ωs for graph states, in relation with the calculation of the Schmidt measure, which is a multipartite entanglement measure; these authors also describe the link between the invariants B_ω and the connectivity function of a graph. In sections 5.3.1 and 5.3.2, the results concerning generating sets of LU invariant polynomials and their relation with binary trees are taken from Grassl et al. [22]; these authors use important ground work performed by Rains [37].

Finally, we also refer to our related work [51] dealing with the invariant algebra of the local Clifford group, which has not been incorporated in this thesis.

Chapter 6

LU versus LC equivalence

6.1 Introduction

In the previous chapters we have studied several aspects of LC and LU equivalence of stabilizer states and codes in detail. During this investigation − and especially in chapter 5, dealing with local invariants − we have encountered several similarities and analogues between LU and LC equivalence of stabilizer states (codes). Hence the natural question imposes itself whether there is in fact a difference between these two equivalences. This question is addressed in the present chapter. In other words, we investigate whether every two LU equivalent stabilizer states are also LC equivalent.

We will show that the answer to the above question is positive for a large subclass of stabilizer states and it is, with this result, our aim to take the first steps towards a complete answer to the above question. The main concept we will use to study the problem at hand is that of *minimal support* of a stabilizer. We will first define this notion and then use it to construct a class of stabilizer states, such that every two LU equivalent states in this class must also be LC equivalent.

Note that the present result, and a possible general proof of the assertion that $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$ for every stabilizer state $|\psi\rangle$, has several interesting implications. Firstly, we showed in chapter 3 that any two SLOCC stabilizer states are also LU equivalent. Together with the present result, this shows that SLOCC, LU and LC equivalence are identical notions within the present subclass of stabilizer states, and therefore there is in fact only a single notion of 'local' equivalence within this class of states. Secondly, we showed in chapter 4 that LC equivalence of graph states (and hence of all stabilizer states) can completely be understood in terms of local complementation of graphs. Finally, also in chapter 4 we presented an algorithm of polynomial complexity in the number of qubits which recognizes whether two given stabilizer states are LC equivalent. This shows that all three local equivalences can be detected efficiently within the present class of stabilizer states.

This chapter is organized as follows: in section 6.2, we define the notion of minimal support; in section 6.3 we present our subclass of stabilizer states such that $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$ for every $|\psi\rangle$ in this class; in section 6.4, we discuss the role of invariants in the discussion whether LU = LC; finally, we formulate a conclusion in section 6.5.

Notation

In this chapter it will be useful to fix some notation. For an operator $M \in \mathcal{G}_n$, we will denote by $M_i \in \{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$ the ith sigma matrix in the tensor product of M, for every $i = 1, \dots, n$. Also, we denote by $\alpha_M \in \{\pm 1, \pm i\}$ the unique overall phase factor such that

$$M = \alpha_M M_1 \otimes \cdots \otimes M_n \tag{6.1}$$

holds. E.g., if $M = -\sigma_x \otimes \sigma_0 \otimes \sigma_z$, then according to this notation we have $\alpha_M = -1$, $M_1 = \sigma_x$, $M_2 = \sigma_0$ and $M_3 = \sigma_z$.

6.2 Minimal supports

In this section we define the notion of *minimal support* of a stabilizer. The latter will be central in the construction of our class of stabilizer states for which $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$.

First we recall that the support $\mathrm{supp}(M)$ of a Pauli operator $M \in \mathcal{G}_n$ is defined to be the subset of $\{1, \dots, n\}$ consisting of all i such that the $M_i \neq \sigma_0$. Letting $|\psi\rangle$ be a stabilizer state on n qubits, we also recall that $A_\omega(\psi)$ is defined as

$$A_\omega(\psi) = |\{M \in \mathcal{S}(\psi) \mid \mathrm{supp}(M) = \omega\}|. \tag{6.2}$$

A *minimal support* of $\mathcal{S}(\psi)$ is a set $\omega \subseteq \{1, \dots, n\}$ such that there exists an element in $\mathcal{S}(\psi)$ with support equal to ω, but there exist no nontrivial elements with support strictly contained in ω. In other words, ω is a minimal support of $\mathcal{S}(\psi)$ if there exists $M_0 \in \mathcal{S}(\psi)$ with $\mathrm{supp}(M_0) = \omega$ and for every $M \in \mathcal{S}$, $M \neq I$, we have

$$\mathrm{supp}(M) \subseteq \omega \Rightarrow \mathrm{supp}(M) = \omega. \tag{6.3}$$

An element $M_0 \in \mathcal{S}(\psi)$ such that $\mathrm{supp}(M_0)$ is a minimal support of $\mathcal{S}(\psi)$ is called a *minimal element* of $\mathcal{S}(\psi)$. We have the following lemmas:

Lemma 6.1 *If two stabilizer states are LU equivalent then their minimal supports coincide.*

Proof: This follows from the fact that the functions $A_\omega(\cdot)$ are LU invariants. □

Lemma 6.2 *Let $|\psi\rangle$ be a stabilizer state and let ω be a minimal support of $\mathcal{S}(\psi)$. Then $A_\omega(\psi)$ is equal to 1 or 3 and the latter case can only occur if $|\omega|$ is even.*

Proof: If $A_\omega(\psi) = 1$ then we are done. If $A_\omega \geq 2$, let M, $M' \in \mathcal{S}(\psi)$ be two different elements with supports equal to ω. These elements must satisfy $\sigma_0 \neq M_i \neq M'_i \neq \sigma_0$ for every $i \in \omega$. Indeed, if this were not the case, then $\text{supp}(MM')$ would be strictly contained in ω, which contradicts the assumption that ω is a minimal support. It follows that also $\text{supp}(MM') = \omega$ and that the set $\{M_i, M'_i, (MM')_i\}$ is equal to $\{\sigma_x, \sigma_y, \sigma_z\}$ for every $i = 1, \ldots, n$. Consequently, M, M', and MM' are the only elements in $\mathcal{S}(\psi)$ with support equal to ω: indeed, suppose there does exist a fourth element $N \in \mathcal{S}(\psi)$ with $\text{supp}(N) = \omega$; fixing any $i_0 \in \omega$, then either M_{i_0}, M'_{i_0} or $(MM')_{i_0}$ is equal to N_{i_0}, say $N_{i_0} = M_{i_0}$; but then $\text{supp}(MN)$ is strictly contained in ω, which leads to a contradiction. This proves the first part of the lemma. Secondly, $|\omega|$ must be even since M and M' commute. $\square$

If ω is a minimal support of $\mathcal{S}(\psi)$, it follows from the proof of lemma 6.2 that $\rho_\omega(\psi)$ is, up to an LC operation, one of the following two states :

$$\frac{1}{2^{|\omega|}}\left(I + \sigma_x^{\otimes|\omega|}\right) \tag{6.4}$$

$$\frac{1}{2^{|\omega|}}\left(I + \sigma_x^{\otimes|\omega|} + (-1)^{|\omega|/2}\sigma_y^{\otimes|\omega|} + \sigma_z^{\otimes|\omega|}\right). \tag{6.5}$$

We denote the state (6.5) by[1] $\rho^{[|\omega|,|\omega|-2,2]}$. The following property of $\rho^{[|\omega|,|\omega|-2,2]}$, proven in Ref. [34], will be a central ingredient to the proof of our main result below:

Proposition 6.3 *Let $m \in \mathbb{N}_0, m \geq 2$. Let ρ, ρ' be two (mixed) states on $2m$ qubits, both LC equivalent to $\rho^{[2m,2m-2,2]}$, and let $U \in U(2)^{\otimes 2m}$ be a local unitary operator such that $U\rho U^\dagger = \rho'$. Then $U \in \mathcal{C}_n^l$.*

Proof: Note that we are done if we prove that every $U \in U(2)^{\otimes 2m}$ satisfying

$$U\rho^{[2m,2m-2,2]}U^\dagger = \rho^{[2m,2m-2,2]} \tag{6.6}$$

is a local Clifford operator. To prove this, we first recall that any 1-qubit unitary operator $V \in U(2)$ acts on the Pauli matrices as follows:

$$\sigma_a \mapsto V\sigma_a V^\dagger = o_{ax}\sigma_x + o_{ay}\sigma_y + o_{az}\sigma_z, \tag{6.7}$$

for every $a = x, y, z$, and where $(o_{ab}) \in SO(3)$. Equipping $\mathbb{R}^3$ with the standard qutrit basis $\{|0\rangle, |1\rangle, |2\rangle\}$, one then observes that the matrix

$$\sigma_x^{\otimes 2m} + (-1)^m\sigma_y^{\otimes 2m} + \sigma_z^{\otimes 2m} \tag{6.8}$$

[1]The state $\rho^{[|\omega|,|\omega|-2,2]}$ is the projector associated with an $[|\omega|, |\omega|-2, 2]$ stabilizer code (which is unique up to local equivalence).

is naturally associated with the vector

$$v = |0\dots 0\rangle + (-1)^m\ |1\dots 1\rangle + |2\dots 2\rangle \in (\mathbb{R}^3)^{\otimes 2m}, \tag{6.9}$$

acted on by $SO(3)^{\otimes 2m}$ in the natural way. In this picture, we have to show that every $O = O_1 \otimes \dots \otimes O_{2m} \in SO(3)^{\otimes 2m}$ satisfying $Ov = v$ is such that all its tensor factors O_i are monomial matrices [2].

