

Quantum Computing from Graphs

by

Andrey Boris Khesin

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN MATHEMATICS

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2025

© 2025 Andrey Boris Khesin. This work is licensed under a [CC BY-NC-ND 4.0](#) license.

The author hereby grants to MIT a nonexclusive, worldwide, irrevocable, royalty-free license to exercise any and all rights under copyright, including to reproduce, preserve, distribute and publicly display copies of the thesis, or release the thesis under an open-access license.

Authored by: Andrey Boris Khesin
 Department of Mathematics
 November 21, 2024

Certified by: Peter Shor
 Professor of Mathematics, Thesis Supervisor

Accepted by: Jonathan Kelner
 Professor of Mathematics
 Graduate Co-Chair, Department of Mathematics

THESIS COMMITTEE

THESIS SUPERVISOR

Peter Shor

*Morss Professor of Applied Mathematics
Department of Mathematics*

THESIS READERS

Isaac Chuang

*Professor of Physics and EECS
Departments of Physics and EECS*

Aram Harrow

*Professor of Physics
Department of Physics*

Jonathan Kelner

*Professor of Applied Mathematics
Department of Mathematics*

Quantum Computing from Graphs

by

Andrey Boris Khesin

Submitted to the Department of Mathematics
on November 21, 2024 in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN MATHEMATICS

ABSTRACT

While stabilizer tableaus have proven exceptionally useful as a descriptive tool for additive quantum codes, they otherwise offer little guidance for concrete constructions or coding algorithm analysis. We introduce a representation of stabilizer codes as graphs with certain structures. Specifically, the graphs take a semi-bipartite form wherein input nodes map to output nodes, such that output nodes may connect to each other but input nodes may not. Intuitively, the graph's input-output edges represent information propagation of the encoding circuit, while output-output edges represent the code's entanglement structure. We prove that this graph representation is in bijection with tableaus and give an efficient compilation algorithm that transforms tableaus into graphs. We then show that this map is efficiently invertible, which gives a new universal recipe for code construction by way of finding graphs with sufficiently nice properties.

The graph representation gives insight into both code construction and algorithms. To the former, we argue that graphs provide a flexible platform for building codes particularly at small non-asymptotic scales. We construct as examples several constant-size codes and several infinite families codes. We also leverage graphs in a probabilistic analysis to extend the quantum Gilbert-Varshamov bound into a three-way distance-rate-weight trade-off. To the latter, we show that key coding algorithms, distance approximation, weight reduction, and decoding, are unified as instances of a single optimization game on a graph. Moreover, key code properties such as distance, weight, and encoding circuit depth, are all controlled by the graph degree. We give efficient algorithms for producing simple encoding circuits whose depths scale as twice the degree and for implementing logical diagonal and certain Clifford gates with non-constant but reduced depth. Finally, we construct a simple efficient decoding algorithm and prove a performance guarantee for a certain classes of graphs. These results give evidence that graphs are generically useful for the study of quantum computing and its practical implementations.

Thesis supervisor: Peter Shor

Title: Professor of Mathematics

Acknowledgements

My first and foremost thanks go out to my advisor, Peter Shor. Your unwavering support of my interests and ideas helped shape not only this thesis but the researcher I am today. Your knowledge and your kindness will always be an inspiration. Thank you for your willingness to explore with me, both inside and outside of the department. My journey into quantum computing would not have been possible without you, in more ways than one.

Thank you to Isaac Chuang for teaching me my first quantum computing class. You immediately caused me to become infatuated with the subject, despite the fact that I was lacking a key prerequisite! Your suggestion of a research problem as a final project led directly to the results in this very thesis.

Thank you to my thesis committee, which also includes Aram Harrow, and Jonathan Kelner. I am very grateful for your support and encouragement in the home stretch of my time at MIT, your comments, and your feedback.

Thank you to the MIT Math Department: to Pavel Etingof, John Urschel, Tanya Khovanova, Michel Goemans, Slava Gerovitch, André Lee Dixon, Michele Gallarelli, Charlotte Rubel, Theresa Cummings, Rosalee Zammuto, Sandi Miller, and all of the other staff, faculty, and students. Your help, friendships, advice, and support have been out of this world. You are all truly the reason why MIT has the best Math Department in the world.

Thank you to Jonathan, my main coauthor and office-mate. Your excitement has always been infectious and I am eternally grateful that your vision helped our work grow into what it is today. It's been a privilege working with you.

Thank you to my friends at ET, SigmaCamp, Tech Squares, $\sqrt{\text{mathroots}}$, TOPS, as well as my other coauthors and office-mates, Sunny, Norah, Kevin, Alex, Alex, Daniil, and Vasily. You made it all so much better. You listened to my riddles and helped me up when I was down. You filled my days with fun and helped me procrastinate. You are all awesome.