We now show that O_1 is a monomial matrix. The proof for the other qutrits is completely analogous. Consider the operator

$$\langle 0|_1\ \mathrm{Tr}_{\{3,\dots,2m\}}\left(vv^T\right)|0\rangle_1, \tag{6.10}$$

acting on the second qutrit, i.e., the second copy of $\mathbb{R}^3$. It is straightforward to verify that this matrix is proportional to the rank one projector $|0\rangle\langle 0|$. Therefore, if $O = O_1 \otimes \dots \otimes O_{2m} \in SO(3)^{\otimes 2m}$ satisfies $Ov = v$, then the operator

$$\langle 0|_1\ \mathrm{Tr}_{\{3,\dots,2m\}}\left(Ovv^TO^T\right)|0\rangle_1 \tag{6.11}$$

must have rank one. A straightforward computation shows that

$$\begin{aligned}\mathrm{Tr}_{\{3,\dots,2m\}}\left(Ovv^TO^T\right) &= (O_1\otimes I)\ \mathrm{Tr}_{\{3,\dots,2m\}}\left(vv^T\right)(O_1^T\otimes I)\\ &\sim (O_1\otimes I)\left(|00\rangle\langle 00| + |11\rangle\langle 11| + |22\rangle\langle 22|\right)(O_1^T\otimes I)\end{aligned} \tag{6.12}$$

for $m \geq 2$. Note that the matrix (6.12) acts on $(\mathbb{R}^3)^{\otimes 2}$, i.e., it is a 9×9 real matrix. One then finds that

$$\langle 0|_1\ \mathrm{Tr}_{\{3,\dots,2m\}}\left(Ovv^TO^T\right)|0\rangle_1 \sim \begin{bmatrix} (O_1)^2_{00} & \cdot & \cdot \\ \cdot & (O_1)^2_{01} & \cdot \\ \cdot & \cdot & (O_1)^2_{02}\end{bmatrix} \tag{6.13}$$

This last matrix has rank one if and only if exactly one the numbers $(O_1)_{00}$, $(O_1)_{01}$ or $(O_1)_{02}$ is nonzero. Repeating the argument for the other rows shows that every row of O_1 has exactly one nonzero entry. Since O_1 is nonsingular, this shows that O_1 is a monomial matrix. This ends the proof. □

Remark. If $m = 1$ then the operator

$$\rho^{[2m,2m-2,2]} = \frac{1}{4}\left(I + \sigma_x^{\otimes 2} + -\sigma_y^{\otimes 2} + \sigma_z^{\otimes 2}\right) \tag{6.14}$$

is a rank one projector, since it is a sum of the form

$$\frac{1}{4}\sum_{M\in\mathcal{S}} M, \tag{6.15}$$

where $\mathcal{S}$ is a stabilizer on 2 qubits of cardinality $|\mathcal{S}| = 4$. In fact, we have seen in (2.16) in chapter 2 that $\mathcal{S}$ is the stabilizer of the EPR state. ◇

[2] A matrix is monomial if it is the product of a permutation matrix and a diagonal matrix.

6.3 Class of stabilizer states where LU=LC

We will now use the concept of minimal support to construct a class of stabilizer states $|\psi\rangle$ that satisfy $\text{LU}(\psi) = \text{LC}(\psi)$. In other words, every two LU equivalent states in this class are necessarily LC equivalent.

6.3.1 Main result

Denoting by $\mathcal{M}(\psi)$ the subgroup of $\mathcal{S}(\psi)$ generated by all minimal elements, we have the following result:

Theorem 6.4 *Let $|\psi\rangle$ be a (fully entangled) n-qubit stabilizer state such that σ_x, σ_y, σ_z occur on every qubit in $\mathcal{M}(\psi)$. Then $LU(\psi) = LC(\psi)$.*

Proof: Let $|\psi'\rangle \in \text{LU}(\psi)$ and fix $U = U_1 \otimes \cdots \otimes U_n \in U(2)^{\otimes n}$ such that $U|\psi\rangle = |\psi'\rangle$. We will show that U_i is a Clifford operation, for every $i = 1, \ldots, n$. Considering e.g. the first qubit, there exists a minimal element $M \in \mathcal{S}(\psi)$ such that $M_1 \neq \sigma_0$, say $M_1 = \sigma_x$. Let $\omega = \{1 = i_1, i_2, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, where $k = |\omega|$, denote the support of M. Then $A_\omega(\psi)$ is equal to either 1 or 3 from lemma 6.2. We will make a distinction between these two cases.

Firstly, suppose that $A_\omega(\psi) = 3$. Then $\rho_\omega(\psi)$ is LC equivalent to $\rho^{[|\omega|,|\omega|-2,2]}$ from the discussion below lemma 6.2. Moreover, as $|\psi'\rangle \in \text{LU}(\psi)$, the set ω is also a minimal support of $\mathcal{S}(\psi')$ with $A_\omega(\psi') = A_\omega(\psi) = 3$. Therefore, $\rho_\omega(\psi')$ is LC equivalent to $\rho^{[|\omega|,|\omega|-2,2]}$ as well. Using the notation $U_\omega = U_{i_1} \otimes \cdots \otimes U_{i_k}$, it follows from $U|\psi\rangle = |\psi'\rangle$ that U_ω maps $\rho_\omega(\psi)$ to $\rho_\omega(\psi')$ under conjugation. Using proposition 6.3, we then find that $U_\omega \in \mathcal{C}_k^l$, and, in particular, U_1 is a Clifford operation. Note that here it is impossible that $m = 1$ in proposition 6.3, since this implies that $\rho_\omega(\psi)$ is a pure state, which yields a contradiction since $|\psi\rangle$ is fully entangled. See also the remark under proposition proposition 6.3.

Secondly, let $A_\omega(\psi) = 1$. Then there exists another minimal element $N \in \mathcal{M}(\psi)$ such that $1 \in \text{supp}(N)$ and $M_1 \neq N_1$ from the assumption in the theorem, say $N_1 = \sigma_z$. Let $\mu = \text{supp}(N)$. Note that if $A_\mu(\psi) = 3$, we can apply the same argument as above and conclude that U_1 is a Clifford operation. On the other hand, suppose that $A_\mu(\psi) = 1$. Denoting $M_\omega = \alpha_M M_{i_1} \otimes \cdots \otimes M_{i_k}$, and N_μ analogously, we can write

$$\rho_\omega(\psi) = \frac{1}{2^{|\omega|}} \left(I_{|\omega|} + M_\omega \right)$$
$$\rho_\mu(\psi) = \frac{1}{2^{|\mu|}} \left(I_{|\mu|} + N_\mu \right). \tag{6.16}$$

Moreover, since the sets ω and μ are also minimal supports of $\mathcal{S}(\psi')$ with $A_\mu(\psi') = A_\omega(\psi') = 1$, there exist unique $M', N' \in \mathcal{S}(\psi')$ such that

$$\rho_\omega(\psi') = \frac{1}{2^{|\omega|}} \left(I_{|\omega|} + M'_\omega \right)$$

$$\rho_\mu(\psi') = \frac{1}{2^{|\mu|}}\left(I_{|\mu|} + N'_\mu\right), \tag{6.17}$$

where M'_ω and N'_μ are defined analogously to M_ω and N_μ. Now, as

$$\begin{aligned} U_\omega\rho_\omega(\psi)U_\omega^\dagger &= \rho_\omega(\psi') \\ U_\mu\rho_\mu(\psi)U_\mu^\dagger &= \rho_\mu(\psi'), \end{aligned} \tag{6.18}$$

where again we have used the notation $U_\omega = U_{i_1}\otimes\cdots\otimes U_{i_k}$ and analogously for U_μ, we have

$$\begin{aligned} U_1 M_1 U_1^\dagger &= \pm M'_1 \\ U_1 N_1 U_1^\dagger &= \pm N'_1 \end{aligned} \tag{6.19}$$

from (6.16)-(6.17). Using $M_1 = \sigma_x$ and $N_1 = \sigma_z$, The identities (6.19) show that U_1 is a Clifford operation.

Repeating the above arguments for all n qubits yields the result. □

Theorem 6.4 shows that it is sufficient that the group $\mathcal{M}(\psi)$ has a sufficiently rich structure in order for LU(ψ) to be equal to LC(ψ). To gain insight in which states meet the requirement of theorem 6.4, it is instructive to consider some sufficient conditions for this criterion to hold. Several sufficient conditions are summarized in the next proposition.

Proposition 6.5 *Let $|\psi\rangle$ be a stabilizer state on n qubits such that one of the assertions (i)-(iv) is true. Then $LU(\psi) = LC(\psi)$.*

(i) $\mathcal{S}(\psi) = \mathcal{M}(\psi)$, i.e. $\mathcal{S}(\psi)$ is generated by its minimal elements.

(ii) The stabilizer $\mathcal{S}(\psi)$ corresponds to a $GF(4)$-linear code.

(iii) For every $M \in \mathcal{S}(\psi)$ with nonminimal support, there exists a minimal support $\omega' \subset$ supp(M) such that $A_{\omega'}(\psi) = 3$.

(iv) There exists minimal supports $\omega_1, \omega_2, \ldots$ satisfying $3 = A_{\omega_1}(\psi) = A_{\omega_2}(\psi) = \ldots$, such that every $i \in \{1,\ldots,n\}$ belongs to at least one ω_j.

Proof: We will show that (i)-(iv) imply that σ_x, σ_y and σ_z occur on every qubit in $\mathcal{M}(\psi)$.

Firstly, using lemma 3 (stated below), one immediately finds that assertion (i) implies the desired result.

Secondly, suppose (ii) holds. Letting S be a generator matrix of $|\psi\rangle$, the space C_S then corresponds to a linear subspace $\tilde{C}$ of $\mathbb{F}_4^n$. The support of a vector in $\mathbb{F}_4^n$ and the notions concerning minimal support are defined in the natural way. We now claim that any linear subspace $\tilde{C}$ of $\mathbb{F}_4^n$ is generated by its minimal elements. To prove this claim, let $v = (v_1,\ldots,v_n) \in \tilde{C}$. We have to show that v is a linear combination of minimal elements of $\tilde{C}$. If v is a minimal element itself then we are done. If not, then there exists a minimal element

$w = (w_1, \ldots, w_n) \in \tilde{C}$ such that $\text{supp}(w) \subset \text{supp}(v)$. Let i be any element in the support of w. Note that the vector

$$v' := v - \frac{v_i}{w_i} w \tag{6.20}$$

belongs to $\tilde{C}$ since $\tilde{C}$ is a linear space. Moreover, by construction the ith component of v' is equal to zero, yielding

$$\text{supp}(v') \subsetneq \text{supp}(v). \tag{6.21}$$

It now follows from an induction argument that v' is a linear combination of minimal elements of $\tilde{C}$. But then the same $v = v' + (v_i/w_i)w$ is also a linear combination of minimal elements, since w is a minimal element of $\tilde{C}$. This yields the result.

Thirdly, we show that (iii) also implies (i): let $M \in \mathcal{S}(\psi)$ be an arbitrary nonzero stabilizer element. We have to show that M is a product of minimal elements. If M is minimal then we are done. For nonminimal M, we will prove the assertion by induction on $|\text{supp}(M)|$. Let ω' be a minimal support such that $\omega' \subset \text{supp}(M)$ and $A_{\omega'}(\psi) = 3$. As $A_{\omega'}(\psi) = 3$, there exists a minimal codeword $M' \in \mathcal{M}(\psi)$ with support equal to ω' such that M and M' are equal on the first qubit (see proof of lemma 1). Consequently, $|\text{supp}(MM')|$ is strictly smaller than $|\text{supp}(M)|$ and therefore $MM' \in \mathcal{M}(\psi)$ by induction. But then also $M \in \mathcal{M}(\psi)$, since M' is minimal. This shows that (iii) implies (i).

Fourthly, suppose that assertion (iv) holds. It then immediately follows from the proof of lemma 1 that σ_x, σ_y and σ_z occur on every qubit in $\mathcal{M}(\psi)$. $\square$

In the proof of proposition 6.5(i) we have used the following result:

Lemma 6.6 *Let $|\psi\rangle$ be a (fully entangled) stabilizer state on $n \geq 2$ qubits. Then all three Pauli matrices σ_x, σ_y, σ_z occur on every qubit in $\mathcal{S}(\psi)$.*

Proof: Let $|\psi\rangle$ be a (fully entangled) stabilizer state on $n \geq 2$ qubits. Consider e.g. the first qubit. Denote $\omega = \{2, \ldots, n\}$ and let $\mathcal{S}_\omega$ be the set consisting of all $M \in \mathcal{S}(\psi)$ such that $M_1 = \sigma_0$, which is a subgroup of $\mathcal{S}(\psi)$. Firstly, note that it is impossible that $\mathcal{S}_\omega = \mathcal{S}(\psi)$; indeed, if this were the case, then the set

$$\mathcal{S}_\omega^\times = \{M_\omega \mid M \in \mathcal{S}(\psi)\} \tag{6.22}$$

would be a stabilizer on $n-1$ qubits with cardinality 2^n, which is a contradiction (in (6.22), we have used the notation $M_\omega = \alpha_M M_2 \otimes \cdots \otimes M_n$ as before). Secondly, suppose that there exists an $a \in \{x, y, z\}$ such that $M_1 \in \{\sigma_0, \sigma_a\}$ for every $M \in \mathcal{S}(\psi)$ (and both σ_0 and σ_a occur). It is then easy to verify that

$$\mathcal{S}(\psi) = \mathcal{S}_\omega \cup M^a \mathcal{S}_\omega \tag{6.23}$$

where M^a is an arbitrary element in $\mathcal{S}(\psi)$ satisfying $M_1^a = \sigma_a$, and $M^a\mathcal{S}_\omega$ is the coset of $\mathcal{S}_\omega$ determined by the element M^a. Therefore, $|\mathcal{S}_\omega| = 2^{n-1}$ and the stabilizer (6.22) now has cardinality 2^{n-1}, consequently defining a stabilizer state $|\psi_\omega\rangle$ on $n-1$ qubits. Using the identities

$$\begin{aligned} |\psi\rangle\langle\psi| &= \frac{1}{2^n}\sum_{M\in\mathcal{S}} M \\ |\psi_\omega\rangle\langle\psi_\omega| &= \frac{1}{2^{n-1}}\sum_{N\in\mathcal{S}_\omega^\times} N \end{aligned} \tag{6.24}$$

and (6.23), it easily follows that

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + M^a)\,(\sigma_0 \otimes |\psi_\omega\rangle\langle\psi_\omega|) \tag{6.25}$$

and therefore $\mathrm{Tr}_1\,\{|\psi\rangle\langle\psi|\} = |\psi_\omega\rangle\langle\psi_\omega|$. This shows that $\mathrm{Tr}_1|\psi\rangle\langle\psi|$ is a pure state, which leads to a contradiction, as $|\psi\rangle$ is fully entangled. It follows that σ_x, σ_y, σ_z must occur on the first qubit of $\mathcal{S}(\psi)$. Repeating the above argument for all qubits yields the result. $\square$

Clearly, conditions (iii) and (iv) are much more operational than theorem 6.4, as it is sufficient to know (only part of) the list of invariants $A_\omega(\psi)$ of a given state $|\psi\rangle$ in order to conclude that LU(ψ) is equal to LC(ψ). Also condition (ii) is easy to check, as we saw in chapter 2.

Let us give an example of a graph states for which theorem 6.4 holds.

Example. Consider the ring cluster graph on 5 vertices, depicted in Fig. 2.1 in chapter 2. The corresponding graph state $|RC_5\rangle$ has a generator matrix

$$S^T = \left[\begin{array}{ccccc|ccccc} \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{array}\right]^T . \tag{6.26}$$

Denoting the left 5×5 block of the above matrix by θ (i.e., the adjacency matrix of RC_5), one immediately sees that $\mathrm{rank}_{\mathbb{F}_2}\theta\langle\{1,2,3\}\rangle = 2$ and therefore $B_{\{1,2,3\}}(RC_5) = 2$ using (2.64). This shows that there is exactly one nontrivial element $I \neq M \in \mathcal{S}(RC_5)$ with $\mathrm{supp}(M) \subseteq \{1,2,3\}$. Moreover, the second column of S has support equal to $\{1,2,3\}$ and we can conclude that $\{1,2,3\}$ is a minimal support of $\mathcal{S}(RC_5)$. By symmetry, also $\{2,3,4\}$, $\{3,4,5\},\ldots$ are minimal supports and the corresponding minimal elements of $\mathcal{S}(RC_5)$ are exactly the columns of S. It follows that $\mathcal{S}(RC_5) = \mathcal{M}(RC_5)$. Using proposition 6.5 then yields LU(RC_5) = LC(RC_5).