Thank you to my family: to Mom, Dad, and Nikita; you are my rock. Though I would get advice from many sources, I would always take end up taking your suggestions over others'. No amount of thanks can express my gratitude for your love and support.

Finally, thank you to my wife, Polina. You are my everything. Nothing I can write here will properly express how I grateful am I that you are in my life. Thank you for the world.

This material is based upon work supported by the Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator, under Grant number DOE DE-SC0012704, as well as NSF grants CCF-1452616 and CCF-1729369.

Contents

<i>List of Figures</i>	13
<i>List of Tables</i>	15
1 Introduction	17
2 Non-Clifford Computation from Graphs	19
2.1 Introduction	19
2.2 The Clifford hierarchy	20
2.3 Stabilizer rank	22
2.4 Graph states	23
2.5 Graph merging	24
2.6 Examples	26
2.6.1 Applying two controlled-S gates	26
2.6.2 Magic states	27
2.7 Proof of merging formula	27
2.8 Runtime	30
2.9 Conclusion	31
3 Quantum States from Graphs	33
3.1 Introduction	33
3.2 The stabilizer and graph formalisms	34
3.3 Canonical forms for stabilizer states	36
3.3.1 Canonical generator matrix	36
3.3.2 A unique canonical form	37
3.3.3 Simplifying extended graph states	41
3.4 Graph state stabilizer simulation	44
3.4.1 Algorithm	44
3.4.2 Discussion	44
3.5 Additive properties of stabilizer states	47
3.5.1 Graph merging	47
3.5.2 Linearly dependent triplets	50
3.5.3 Inner product algorithm	52
3.6 Conclusion	53

4	Quantum Codes from Graphs	55
4.1	Introduction	55
4.1.1	Contributions, scope, and conjectures	56
4.1.2	Related work	59
4.2	From tableaux to graphs	60
4.2.1	ZX canonical form construction	61
4.2.2	Tableau to encoder	63
4.2.3	Proof of canonicity	64
4.2.4	ZXCF to graph	65
4.3	Application to quantum codes	66
4.4	The inverse map: from graphs to stabilizer codes	68
4.4.1	Encoding circuit with degree-bounded depth	72
4.4.2	Logical non-Pauli gates on graph codes	74
4.4.3	Unification of stabilizer coding algorithms	76
4.5	Applications of the graph formalism	80
4.5.1	Flexible code design	80
4.5.2	The dodecahedral code	81
4.5.3	Covering spaces and the 5-covered icosahedral code	83
4.5.4	Planar and higher-dimensional lattice-type codes	84
4.5.5	Decoding algorithms and analysis	86
4.5.6	Random codes with reduced stabilizer weights	92
4.6	Conclusion and outlook	95
5	Equivalent Quantum Codes	97
5.1	Introduction	97
5.2	Background	99
5.3	Canonical form for CSS codes and states	103
5.4	Toric and surface codes	111
5.5	Prime codes	116
5.6	Another definition of equivalence	119
5.7	Tabulations from code	122
5.8	Equivalence classes with bipartite forms	125
5.9	Conclusion	129
6	Conclusion	131
A	Stabilizer rank of magic states	133
B	Proofs of transformation rules	135
C	Basics of the ZX-calculus	143
D	Tableau to graph proofs	147
E	Derivation of ZXCF counting recursion	151

F	Quantum Gilbert-Varshamov bound	153
G	Constructing the 3-by-3 toric code	155
H	Converting ZXCF's into quantum circuits	157
	<i>References</i>	161

List of Figures

3.1	A state in HK form	37
3.2	Orbits under local complementation	47
4.1	Examples of ZXCF rule violations	63
4.2	9-qubit code	67
4.3	7-qubit code	67
4.4	5-qubit code	68
4.5	Pivot assignment constraint example	69
4.6	Dodecahedral code	81
4.7	Encoder examples	82
4.8	Icosahedral graph	83
4.9	Toggling nodes in hypercube code	91
4.10	Family of random graphs	94
5.1	Works on graph representations under various equivalences	98
5.2	Encoder in the ZX-calculus	101
5.3	KL form code example	103
5.4	Toric code stabilizers	111
5.5	ZX diagram of 2×2 toric code	112
5.6	ZX diagram of 3×3 toric code	112
5.7	ZX normal form and diagram of 4×4 toric code	113
5.8	KL form of 4×4 toric code	114
5.9	KL form of 5×5 surface code	116
5.10	Graph code from adjacency matrix	120
5.11	$J_n, 1\mathbb{K}$ encoder graph equivalence classes	123
5.12	$J_n, 2\mathbb{K}$ encoder graph equivalence classes	124
5.13	$J_4, 2\mathbb{K}$ equivalence class example graphs	126
5.14	Non-bipartite $J_4, 2\mathbb{K}$ codes	127
5.15	Minimal diagram of $J_4, 2\mathbb{K}$ equivalence class	129
G.1	Nodes of 3×3 toric code	155
H.1	Conversion of graph code into quantum circuit	158