6.3.2 Discussion

We now discuss the above results. Our main result was the presentation of a subclass of stabilizer states, such that any two LU equivalent stabilizer states in this class must also be LC equivalent. To construct our class, a central concept was that of minimal support. In particular, we showed that if the subgroup $\mathcal{M}(\psi)$ generated by all minimal elements in a stabilizer $\mathcal{S}(\psi)$ has a sufficiently rich structure, then the LU equivalence class and the LC equivalence class of the state $|\psi\rangle$ coincide.

The main objectives of this chapter were to give support to the conjecture that LU$(\psi) =$ LC(ψ) for every stabilizer state and to investigate the relevance of the notion of minimal support in this problem. The next insight that needs to be gained in the present research, is what constraints are imposed on those stabilizer states that do not meet the requirement of theorem 6.4 and what the structure and the size of this remaining set of states is. It is in fact not easy to find many examples of states outside of our class, and it is not unlikely that the constraints imposed on such states are sufficiently strict, such that the question whether LU$(\psi) =$ LC(ψ) for these remaining states can be settled by considering these states case by case. We note that it is not our hope that our class covers all stabilizer states. Indeed, there do exist states that do not belong to the class we have considered. An important example is the generalized GHZ state $|GHZ_n\rangle$ on n qubits. All elements $M \in \mathcal{M}(GHZ_n)$ satisfy $M_i \in \{\sigma_0, \sigma_z\}$, for every $i = 1, \ldots, n$. This easily follows from the definition of $\mathcal{S}(GHZ_n)$. Therefore, $|GHZ_n\rangle$ does not meet the requirement of theorem 6.4. However, also for the GHZ state (and therefore for every state in its LC equivalence class) one has LU$(GHZ_n) =$ LC(GHZ_n). This is stated in the following proposition.

Proposition 6.7 *Let $|\psi\rangle$ be a fully entangled stabilizer state. Then $|\psi\rangle \in$ LC(GHZ_n) if and only if $A_\omega(\psi) = 1$ for every $\omega \in \{\{1,2\},\{2,3\},\ldots\}$. Consequently, LU$(GHZ_n) =$ LC(GHZ_n).*

Proof: If $|\psi\rangle \in$ LU(GHZ_n) then clearly $A_\omega(\psi) = 1$ for every $\omega \in \{\{1,2\},\{2,3\}, \ldots\}$. Conversely, suppose that $|\psi\rangle$ is a fully entangled stabilizer state on n qubits such that $A_\omega(\psi) = 1$ for every $\omega \in \{\{1,2\},\{2,3\},\ldots\}$. Then $\mathcal{S}(\psi)$ has $n-1$ elements of the form

$$\begin{aligned}
&\alpha_1\ \sigma_{k_1} \otimes \sigma_{k_2} \otimes \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0,\\
&\alpha_2\ \sigma_0 \otimes \sigma_{l_2} \otimes \sigma_{l_3} \otimes \sigma_0 \otimes \cdots \otimes \sigma_0,\\
&\alpha_3\ \sigma_0 \otimes \sigma_0 \otimes \sigma_{m_3} \otimes \sigma_{m_4} \otimes \cdots \otimes \sigma_0,\\
&\ldots
\end{aligned} \tag{6.27}$$

where $\alpha_1, \alpha_2, \alpha_3, \dots \in \{\pm 1\}$ and $k_1, k_2, l_2, l_3, \dots \in \{x, y, z\}$. Moreover, $k_2 = l_2$, $l_3 = m_3, \ldots$ since $\mathcal{S}(\psi)$ is an Abelian group. This yields $n-1$ independent elements of $\mathcal{S}(\psi)$. Therefore, to obtain a complete set of n generators, we need one additional element. We claim that any such additional generator M of $\mathcal{S}(\psi)$ must have full support and additionally satisfy $M_1 \neq \sigma_{k_1}$, $M_2 \neq \sigma_{l_2}, \ldots$: indeed, this readily follows from lemma 6.6. We therefore obtain a set of generators of the form

$$\gamma_1\ \sigma_{a_1} \otimes \sigma_{a_2} \otimes \sigma_{a_3} \otimes \sigma_{a_4} \otimes \cdots \otimes \sigma_{a_n},$$

$$\begin{aligned}
&\gamma_2\ \sigma_{b_1}\otimes\sigma_{b_2}\otimes\sigma_0\otimes\sigma_0\otimes\cdots\otimes\sigma_0,\\
&\gamma_3\ \sigma_0\otimes\sigma_{b_2}\otimes\sigma_{b_3}\otimes\sigma_0\otimes\cdots\otimes\sigma_0,\\
&\gamma_4\ \sigma_0\otimes\sigma_0\otimes\sigma_{b_3}\otimes\sigma_{b_4}\otimes\cdots\otimes\sigma_0,\\
&\ldots,
\end{aligned} \tag{6.28}$$

with $\gamma_i \in \{\pm 1\}$, $a_i, b_i \in \{x, y, z\}$ and $a_i \neq b_i$ for every $i = 1, \ldots, n$. One can now always find a local unitary operator which maps these operators to the set of generators 2.32, which shows that $|\psi\rangle \in LC(GHZ_n)$. Finally, suppose that $|\psi\rangle$ is a stabilizer state LU equivalent to $|GHZ_n\rangle$. Then $|\psi\rangle$ is fully entangled and $A_\omega(\psi) = A_\omega(GHZ) = 1$ for every $\omega \in \{\{1,2\},\{2,3\},\ldots\}$. But then $|\psi\rangle \in LC(GHZ_n)$ from the above. This ends the proof. □

Therefore, while the GHZ state does not belong to our subclass of stabilizer states, it does still satisfy LU(GHZ_n) = LC(GHZ_n), which can be proven with simple arguments.

6.4 Role of invariants

An entirely different approach one can adopt to settle whether LU = LC is to use the study of local invariants that we performed in chapter 5. We showed that both LU and LC invariants of stabilizer states have very similar presentations in terms of dimensions of certain subspaces of $C_S^{\times r}$. Therefore, a straightforward approach to prove that LU=LC is to show that every LC invariant $B^\Omega_{n,r}(\psi)$ is also an LU invariant. Note that we have proven this assertion for $r = 1$ and $r = 2$. The proof for general r, however, seems to be hard. On another note, we also ask the question whether the invariants $B^\Omega_{n,r}$, where $r = 1, 2$, form a complete set of LC invariants. We note that it already has been conjectured and later disproven that the invariants $B^\Omega_{n,1}$, corresponding to the functions B_ω, form a complete set of LC invariants. Indeed, the invariants $B_\omega(G)$, where G is a graph, correspond to the connectivity function of G, which is known to constitute a non-complete set of LC invariants (see chapter 5). We now ask whether extending the set $\{B_\omega\}$ to the set $\{B_\omega, B^\omega_{n,2}\}$ yields a complete set of LC invariants. The answer to this question is to date unknown.

6.5 Conclusion

In conclusion, we have studied the relation between local unitary equivalence and local Clifford equivalence of stabilizer states. In particular, we have investigated the question whether every two LU equivalent stabilizer states are also LC equivalent. We have shown that the answer to this question is positive for a large class of stabilizer states, which can be regarded as an extension of the set of those stabilizer states that correspond to $\mathbb{F}_4$-linear codes. We have given sufficient conditions for a state to belong to our specific class. However, the answer to the general question whether $\mathrm{LU}(\psi) = \mathrm{LC}(\psi)$ for every stabilizer state $|\psi\rangle$ is to date unknown. We formulate it as a conjecture:

Conjecture 6.8 *$LU(\psi) = LC(\psi)$ for every stabilizer state $|\psi\rangle$.*

This ends our study of LU versus LC equivalence of stabilizer states.

References

The main results in this chapter were the topic of our work [50] (thm. 6.4, prop. 6.5, prop. 6.7).

There is in fact not much literature dealing with the question whether every two LU equivalent stabilizer states are also LC equivalent; in fact, we can only refer to Rains [34]. The notion of minimal support can be traced back to classical coding theory, where it has been studied quite recently in e.g. Ref. [1] (see also refs within).

Chapter 7

Conclusion

In this thesis we have studied local equivalence of stabilizer states and codes. This problem is relevant in the study of multipartite entanglement, quantum error-correction and quantum computing. In our study of local equivalence, we mostly used a description of stabilizer states and codes in terms of binary algebra; our proofs, calculations and results are almost always formulated within this description.

We studied several aspects of local equivalence of stabilizer states and codes. Our main contributions were the following:

- We proved that every two SLOCC equivalent stabilizer states are necessarily LU equivalent [48].
- We gave a characterization of when a stabilizer state corresponds to a GF(4)-linear classical code [50].
- We performed a detailed study of LC equivalence of graph states in terms of transformations of the associated graphs and adjacency matrices.
  - We considered fractional linear transformations of adjacency matrices and used these transformations to count the number of graph states in an LC equivalence class.
  - We described LC equivalence of graph states in terms of a single graph transformation called local complementation [47].
  - We used this characterization in terms of local complementation to obtain a polynomial-time algorithm to recognize LC equivalence of stabilizer states [45].
- We constructed a finite complete set of invariants that characterizes the LC equivalence class of any stabilizer state and code. [46].
- We studied an existing complete set of LU invariant polynomials and evaluated these invariants in an arbitrary stabilizer state or code, yielding a

complete translation of these invariants in the binary stabilizer framework. We showed that for low degrees these invariants coincide with the above LC invariants. [49]

- We constructed a large class of stabilizer states such that any two LU equivalent stabilizer states in this class are also LC equivalent. We conjecture that this claim holds for all stabilizer states. [50]

In the course of this PhD, many interesting problems presented itself. The following is a list of open problems in the broad context of stabilizer theory, graph theory, invariant theory, etc.

- Most importantly, we would like to prove that every two LU equivalent stabilizer states are also LC equivalent.

- In our conclusion in chapter 4 we mention the probable link between our algebraic description of local complementation using fractional linear transformations, and the theory of isotropic systems developed by Bouchet [3]. A further investigation of this connection is certainly appropriate − we note that this is ongoing research.

- Near the end of this PhD we noticed the work of Glynn [17], who studied LC equivalence of graph states as well and also proved that two graph states are LC equivalent iff the corresponding graphs are related by a sequence of local complementations. However, the mathematics involved in his work is entirely different from our work and is situated more in the context of finite- geometry. It would be interesting to explore the links with our work.

- It has come to our attention that the study of LC equivalence of graph states is, surprisingly, also of interest in classical cryptography, where this problem is relevant in the study of so-called *bent functions*. It would be interesting to see whether insights from our QIT point of view may be of use in this entirely different field of research, and vice versa.

- We are convinced that the complete set of LC invariants presented in chapter 5 contains many redundancies; we believe that a considerably smaller subset of this set of invariants is still sufficient to characterize LC equivalence of stabilizer states and/or codes. The construction of such a "minimal" set of LC invariants is an important and difficult open problem.

- In our investigations on LU and LC invariants we briefly touched the study of the Molien series of the groups $U(2)^{\otimes n}$ and $\mathcal{C}_n^l$. From the perspective of entanglement theory and coding theory it would be interesting to have some insights in these Molien series.

- Surprisingly, the invariant theory of the Clifford group is important in the study of classical binary codes, more specifically in the study of so-called generalized weight polynomials [39, 30]. It would be interesting to investigate the relevance of the stabilizer formalism in this context.

- ...

Appendix A

Basic concepts of quantum mechanics

In this appendix we outline the basic concepts of the theory of quantum mechanics. The text is based on [8].

Hilbert space and Dirac notation

Associated to any isolated quantum system is a (finite- or infinite-dimensional) complex *Hilbert space* $\mathcal{H}$, which is called the *state space* of the system. In this thesis Hilbert spaces are always finite-dimensional.

The standard notation in quantum mechanics to denote a unit vector in $\mathcal{H}$ is the following:

$$|\psi\rangle. \tag{A.1}$$

The notation $|\cdot\rangle$ is the *Dirac notation*; it is used to indicate that the object (A.1) is a vector[1]. If $\mathcal{H}$ is a d-dimensional Hilbert space, we fix an arbitrary orthonormal basis of $\mathcal{H}$ and identify every element of $\mathcal{H}$ with the d-dimensional complex vector containing its coordinates with respect to this basis, yielding an identification between the spaces $\mathcal{H}$ and $\mathbb{C}^d$. Once the aforementioned orthonormal basis has been fixed, it is in QIT terminology called the *computational basis* of $\mathcal{H}$ and is usually denoted by

$$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{A.2}$$

Thus, an arbitrary unit vector

$$|\psi\rangle = \sum_{i=0}^{d-1} \psi_i |i\rangle \ \in \mathcal{H}, \tag{A.3}$$

[1] Typically, the dirac notation is not used for the zero vector, which is simply denoted by 0.

where the ψ_is are complex numbers satisfying $\sum_i |\psi_i|^2 = 1$, is identified with its coordinate vector $(\psi_0, \ldots, \psi_{d-1}) \in \mathbb{C}^d$. We will also identify d-tuples of complex numbers with $d \times 1$ column matrices, as is commonly done.

Given an arbitrary vector

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d-1} \end{bmatrix} \in \mathcal{H}, \tag{A.4}$$

one denotes by $\langle\psi|$ the vector dual to $|\psi\rangle$, which is written as a $1 \times d$ row vector

$$\langle\psi| = \begin{bmatrix} \bar{\psi}_0 & \ldots & \bar{\psi}_{d-1} \end{bmatrix}, \tag{A.5}$$

where the overbar denotes complex conjugation. Given two vectors

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d-1} \end{bmatrix}, \ |\phi\rangle = \begin{bmatrix} \phi_0 \\ \vdots \\ \phi_{d-1} \end{bmatrix} \in \mathcal{H}, \tag{A.6}$$

the *inner product* $\langle\psi|\phi\rangle \in \mathbb{C}$ is defined as

$$\langle\psi|\phi\rangle = \begin{bmatrix} \bar{\psi}_0 & \ldots & \bar{\psi}_{d-1} \end{bmatrix} \begin{bmatrix} \phi_0 \\ \vdots \\ \phi_{d-1} \end{bmatrix} = \sum_{i=0}^{d-1} \bar{\psi}_i \phi_i. \tag{A.7}$$

Thus, $\langle\psi|\phi\rangle$ is the standard inner product of the vectors $|\psi\rangle$ and $|\phi\rangle$. The *outer product* $|\psi\rangle\langle\phi|$ of the vector $|\psi\rangle$ with the vector $\langle\phi|$ is the rank one operator on $\mathcal{H}$ defined as

$$|\psi\rangle\langle\phi| = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d-1} \end{bmatrix} \begin{bmatrix} \bar{\phi}_0 & \ldots & \bar{\phi}_{d-1} \end{bmatrix} = \begin{bmatrix} \psi_0\bar{\phi}_0 & \ldots & \psi_0\bar{\phi}_{d-1} \\ \vdots & \vdots & \vdots \\ \psi_{d-1}\bar{\phi}_0 & \ldots & \psi_{d-1}\bar{\phi}_{d-1} \end{bmatrix} \tag{A.8}$$

(to be precise, the matrix on the r.h.s. of (A.8) is the representation of the operator $|\psi\rangle\langle\phi|$ in the computational basis of $\mathcal{H}$). If A is an arbitrary linear operator on $\mathcal{H}$ with matrix representation $(a_{ik}) \in \mathbb{C}^{d\times d}$ in the computational basis, then $A|\psi\rangle \in \mathcal{H}$ is the vector defined by

$$A|\psi\rangle = \begin{bmatrix} a_{00} & \ldots & a_{0,d-1} \\ \vdots & \vdots & \vdots \\ a_{d-1,0} & \ldots & a_{d-1,d-1} \end{bmatrix} \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d-1} \end{bmatrix}. \tag{A.9}$$

Finally, the notation $\langle\phi|A|\psi\rangle$ is used to denote the inner product between the vectors $|\phi\rangle$ and $A|\psi\rangle$.

The simplest (nontrivial) example of a Hilbert space is the *one-qubit Hilbert space* $\mathbb{H}_1 \cong \mathbb{C}^2$, which is 2-dimensional. The standard basis or computational basis in $\mathbb{H}_1$ is denoted by $\{|0\rangle, |1\rangle\}$, and we have the identification

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{A.10}$$

An arbitrary unit vector $|\psi^{(1)}\rangle$ in $\mathbb{H}_1$ has the form

$$|\psi^{(1)}\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \tag{A.11}$$

where a, b are complex coefficients satisfying $|a|^2 + |b|^2 = 1$.

Composite systems and tensor products

The state space of a composite quantum system is the tensor product of the state spaces of the component systems. Thus, a quantum system composed of two subsystems with state spaces $\mathcal{H}_1 \cong \mathbb{C}^{d_1}$ and $\mathcal{H}_2 \cong \mathbb{C}^{d_2}$, respectively, has a d_1d_2-dimensional state space given by given by $\mathcal{H}_1 \otimes \mathcal{H}_2 \cong \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} = \mathbb{C}^{d_1d_2}$.

Let us review some basic definitions and properties concerning tensor products.