List of Tables

2.1	Decompositions of select non-Clifford gates	24
3.1	Formulas for Pauli projector operations	45

Chapter 1

Introduction

The work done in the past half century on quantum computing has brought large-scale quantum computers closer to reality. Today, quantum computers are just barely crawling out of their proverbial infancy but remain far removed from the public eye. Quantum computers differ from classical computers and classical supercomputers through the use of qubits rather than bits. The properties of quantum mechanics inherent in qubits, including superposition and entanglement, allow quantum computers to efficiently simulate quantum systems, making certain calculations much more efficient when done on quantum computers [1]. However, most quantum algorithms which are believed to provide significant speedups to certain computational problems require both many qubits and error correction to succeed in practice [1–8].

As with classical systems, quantum information processors face noise that disrupts information transmission between the sender and receiver. Due to the vulnerability of qubits to this noise, one of the principal challenges in quantum computing is to account for this noise [9]. To this end, quantum error-correcting codes are developed so that quantum information can be transmitted successfully in the presence of noise [1].

An important restriction on quantum error-correcting codes stems from the no-cloning theorem: while classical computers can copy bits, quantum mechanics does not allow for the cloning of unknown qubits, and the measurement of a qubit eliminates the information available in the qubit [1]. As such, constructing suitable quantum error-correcting codes presents new challenges compared to their classical counterparts.

As advancements in the experimental scaling of quantum computers have steadily marched forward, the problem of designing good quantum codes for the practical implementation of various quantum algorithm has in turn become of more pressing interest [10–14]. With a few exceptions, stabilizer codes have emerged as one of the most intensely studied families of codes due to their simple description [1, 15–20].

In this thesis, we explore ways of working with stabilizer codes, quantum states, and quantum circuits through the use of graphs. We present the graph formalism of quantum computing, a framework with all the necessary parts to discuss various aspects of quantum computation. We highlight ways to transform quantum states, circuits, and codes from one representation to another. Any representation of a quantum state or code in the stabilizer formalism will be part of a large class of equivalent presentations. We several examples of representations in the graph formalism which uniquely represent the most well-studied

families of quantum states and codes. We discuss avenues that the graph formalism can be used for universal quantum computation, fault tolerance, decoding, and code search.

Chapter 2 is based on work with Kevin Ren [21]. We present universal formulas for applying non-Clifford gates to graphs. Such gates are critical for universal quantum computation and fault tolerance [1, 22]. Applying these gates results in linear combinations of quantum states expressed as graphs. We provide formulas for merging such graphs together and discuss their use and runtime.

Chapter 3 is based on work with Alexander Hu [23]. We present a canonical form for expressing stabilizer states as graph states with local Clifford operations. We also showcase an algorithm for turning any stabilizer state expressed this way into its canonical form. Lastly, we expand on our work from Chapter 2 by proving exact conditions for the merging of a linear combination of two stabilizer states into one.

Chapter 4 is based on work with Jonathan Lu and Peter Shor [24, 25]. We extend our results from Chapter 3 and derive a canonical form for all stabilizer codes using graphs with input, pivot, and output vertices. These graphs allow for the efficient calculation of stabilizers and logical operators. Additionally, we show results on the quality of a randomly selected graph code from a given family. We give algorithms for converting between various representations of quantum codes as circuits, stabilizer tableaus, and graphs. Most importantly, we unify the algorithms of distance calculation, stabilizer weight reduction, and decoding in error-correction into a playing a single game on a graph, which we call Quantum Lights Out. We present results for sufficient conditions on when Quantum Lights Out can be played efficiently. From this, we prove that we can bound properties of codes by bounding properties of their corresponding graphs, highlighting a promising avenue for future graph search.

Chapter 5 is based on work with Alexander Li [26]. We specialize the canonical form for codes from Chapter 4 to CSS codes. We present results relating graph properties to whether those graphs correspond to CSS codes, as well as what properties the resulting CSS codes might have. We also analyze the classification of codes under a larger family of equivalence relations.

Appendix A contains a discussion on optimizing the stabilizer rank of magic states as well as a description of several decompositions using graphs. Appendix B contains a collection of proofs regarding the possible value of a term in the formula for merging two graphs. Appendix C contains an introduction to the ZX-calculus, a graphical language for representing and manipulating quantum systems which we use throughout this thesis. Appendix D contains an efficient algorithm for turning any Clifford encoder into a graph code in canonical form. Appendix E contains the derivation for a particular recursive formula, used to count the number of graphs in canonical form. Appendix F contains a proof of the Quantum Gilbert-Varshamov bound, which we include for completeness. Appendix G contains a discussion of how derive a graph representation of a small toric code. Appendix H contains an illustrated algorithm for how to convert a graph code into a quantum encoding circuit.