(i) Let the sets $\{|i\rangle_1\}_{i=0}^{d_1-1}$, $\{|j\rangle_2\}_{j=0}^{d_2-1}$ be the computational bases of the spaces $\mathcal{H}_1$, $\mathcal{H}_2$, respectively. Then the set of d_1d_2 vectors

$$\{|i\rangle_1 \otimes |j\rangle_2\}_{i,j} \equiv \{|i\rangle_1|j\rangle_2\}_{i,j} \tag{A.12}$$

is taken to be the computational basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$. A general unit vector $|\psi\rangle_{12} \in \mathcal{H}_1 \otimes \mathcal{H}_2$ has the form

$$|\psi\rangle_{12} = \sum_{ij} \psi_{ij}|i\rangle_1|j\rangle_2, \tag{A.13}$$

where the ψ_{ij}s are complex coefficients satisfying $\sum_{ij} |\psi_{ij}|^2 = 1$. We identify vectors in $\mathcal{H}_1 \otimes \mathcal{H}_2$ with their coordinate vectors with respect to the basis $\{|i\rangle_1|j\rangle_2\}$. The inner product of two vectors in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined in the natural way as the inner product of their coordinate vectors with respect to the computational basis.

(ii) Let

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d_1-1} \end{bmatrix} \in \mathcal{H}_1, \; |\psi'\rangle = \begin{bmatrix} \psi'_0 \\ \vdots \\ \psi'_{d_2-1} \end{bmatrix} \in \mathcal{H}_2 \tag{A.14}$$

be two vectors. Then the coordinate vector of $|\psi\rangle \otimes |\psi'\rangle$ with respect to the computational basis $\{|i\rangle_1|j\rangle_2\}_{i,j}$ is given by the Kronecker product[2] of the coordinate vector of $|\psi\rangle$ w.r.t. the basis $\{|i\rangle_1\}$ with the coordinate vector of $|\psi'\rangle$ w.r.t. the basis $\{|j\rangle_2\}$:

$$\begin{aligned} |\psi\rangle \otimes |\psi'\rangle &= (\sum_i \psi_i|i\rangle_1) \otimes (\sum_j \psi'_j|j\rangle_2) \\ &= \sum_{i,j} \psi_i\psi'_j|i\rangle_1|j\rangle_2 = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{d_1-1} \end{bmatrix} \otimes \begin{bmatrix} \psi'_0 \\ \vdots \\ \psi'_{d_2-1} \end{bmatrix}, \end{aligned} \tag{A.15}$$

where in the last equality we have identified the vector $|\psi\rangle \otimes |\psi'\rangle$ with its coordinate vector. We note that it is common to use the notation

$$|\psi\rangle|\psi'\rangle \equiv |\psi\rangle \otimes |\psi'\rangle. \tag{A.16}$$

(iii) Let A, B be operators on $\mathcal{H}_1$, $\mathcal{H}_2$ with representations $(a_{ik}) \in \mathbb{C}^{d_1\times d_1}$, $(b_{jl}) \in \mathbb{C}^{d_2\times d_2}$ with respect to the bases $\{|i\rangle_1\}$, $\{|j\rangle_2\}$, respectively. Then $A\otimes B$ is (by definition) the operator on $\mathcal{H}_1\otimes\mathcal{H}_2$ with matrix representation in the basis $\{|i\rangle_1|j\rangle_2\}_{i,j}$ given by the Kronecker product $(a_{ik})\otimes(b_{jl})$.

For example, the state space of a system of 2 qubits is the Hilbert space

$$\mathbb{H}_2 \equiv \mathbb{H}_1 \otimes \mathbb{H}_1 \cong \mathbb{C}^4. \tag{A.17}$$

A basis of this space is given by the set of 4 vectors $\{|a\rangle|b\rangle\}_{a,b\in\mathbb{F}_2}$. It is common to denote $|ab\rangle \equiv |a\rangle|b\rangle$ for every $a, b \in \mathbb{F}_2$. A unit vector $|\psi^{(2)}\rangle$ in $\mathbb{H}_2$ can be expanded as

$$|\psi^{(2)}\rangle = \sum_{a,b\in\mathbb{F}_2} \psi_{ab}|ab\rangle, \tag{A.18}$$

where the ψ_{ab}s are complex coefficients satisfying $\sum_{a,b} |\psi_{ab}|^2 = 1$.

In this thesis we are interested in many-qubit systems, which have a state space $\mathbb{H}_n = \mathbb{H}_1^{\otimes n}$ for some $n \in \mathbb{N}_0$. A unit vector $|\psi^{(n)}\rangle$ in $\mathbb{H}_n$ can be expanded as

$$|\psi^{(n)}\rangle = \sum_{x\in\mathbb{F}_2^n} \psi_x|x\rangle, \tag{A.19}$$

[2]The *Kronecker product* of two matrices is defined as follows; letting $A = (a_{uv})$ be an $m \times n$ matrix and $B = (b_{xy})$ a $p \times q$ matrix, then $A \otimes B$ is the $mp \times nq$ matrix defined by

$$\begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}.$$

The Kronecker product $v \otimes v'$ of two vectors $v \in \mathbb{C}^{d_1}$ and $v' \in \mathbb{C}^{d_2}$ is obtained by regarding these vectors as $d_1\times 1$ and $d_2\times 1$ column matrices, respectively, and using the above definition of the tensor product of matrices.

where $\psi_x \in \mathbb{C}$ for every $x \in \mathbb{F}_2^n$, such that $\sum_x |\psi_x|^2 = 1$, and where we have denoted the computational basis states by $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$, for every $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

Density matrices

The *state* of a quantum system with state space $\mathcal{H} \cong \mathbb{C}^d$ is described by a positive operator ρ on $\mathcal{H}$ with trace equal to one, which is called a *density operator* (or *density matrix*)[3]. Every density operator ρ can be written (generically in a non-unique way) as a sum of the following form:

$$\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|, \tag{A.20}$$

where $N \in \mathbb{N}_0$, $\{p_i\}$ is a probability distribution (i.e., a collection of positive real numbers satisfying $\sum_i p_i = 1$), and $\{|\psi_i\rangle\}$ is a collection of unit vectors in $\mathcal{H}$. Note that the rank one operators $|\psi_i\rangle\langle\psi_i|$ are density operators in their own right, as they are indeed positive operators with trace equal to 1. Density matrices of the form $|\phi\rangle\langle\phi|$ are called *pure states* and correspond to states of maximal knowledge. Thus, the above expansion states that every density operator can be written as a convex sum of pure states. This expansion gives rise to the *ensemble interpretation* of a density matrix, which states that the density matrix ρ describes a system that is in the pure state $|\psi_i\rangle$ with probability p_i, for every $i = 1, \ldots, N$.

If ρ is a pure state, then the vector $|\psi\rangle$ satisfying $\rho = |\psi\rangle\langle\psi|$ is defined uniquely up to a global phase factor. As this overall phase factor is irrelevant in the present research, we will often refer to an arbitrary unit vector as a "pure state"as well.

Consider a composite system with state space $\mathcal{H}_1 \otimes \mathcal{H}_2 \cong \mathbb{C}^{d_1 d_2}$. If ρ_{12} is a state of the composed system, then the state ρ_1 of the subsystem 1 is given by

$$\rho_1 = \mathrm{Tr}_2\left(\rho_{12}\right), \tag{A.21}$$

where Tr_2 is a linear map of operators known as the *partial trace over the system 2.* The partial trace Tr_2 maps an operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$ to an operator on $\mathcal{H}_1$ and is defined by

$$\mathrm{Tr}_2\left(|i\rangle_1\langle k|_1 \otimes |j\rangle_2\langle l|_2\right) = \delta_{jl} |i\rangle_1\langle k|_1, \tag{A.22}$$

for every $i, k \in \{0, \ldots, d_1 - 1\}$ and $j, l \in \{0, \ldots, d_2 - 1\}$, where the sets $\{|i\rangle_1\}_{i=0}^{d_1-1}$, $\{|j\rangle_2\}_{k=0}^{d_2-1}$ are the computational bases of $\mathcal{H}_1$, $\mathcal{H}_2$, respectively,

[3]We emphasize that a general state of a quantum system is *not* given by an element of the state space, i.e., a vector in $\mathcal{H}$. We will see below that unit vectors in $\mathcal{H}$ do define particular types of states, called *pure states*, but a quantum state in its general definition is described by a density operator as we define here.

as before. The state ρ_1 is called the *reduced density operator* for system 1. The partial trace over system 1 and the reduced density operator ρ_2 are defined analogously.

For example, consider the pure state $|\psi^{(2)}\rangle$ in (A.18). Denoting

$$\Psi = \begin{bmatrix} \psi_{00} & \psi_{01} \\ \psi_{10} & \psi_{11} \end{bmatrix}, \tag{A.23}$$

it is straightforward to show that $|\psi^{(2)}\rangle$ has the following reduced density operators

$$\mathrm{Tr}_2(|\psi^{(2)}\rangle\langle\psi^{(2)}|) = \Psi\Psi^\dagger, \quad \mathrm{Tr}_1(|\psi^{(2)}\rangle\langle\psi^{(2)}|) = \Psi^T\Psi^*. \tag{A.24}$$

Unitary evolution

The evolution of a *closed* quantum system with state space $\mathcal{H}$ is described by a *unitary transformation*. That is, the state ρ of the system at time t is related to the state ρ' of the system at time t' by a unitary operator U on $\mathcal{H}$ which depends only on the times t and t',

$$\rho' = U\rho U^\dagger. \tag{A.25}$$

Measurements

A quantum measurement (or POVM[4] measurement) of a system with state space $\mathcal{H}$ is described by a collection of *measurement operators* $\{A_m\}$, which are operators on $\mathcal{H}$. The index m refers to the measurement outcomes that may occur in the experiment. Every measurement outcome m occurs with a certain probability. If the state of the quantum system is ρ immediately before the measurement then the probability p_m of obtaining the outcome m is equal to

$$p_m = \mathrm{Tr}(A_m^\dagger A_m \rho). \tag{A.26}$$

Moreover, when the outcome of the measurement is m, then the state of the system after the measurement is

$$\frac{A_m \rho A_m^\dagger}{\mathrm{Tr}(A_m \rho A_m^\dagger)}. \tag{A.27}$$

The measurement operators satisfy the completeness relation $\sum_m A_m^\dagger A_m = I$. This ensures that the numbers $\{\mathrm{Tr}(A_m^\dagger A_m \rho)\}_m$ form a probability distribution for every ρ.

[4]The letters POVM are short for *positive operator-valued measure*.

If all the operators $A_m \equiv P_m$ are orthogonal projectors, i.e., if they satisfy $P_m^2 = P_m$ and $P_m^\dagger = P_m$, then the corresponding measurement is called a von Neumann measurement. In the case of a von Neumann measurement, the formulas (A.26)-(A.27) are simplified as follows:

$$p_m = \mathrm{Tr}(P_m \rho) \tag{A.28}$$

and the state after the measurement is

$$\frac{P_m \rho P_m}{\mathrm{Tr}(P_m \rho)}. \tag{A.29}$$

Local operations

A local operation on a composite quantum system is an operator that acts on each of the subsystems of the composite system separately. In this thesis we consider two main classes of local operations, viz. local unitary (LU) operations and stochastic local operations assisted by classical communication (SLOCC). We note that LC equivalence is a specific kind of LU equivalence.

(i) Consider e.g. a 2-qubit state ρ. A *local unitary operator* is then an element U of $U(2)^{\otimes 2}$, which has the form $U = U_1 \otimes U_2$, where $U_i \in U(2)$ for every $i = 1, 2$. If ρ is mapped to $U\rho U^\dagger$ then $\rho_1 \equiv \mathrm{Tr}_2(\rho)$ is mapped to $U_1 \rho_1 U_1^\dagger$ and $\rho_2 \equiv \mathrm{Tr}_1(\rho)$ is mapped to $U_2 \rho_2 U_2^\dagger$. This illustrates that the 1-qubit unitaries U_1 and U_2 constituting the operator U act independently on their part of the system. A local unitary operation on an n-qubit system has the form

$$U = U_1 \otimes \cdots \otimes U_n, \tag{A.30}$$

where $U_i \in U(2)$ for every $i = 1, \ldots, n$.

(ii) An *SLOCC operator* on an n-qubit system is an element A of $SL(2, \mathbb{C})^{\otimes n}$, which has the form

$$A = A_1 \otimes \cdots \otimes A_n, \tag{A.31}$$

where $A_i \in SL(2, \mathbb{C})$ for every $i = 1, \ldots, n$. The letters SLOCC are short for *stochastic local operations and classical communication*; the reason for this terminology is the following. Suppose that an n-qubit system is in a state ρ and that each of the n parties performs a *local* POVM measurement, i.e., every party i performs a measurement with measurement operators $\{A_m^{(i)}\}_{m=1}^{N_i}$ acting on the ith qubit only, for every $i = 1, \ldots, n$. Denoting the outcome of the ith local measurement by m_i, for every

$i = 1, \ldots, n$, it follows that after every party has implemented its measurement, the state ρ has collapsed to the state

$$\left\{A^{(1)}_{m_1} \otimes \cdots \otimes A^{(n)}_{m_n}\right\} \rho \left\{A^{(1)}_{m_1} \otimes \cdots \otimes A^{(n)}_{m_n}\right\}^\dagger \tag{A.32}$$

up to a normalization. Note that $[A^{(i)}_k, A^{(j)}_m] = 0$ for every k, m and $i \neq j$, such that the order in which the measurements are performed by the n parties does not affect which final output state is eventually obtained. It follows from (A.32) that this final state is an element of the set

$$S_{\text{SLOCC}}(\rho) = \left\{A\rho A^\dagger \mid A \in (\mathbb{C}^{2\times 2})^{\otimes n}\right\}. \tag{A.33}$$

Conversely, it is clear that every state in the set $S_{\text{SLOCC}}(\rho)$ can be realized as a possible outcome of a scheme of n one-qubit measurements implemented as above. Note that every element in $S_{\text{SLOCC}}(\rho)$ can typically be obtained with a non-unit probability − hence the term *stochastic* in SLOCC.

A possible procedure for practically realizing a prescribed state $\rho' = (A_1 \otimes \cdots \otimes A_n)\rho(A_1 \otimes \cdots \otimes A_n)^\dagger$ in the set $S_{\text{SLOCC}}(\rho)$ is the following. First, every party i devises a local measurement experiment such that the operator $A_i \otimes I$ belongs to its set of measurement operators, for every $i = 1, \ldots, n$. Then every party implements its measurement, collapsing ρ to a final state ρ'', which may or may not be equal to ρ' depending on the outcomes of the different measurements. Then the n parties communicate their outcomes to each other, such that they can decide whether the state ρ'' coincides with the desired state ρ'.

Note that the above explains the notion of *classical communication* in SLOCC: the n parties need some means of communicating their measurement outcomes to each other in order to decide whether they have obtained the correct final state.

Finally, the reason for considering only *determinant 1* operations is the following: in this dissertation we are interested in transformations which map a state ρ to a state $\rho' \in S_{\text{SLOCC}}(\rho)$ and which can also be inverted, since we consider *equivalence* of states under the above operations. Two states ρ and ρ' on n qubits are called SLOCC equivalent if there exists an operator $B \in GL(2, \mathbb{C})^{\otimes n}$ such that $B\rho B^\dagger \sim \rho'$. One can readily verify that this is equivalent to requiring the existence of an operator $A \in SL(2, \mathbb{C})^{\otimes n}$ such that $A\rho A^\dagger \sim \rho'$. Therefore, we only consider determinant 1 local operations.

It is important to note that, while LU and SLOCC equivalence have definitions that are mathematically rather similar, the physical significance of these equivalences is very different, as we have illustrated above. Most importantly, LU transformations occur with unit probability, while SLOCC transformations do not.

List of Publications

- J. Dehaene, M. Van den Nest, B. De Moor, F. Verstraete. Local permutations of products of Bell states and entanglement distillation. *Phys. Rev. A* 67, 022310 (2003). `quant-ph/0207154`.
- M. Van den Nest, J. Dehaene, B. De Moor. Graphical description of the action of local Clifford operations on graph states. *Phys. Rev. A* 69, 022316 (2004). `quant-ph/0308151`.
- M. Van den Nest, J. Dehaene, B. De Moor. Local invariants of stabilizer codes. *Phys. Rev. A* 70, 032323 (2004). `quant-ph/0404106`.
- M. Van den Nest, J. Dehaene, B. De Moor. Efficient algorithm to recognize local Clifford equivalence of graph states. *Phys. Rev. A* 70, 034302 (2004). `quant-ph/0405023`.
- M. Van den Nest, J. Dehaene, B. De Moor. Local equivalence of stabilizer states. *Proceedings of the 16th International Symposium of Mathematical Theory of Networks and Systems (MTNS2004)*, K.U. Leuven, 5-9 Juli 2004.
- M. Van den Nest, J. Dehaene, B. De Moor. Invariants of the local Clifford group. *Phys. Rev. A* 71, 022310 (2005). `quant-ph/0410035`.
- M. Van den Nest, J. Dehaene, B. De Moor. Local unitary versus local Clifford equivalence of stabilizer states. Accepted for publication in *Phys. Rev. A*. `quant-ph/0411115`.
- M. Van den Nest, J. Dehaene, B. De Moor. Finite set of invariants to characterize local Clifford equivalence of stabilizer states. Submitted to *Phys. Rev. A*. `quant-ph/0410165`.

Curriculum Vitae

Maarten Van den Nest was born December 10th, 1978 in Aalst, Belgium. He studied Physics at the Katholieke Universiteit Leuven, Belgium, and received his Master degree (Licentiaat) in June 2001. His Master's thesis is entitled *The non-abelian Born-Infeld action for D-branes: study of odd terms* and was obtained at the Institute for Theoretical Physics at the Katholieke Universiteit Leuven under the supervision of Prof. Dr. Walter Troost.