Chapter 2

Non-Clifford Computation from Graphs

2.1 Introduction

Quantum logic gates play a crucial role in quantum informatics. These gates allow us to perform the elementary steps of quantum computation and produce some desirable final state. While classical computations can all be carried out using a Turing machine, the physical reality of how classical circuits are implemented makes it useful to describe such circuits in terms of gates. Specifically, the NAND gate behaves similarly to a transistor and is therefore a good atom out of which to build other gates. The NAND gate is in fact universal, meaning all Boolean circuits can be constructed solely out of NAND gates.

It is harder to describe the concept of universality in the quantum case because quantum operations are continuous and not discrete. Notably, if we limit ourselves to using a finite number of universal quantum gates, we will never be able to describe all possible unitary operations that can be performed, as we could only ever construct a countable number of circuits. Universal quantum computation must be able to approximate unitary quantum operations with arbitrary precision.

As shown by Aharonov [22], a small set of gates, such as the Clifford and Toffoli gates, allow for universal quantum computation. It is thus desirable to not only be able to classically simulate how these gates act on quantum states, but also to do it quickly and in a small amount of space. Notably, it is worth asking how much time and space will this simulation take as a function of the number of qubits being simulated as well as of the number of operations performed.

There is a classification of certain operations on quantum states called the Clifford hierarchy. We denote the operations at the lower levels, Pauli gates and Clifford gates, \mathcal{C}_1 and \mathcal{C}_2 , respectively. The Toffoli gate is in a larger set of gates called \mathcal{C}_3 . We wish to be able to efficiently approximate universal circuits by simulating the action of \mathcal{C}_3 gates on quantum states. We can accomplish this by considering only a particular set of quantum states called stabilizer states, which can be represented efficiently. While Clifford gates take stabilizer states to stabilizer states, \mathcal{C}_3 gates take stabilizer states to linear combinations of two stabilizer states. Additionally, being able to implement \mathcal{C}_3 gates is of additional interest since they allow preparing quantum states known as magic states, which allow for the fault tolerant implementation of quantum circuits [27].

In this chapter, we show one way to simulate this action by using a representation of quantum states using graphs, as well as how to reduce the complexity of the representation combining some of the resulting terms. Informally, we give an explicit formula for expressing a set of \mathcal{C}_3 gates using linear combinations of Pauli and Clifford gates. By using a representation of stabilizer states with Clifford operations applied to graph states, we are able to apply the afore-mentioned formula for a \mathcal{C}_3 gate to a stabilizer state and express it as a linear combination of several such states. Next, we describe a procedure to merge these multiple states into just two stabilizer states using an explicit formula. Our algorithm runs in $O(nd)$ time where n is the number of qubits in the stabilizer state and d is the largest degree of a vertex in the graph used to express the state. This means that we can simulate the application of k \mathcal{C}_3 gates in time $O(2^k nd)$, where d is the largest degree of any graph encountered in the computation. We believe these results have applications in universal quantum computation and computation of stabilizer rank.

In Section 2.2, Section 2.3, and Section 2.4 we introduce definitions of the Clifford hierarchy, stabilizer rank, and graph states, respectively. In Section 2.5 we state our results and show examples of how to apply them in Section 2.6. The proof of the main result is shown in Section 2.7 and our graph merging algorithm's runtime is computed in Section 2.8.

2.2 The Clifford hierarchy

We begin by introducing a family of sets of quantum operations known as the *Clifford hierarchy*. These are key to the study of quantum circuits.

We begin by defining a fundamental set of operations, the Pauli group. Let n be the number of qubits we are simulating.

Definition 2.2.1. Let \mathcal{C}_1 , the *Pauli group*, be the group generated by matrix products and tensor products of the unitary matrices $\{X, Y, Z\}$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We also let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. \mathcal{C}_1 is the first level of the Clifford hierarchy. The Pauli group is also often denoted \mathcal{P} .

The matrices X , Y , and Z are called Pauli matrices, and have many nice properties.

Remark 2.2.2. The Pauli matrices obey $XY = iZ$, as well as similar expressions obtained by cyclically permuting X , Y , and Z . This means the Pauli group contains matrices which differ from X , Y , Z , and I by a phase, a scalar multiple by a complex unit, but since the quantum operations represented by those matrices ignore phase, we only need to consider the four matrices above. Additionally, the matrices X , Y , and Z are often denoted σ_x , σ_y , and σ_z or σ_1 , σ_2 , and σ_3 , respectively.

In general, if we wish to denote a gate U applied to a specific qubit a or pair of qubits a and b , we will write U_a or $U_{a,b}$, respectively. It is implied that the n -qubit operation is constructed by taking the tensor product of U on qubit a and identity matrices I applied to all other qubits. Furthermore, when writing tensor products of several matrices, we will usually omit the \otimes sign for brevity.

Since unitary matrices represent quantum gates, it is useful to examine the conjugation of one matrix by another. In other words, if a circuit contains the matrix A , we want to

know whether the matrix B commutes with it, and if it doesn't, what is the value of C in the expression $AB = CA$. Equivalently, we want to know what B turns into if we push operation A through B . We find that $C = ABA^{-1}$.

It is now natural to examine the normalizer of \mathcal{P} , the set of such matrices C through which we can pull a Pauli matrix and be sure to produce a Pauli matrix.

Definition 2.2.3. Let \mathcal{C}_2 , the Clifford group, be the normalizer of \mathcal{C}_1 , the set of operations U where for any Pauli matrix P , the matrix UPU^{-1} is Pauli. This condition is often written as $UPU^{-1} = \mathcal{P}$.

As Gottesman shows in [28], \mathcal{C}_2 is generated by the matrices H , S , and CX , which are Hadamard gate, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, the phase gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, and the controlled- X gate, $CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, respectively. The CX gate applies the X gate to the target qubit if the control qubit is in the $|1\rangle$ state, and any controlled-Pauli gate can be used as the third generator. When using subscripts to indicate the qubits to which the gate CX is applied, we write the control qubit first. The above matrix shows $CX_{1,2}$.

Example 2.2.4. The $SWAP$ gate is a \mathcal{C}_2 gate formed by $CX_{1,2} \cdot CX_{2,1} \cdot CX_{1,2}$, which swaps the values of qubits 1 and 2 and is written as $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Example 2.2.5. The CZ gate is a \mathcal{C}_2 gate written as $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$. Note that it is symmetric in terms of its control and target. Stated mathematically, $SWAP_{1,2} \cdot CZ_{1,2} \cdot SWAP_{1,2} = CZ_{1,2}$. This means that the diagonal CZ gate commutes with all other diagonal gates, and also that we do not need to specify which of the gate's two qubits is the control. Note that a controlled- U gate, CU , is written in general as $CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$.

Definition 2.2.6. We define a *local Clifford (LC) operation* as any of the matrices generated by H and S through matrix products and tensor products. The 24 matrices in the set $\langle H, S \rangle$, formed only by multiplying sequences of H and S matrices, form the set of single-qubit local Clifford operations.

We can further extend this idea and ask ourselves which operators map Pauli gates to the Clifford group under conjugation. This leads us to the following definition.

Definition 2.2.7. For $k \in \mathbb{N}$, let \mathcal{C}_k , the *operators on level k of the Clifford hierarchy*, be defined recursively as \mathcal{C}_k is the set of all unitary operations U where $UPU^{-1} = U\mathcal{P}U^\dagger \subseteq \mathcal{C}_{k-1}$, with the base case being $\mathcal{P} = \mathcal{C}_1$. Note that the Clifford group is indeed \mathcal{C}_2 under this definition. Furthermore, we note that for $k > 2$, these operators do not form a group.

As mentioned earlier, we can achieve universal quantum computation by just using Clifford gates and the Toffoli gate, which is in \mathcal{C}_3 [22].

The particular gates in \mathcal{C}_3 that we study are $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$, CH , CS , CCX , CCZ , $CSWAP$. These are the $\frac{\pi}{8}$ gate, the controlled- H gate, the controlled- S gate, the Toffoli or controlled-controlled- X gate, the controlled-controlled- Z gate, and the controlled- $SWAP$ gate, respectively. For ease of notation we denote the set of these six \mathcal{C}_3 operators as \mathcal{S} .

We note the following regarding controlled operations.

Remark 2.2.8. To apply a controlled operation U , the matrix used is $\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$. The operation U is controlled by qubit 1 and applied to the remaining qubits. This operation is denoted CU , which can be nested if U is already a controlled operation. Note that applying a control operation to a gate often raises its level in the Clifford hierarchy, although the exact conditions for when this is true are unclear. For certain special gates U , such as Z , S , and T , we use the convention that if the controlled operation $CU_{a,b}$ is applied to qubits a and b , then when $b = a$ this operation is equal to U_a . The gates Z , S , and T are special in this regard since they can be viewed as a controlled global phase.

2.3 Stabilizer rank

When doing quantum simulations, it is convenient to start the simulation with a particular state, such as $|0\rangle^{\otimes n}$, and then proceed from there. In fact there is a specific finite subset of all n -qubit states which is convenient to work with. For this we introduce the stabilizer formalism.

Definition 2.3.1. We say that a state $|\psi\rangle$ is a *stabilizer state* if there exists a set of n independent Pauli operators $U \in \mathcal{C}_1$ such that $U|\psi\rangle = |\psi\rangle$. We say that the operators U *stabilize* $|\psi\rangle$.