In September 2001 he started working as a PhD student on the subject of quantum information theory in the lab *Signals, Identification, System theory and Automation* (SCD-SISTA) in the department of Electrical Engineering ESAT of the Katholieke Universiteit Leuven. His supervisors were Prof. dr. ir. Bart De Moor and Prof. dr. Mark Fannes.

References

[1] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inf. Theory*, IT-44(5):2010–2017, 1998.

[2] A. Bouchet. An efficient algorithm to recognize locally equivalent graphs. *Combinatorica*, 11(4):315 –329, 1991.

[3] A. Bouchet. Recognizing locally equivalent graphs. *Discrete Math.*, 114(1-3):75–86, 1993.

[4] S. Bravyi and A. Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. quant-ph/0403025, 2004.

[5] R. K. Brylinski and G. Chen, editors. *Mathematics of Quantum Computation.* Computational mathematics series. Chapman and Hall/CRC, 2002.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, 1997.

[7] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over gf(4). *IEEE trans. Inform. Theory*, 44(4):1369–1387, 1998. quant-ph/9608006.

[8] I. Chuang and M. Nielsen. *Quantum computation and quantum information.* Cambridge University press, Cambridge, 2000.

[9] S. R. Clark, C. M. Alves, and D. Jaksch. Efficient generation of graph states for quantum computation. quant-ph/0406150, 2004.

[10] J. Dehaene and B. De Moor. The clifford group, stabilizer states, and linear and quadratic operations over gf(2). *Phys. Rev. A*, 68:042318, 2003. quant-ph/0304125.

[11] J. Dehaene, M. Van den Nest, and B. De Moor. Local permutations of products of bell states and entanglement distillation. *Phys. Rev. A*, 67:022310, 2003. quant-ph/0207154.

[12] R Diestel. *Graph theory.* Springer, Heidelberg, 2000.

[13] W. Dür, H. Aschauer, and H.J. Briegel. Multiparticle entanglement purification for graph states. *Phys. Rev. Lett.*, 91:107903, 2003. quant-ph/0303087.

[14] W. Dür and H.J. Briegel. Stability of macroscopic entanglement under decoherence. *Phys. Rev. Lett.*, 92(18):180403, 2004.

[15] W. Dür, J. Casamiglia, and H.J. Briegel. Blind purification of multipartite entangled states. quant-ph/0411209, 2004.

[16] A.M. Gleason. Weight polynomials of self-dual codes and the macwilliams identities. In *Actes, congres international de Mathematiques*, volume 3, pages 211–215, Paris, 1970. Gautier-Villars.

[17] D. Glynn. On self-dual quantum codes and graphs. http://homepage.mac.com/dglynn/.cv/dglynn/Public/SD-G3.pdf-link.pdf, 2002.

[18] C. Godsil and G. Royle. *Algebraic graph theory.* Springer-Verlag, New York, 2001.

[19] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, Caltech, 1997. quant-ph/9705052.

[20] D. Gottesman. The heisenberg representation of quantum computers. quant-ph/9807006, 1998.

[21] M. Grassl, A. Klappenecker, and M. Roetteler. Graphs, quadratic forms and quantum codes. In *Proc. of the IEEE international symposium on information theory*, Lausanne, 2001.

[22] M. Grassl, M. Rötteler, and T. Beth. Computing local invariants of quantum-bit systems. *Phys.Rev. A*, 58(3):1833–1839, 1998. quant-ph/9712040.

[23] O. Guehne, G. Toth, P. Hyllus, and H.J. Briegel. Bell inequalities for graph states. quant-ph/0410059, 2004.

[24] M. Hein, W. Dür, and H.J. Briegel. Entanglement properties of multipartite entangled states under the influence of decoherence. quant-ph/0408165.

[25] M. Hein, J. Eisert, and H.J. Briegel. Multi-party entanglement in graph states. *Phys. Rev. A*, 69:062311, 2004. quant-ph/0307130.

[26] G. Hoehn. Self-dual codes over the kleinian four group. *Mathematische Annalen*, 327(2):227–255, 2003.

[27] E.. Hostens, J. Dehaene, and B. De Moor. Stabilizer states and clifford operations for systems of arbitrary dimensions, and modular arithmetic. quant-ph/0408190.

[28] A. Kay, J. K. Pachos, and C. S. Adams. Graph state preparation and cluster computation with global addressing of optical lattices. quant-ph/0501166, 2005.

[29] M. Mhalla and S. Perdrix. Complexity of graph state preparation. quant-ph/0412071, 2004.

[30] G. Nebe, E. Rains, and N.J.A. Sloane. The invariants of the clifford groups. *Designs, Codes and Cryptography*, 24(1):99–122, 2001. math.CO/0001038.

[31] G. Nebe, E. Rains, and N.J.A. Sloane. Codes and invariant theory. math.NT/0311046, 2003.

[32] A.L. Onishchik and E.B. Vinberg. *Lie groups and algebraic groups*. springer, Berlin, 1990.

[33] J. Preskill. Lecture notes on quantum computation. http://www.theory.caltech.edu/people/preskill/ph219/.

[34] E. Rains. Quantum codes of minimum distance two. *IEEE Trans. Inform. Theory*, 45(1):266–271, 1999. quant-ph/9704043.

[35] E. Rains and N.J.A. Sloane. Self-dual codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 177–294. 1998. math.CO/0208001.

[36] E.M. Rains. Quantum weight enumerators. *IEEE Trans. Inform. Theory*, 44(4):1388–1394, 1998. quant-ph/9612015.

[37] E.M. Rains. Polynomial invariants of quantum codes. *IEEE Trans. Inform. Theory*, 46(1), 2000. quant-ph/9704042.

[38] R. Raussendorf, D.E. Browne, and H.J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A*, 68:022312, 2003. quant-ph/0301052.

[39] B Runge. Codes and siegel modular forms. *Discrete Math.*, 148(1-3):175–204, 1996.

[40] D. Schlingemann. Stabilizer codes can be realized as graph codes. *Quant. Inf. Comp.*, 2(4), 2002. quant-ph/0111080.

[41] D. Schlingemann. Cluster states, algorithms and graphs. quant-ph/0305170, 2003.

[42] P. Shor and R. Laflamme. Quantum analog of the macwilliams identities for classical coding theory. *Phys. Rev. Lett.*, 78(8):1600–1602, 1997. quant-ph/9610040.

[43] T.A. Springer. *Invariant theory*, volume 585 of *Lecture notes in mathematics.* Springer, Berlin, 1977.

[44] M. S. Tame, M. Paternostro, M. S. Kim, and V. Vedral. Towards a more economical cluster state quantum computation. quant-ph/0412156, 2004.

[45] M. Van den Nest, J. Dehaene, and B. De Moor. Efficient algorithm to recognize local clifford equivalence of graph states. *Phys. Rev. A*, 70:034302, 2004. quant-ph/0405023.

[46] M. Van den Nest, J. Dehaene, and B. De Moor. Finite set of invariants to characterize local clifford equivalence of stabilizer states. quant-ph/0410165, submitted to Phys. Rev. A, 2004.

[47] M. Van den Nest, J. Dehaene, and B. De moor. Graphical description of the action of local clifford transformations on graph states. *Phys. Rev. A*, 69:022316, 2004. quant-ph/0308151.

[48] M. Van den Nest, J. Dehaene, and B. De Moor. Local equivalence of stabilizer states. In *Proceedings of the 16th international symposium on mathematical theory of networks and systems (MTNS).* K.U. Leuven, Belgium, 2004.

[49] M. Van den Nest, J. Dehaene, and B. De Moor. Local invariants of stabilizer codes. *Phys. Rev. A*, 70:032323, 2004. quant-ph/0404106.

[50] M. Van den Nest, J. Dehaene, and B. De moor. Local unitary versus local clifford equivalence of stabilizer states. quant-ph/0411115, submitted to Phys. Rev. A, 2004.

[51] M. Van den Nest, J. Dehaene, and B. De Moor. Invariants of the local clifford group. *Phys. Rev. A*, 71:022310, 2005. quant-ph/0410035.

[52] F. Verstraete and J.I. Cirac. Valence bond solids for quantum computation. *Phys. Rev. A*, 70:060302, 2004. quant-ph/0311130.

[53] F. Verstraete, J. Dehaene, and B. De Moor. Normal forms and entanglement measures for multipartite quantum states. *Phys. Rev. A*, 68:012103, 2003.

[54] A.-N. Zhang, C.-Y. Lu, X.-Q. Zhou, Y.-A. Chen, Z. Zhao, T. Yang, and J.-W. Pan. Experimental construction of optical multi-qubit cluster states from bell states. quant-ph/0501036, 2005.