Remark 2.3.2. If $|\psi\rangle$ is a stabilizer state and $U \in \mathcal{C}_2$, then $U|\psi\rangle$ will also be a stabilizer state. Furthermore, any stabilizer state can be expressed as $U|0\rangle^{\otimes n}$ for some $U \in \mathcal{C}_2$.

One of the things that make stabilizer states useful is that they can be represented efficiently. An n -qubit state requires 2^n components to represent as a state vector, but an $n \times n$ *stabilizer tableau* of Pauli matrices that identify the stabilizer state only requires $O(n^2)$ space.

If we wish to perform universal quantum computation, the natural step after defining stabilizer states is trying to describe the action of \mathcal{C}_3 gates on these states. Immediately, we see that if $|\psi\rangle$ is a stabilizer state and $U \in \mathcal{C}_3$, then $U|\psi\rangle$ will not always be a stabilizer state, as that is only true for gates in \mathcal{C}_2 . In fact, representing the action of several \mathcal{C}_3 gates on $|\psi\rangle$ is of great interest as this lets us perform universal quantum computation, magic state distillation, and fault tolerant quantum computation [22, 27]. For now, we need to introduce new terminology to talk about the resulting states after applying \mathcal{C}_3 gates on stabilizer states.

Definition 2.3.3. As defined by [29], let the *stabilizer rank* $\chi(|\psi\rangle)$ of an n -qubit state $|\psi\rangle$ be the smallest number k of stabilizer states $|\phi_i\rangle$ needed to write $|\psi\rangle = \sum_{i=1}^k c_i |\phi_i\rangle$. Note that $\chi(|\psi\rangle) \geq 1$ with equality iff $|\psi\rangle$ is a stabilizer state. Also we observe that $\chi(|\psi\rangle) \leq 2^n$, since the standard basis vectors are all stabilizer states.

We will later show that if $|\psi\rangle$ is a stabilizer state and $U \in \mathcal{S}$ is one of the \mathcal{C}_3 gates, then we can always write $U|\psi\rangle$ as a linear combination of no more than 2 stabilizer states. In other words, $\chi(U|\psi\rangle) \leq 2$.

This is a very important point, as this means that we can represent the action of a \mathcal{C}_3 gate in a circuit as a linear combination of two stabilizer states. Since matrix multiplication

is additive, a second \mathcal{C}_3 gate would act on both parts independently. This means that we have reduced the problem of finding out how a series of \mathcal{C}_3 gates acts on a stabilizer state, to learning the behaviour of just one. The cost we pay for this is that our memory system must be able to store a linear combination of stabilizer states.

Presently, this means that applying m \mathcal{C}_3 gates will result in a linear combination of 2^m stabilizer states, which we would like to avoid. What we focus on is detecting when a linear combination of two stabilizer states can be merged into one. By applying such a merging operation after every application of a \mathcal{C}_3 gate, we can massively reduce the exponential growth in the space required to represent our state. However, with our current representation of stabilizer states, this merging operation would require us to identify when a linear combination of two stabilizer matrices can be merged and produce a stabilizer matrix of the sum. We are not currently aware of a method that would allow us to do this, which is why we have to turn to a different representation of stabilizer states.

2.4 Graph states

A lot of work in quantum cryptography has been done using codes based on graphs. Similar techniques allow us to adapt graphs for our purposes.

Definition 2.4.1. A *graph* $G = (V, E)$ consists of a set of vertices V and a set of edges $E \subseteq V \times V$ connecting those vertices. For now, we will always take V to be the set of n qubits numbered from 1 to n . By $N(a)$ we denote the neighbourhood of a , the set of all vertices b such that $(a, b) \in E$. We do not allow edges from a vertex to itself, so $a \notin N(a)$.

A useful set of stabilizer states that can be described by a graph is the set of graph states.

Definition 2.4.2. Let the *graph state* $|G\rangle$ of an n -vertex graph G be the state stabilized by the operators $g_v = X_v \prod_{u \in N(v)} Z_u$, for all vertices v . Note that $|G\rangle$ is a stabilizer state.

Additionally,

$$|G\rangle = \prod_{(u,v) \in E} CZ_{u,v} |+\rangle^{\otimes n} \quad \text{where } |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \quad (2.1)$$

However, not all stabilizer states can be expressed as graph states, which means we need to supplement our graphs with additional information. As shown by Van den Nest, Dehaene, and De Moor [30], any stabilizer state can be expressed as a graph state with local Clifford operations performed on the vertices. This fact will be key to our use of graphs. Now, any stabilizer state can be denoted by $U|G\rangle$ where U is a local Clifford operation and G is a graph. Storing such a graph takes $O(1)$ additional space per qubit, as the number of local Clifford operations is fixed. Storing the entire graph as an adjacency list takes $O(nd)$ space where d is the average degree of the graph.

Now we examine when and how we can merge a linear combination of two graphs into one.

2.5 Graph merging

We begin with the statement of our main results and will then build up to its proof. Let \mathcal{S} be $\{T, CS, CH, CCZ, CCX, CSWAP\}$, a collection of \mathcal{C}_3 gates.

Theorem 2.5.1. *Let $C \in \mathcal{S}$ be a \mathcal{C}_3 operator and let state $|\psi\rangle$ be $U|G\rangle$ where U is local Clifford and G is an n -vertex graph with largest degree d . Then we can find two states $U_1|G_1\rangle$ and $U_2|G_2\rangle$ such that $C|\psi\rangle = U_1|G_1\rangle + U_2|G_2\rangle$ in runtime $O(nd)$.*

\mathcal{C}_3 Gate	Decomposition
T	$\frac{1}{2}(I + Z) + \frac{1}{2}e^{\frac{i\pi}{4}}(I - Z)$
CS	$\frac{1}{2}(I + Z)I + \frac{1}{2}(I - Z)S$
CH	$\frac{1}{2}(I + Z)I + \frac{1}{2}(I - Z)H$
CCZ	$III - \frac{1}{4}(I - Z)(I - Z)(I - Z)$
CCX	$III - \frac{1}{4}(I - Z)(I - Z)(I - X)$
CSWAP	$III - \frac{1}{4}(I - Z) \otimes (II - ZZ) \cdot (II - XX)$

Table 2.1: A decomposition of the \mathcal{C}_3 gates we examined into a sum of two products of projectors and \mathcal{C}_2 gates. Note that all tensor products have been removed for brevity except for that in the final entry, to highlight the distinction between matrix product and tensor product.

Let us first attempt to apply the gates in \mathcal{S} as directly as we can. Table 2.1 allows us to decompose gates in \mathcal{S} into the sum of two terms, each consisting of the products of Pauli projectors and \mathcal{C}_2 gates. This highlights the following key fact: if we can describe the action of a Pauli projector on a stabilizer state in terms of graph, we will be able to express a stabilizer decomposition of any gate in \mathcal{S} . This is nothing more than the outcome of a post-selected measurement, which can easily be described in terms of stabilizer generators. In the stabilizer formalism, this is done by adding the measurement projector to a set of $n - 1$ stabilizer generators that all commute with the measurement.

The goal of constructing the action of a Pauli projection on graphs is the first step in generalizing a graph merging operation, whereby certain linear combinations of two stabilizer states turn into one state. In a later chapter, we will describe more precisely when two graphs can be merged this way. With further study, it may be possible to describe conditions for merging and simplifying more complicated linear combinations, such as those of three or more states into fewer.

We will prove Theorem 2.5.1 by means of the following result, generalizing Proposition 1 of [31].

Theorem 2.5.2. *Let v be a vertex, let A be the set $N(v) \cup \{v\}$, and let B be any set containing v . Then, for any integer k ,*

$$\frac{1}{\sqrt{2}} \left(I + i^k \prod_{u \in B} Z_u \right) |G\rangle = H_v Z_v \left(\prod_{u,w \in A} CS_{u,w}^k \right) \left(\prod_{u \in A, w \in B} CZ_{u,w} \right) |G\rangle. \quad (2.2)$$

(Note the convention from Remark 2.2.8.)

Note that the expression in Theorem 2.5.2 may contain a CS operation, which is a \mathcal{C}_3 gate that we are not allowed to apply to a graph. In the expression, the product of such terms iterates over $u \in A$ and $w \in A$. Thus, for every pair $u \neq w$, we will apply both $CS_{u,w}$ and $CS_{w,u}$ which together produce $CZ_{u,w}$, the toggling of an edge. Meanwhile, if $u = w$, then by the convention from Remark 2.2.8, $CS_{u,w} = CS_{u,u} = S_u$, which we are allowed to apply.

The proof of Theorem 2.5.2 is technical and will be given in a later section.

Theorem 2.5.2 shows us how to apply certain Pauli projectors and operations to graph states. A general Pauli projector is a term proportional to $I + P$, where P is a Pauli matrix. Specifically, we need P to be a matrix whose eigenvalues are ± 1 . In Equation (2.2), we find that the operation on the left side will not be a projector if k is odd. However, we will find that our formula works in the case of odd k as well. If one is strictly interested in the case when the operation is a projector, the i^k should be replaced with $(-1)^k$ and the CS product should be replaced by the same product with CZ , which is equivalent to $\prod_{u \in A} Z_u$.

The projectors have the nice property that conjugation by a local Clifford operation gives another projector. For example,

$$H \cdot \frac{(I + Z)}{2} \cdot H = \frac{I + X}{2}. \quad (2.3)$$

Thus, for any local Clifford gate U and projector R , we have

$$RU |\psi\rangle = UR' |\psi\rangle, \quad (2.4)$$

where R' is another projector. This means that if we ever find ourselves applying a projector to a state with local Clifford operations, we can commute the projector through those operations and applied the modified projector to a graph state directly.

With the local Clifford operations out of the way, we merely need to compute the state $P' |\psi\rangle$. Splitting $P' = P_1 P_2 \dots P_k$ into a product of projectors, we will apply P_k, P_{k-1}, \dots, P_1 in order to $|\psi\rangle$. Now we need to outline how to apply a single projector P to $|\psi\rangle$.

If P is a product of Z gates, then we can directly apply the merge described in Theorem 2.5.2. Otherwise, we convert $Y = iXZ$ to replace all Y 's, and we can use the identity

$$X_v |G\rangle = \left(\prod_{u \in N(v)} Z_u \right) |G\rangle \quad (2.5)$$

to convert all X gates to Z gates on other qubits. This identity is valid because $X_v \prod_{u \in N(v)} Z_u$ is a stabilizer for the graph state $|G\rangle$. This operation might cause Z gates to appear on other

qubits that still had X gates that needed to be applied to the graph. In this case, we use the anti-commutativity of the Pauli matrices to fix their order, commuting the Z through the X and applying an overall phase of -1 . While global phases are usually ignored, they are important when working with linear combinations of stabilizer states when expressed as state vectors or any other representation which is sensitive to phases.

Repeating the above allows us to make sure there are only Z gates left, and we can apply the merging algorithm of Theorem 2.5.2 to the graph under the resulting projector. The application of P_k is thus another stabilizer state, and then we can apply P_{k-1} , P_1 , and so on. This proves most of the statement of Theorem 2.5.1. The runtime will be analyzed in a later section.

2.6 Examples

One important concern is that our algorithm behaves well with circuit identities. For example, applying two CCX gates gives the identity, but since each CCX would turn one stabilizer state into two, two CCX gates should initially leave us with four stabilizer states. A robust algorithm would find a way to merge or otherwise annihilate these four stabilizer states such that only one remains. In the following example, we use the identity $CS \cdot CS = CZ$. Since CZ is a Clifford operation, we should expect the output of the application of two CS gates to be a single stabilizer state. In the second example, we show that the stabilizer rank of the 2-qubit magic state $TT|++\rangle$ is 2 and not 4.

2.6.1 Applying two controlled-S gates

We showcase the example of applying two CS to a stabilizer state. We begin with a stabilizer state $|\psi\rangle = U|G\rangle$. Then

$$CS|\psi\rangle = \frac{1}{2}((I+Z)I + (I-Z)S)U|G\rangle. \quad (2.6)$$

If we apply CS again then we get

$$CZ|\psi\rangle = \left(\frac{1}{2}((I+Z)I + (I-Z)S)\right)^2 U|G\rangle. \quad (2.7)$$

Now, we use the identity $(I+Z)(I-Z) = 0$ and $(I \pm Z)^2 = 2(I \pm Z)$ to simplify this to

$$CZ|\psi\rangle = \frac{1}{2}((I+Z)I + (I-Z)Z)U|G\rangle \quad (2.8)$$

We should have four stabilizer states, but two of them (corresponding to the cross terms) collapsed to zero. We can now perform merges on $(I+Z)U|G\rangle$ and $(I-Z)U|G\rangle$. Note that in Theorem 2.5.2, the two projectors are identical with the sole exception being the value of k differing by 2. The resulting graphs will thus be identical, since the right-hand sides of Equation (2.2) will differ only by a factor of $\prod_{u,w \in A} CS_{u,w}^2 = \prod_{u,w \in A} CZ_{u,w} = \prod_{u \in A} Z_u$.

Thus, the output of the algorithm will be two stabilizer states $U_1 |G'\rangle$ and $U_2 |G'\rangle$, where $U_1 = U_2 \prod_{u \in A} Z_u$.

Thus, the operators differ by a Pauli, so they form a projector and we can merge $U_1 |G'\rangle$ and $U_2 |G'\rangle$ into a single final state. As expected, two CS gates produce a single stabilizer state.

2.6.2 Magic states

We now show the application of two T gates. Consider $T_1 T_2 |++\rangle$, where $|++\rangle$ is the graph state of the empty graph on 2 vertices. As expected, one application of the merging algorithm leads to two stabilizer states:

$$T_1 |++\rangle = \frac{1}{\sqrt{2}} H_1 |++\rangle + \frac{1}{\sqrt{2}} e^{\frac{i\pi}{4}} H_1 Z_1 |++\rangle. \quad (2.9)$$

Applying the algorithm again for the second T gate, we get four stabilizer states:

$$T_2 T_1 |++\rangle = \left(\frac{1}{2} H_1 H_2 + \frac{1}{2} e^{\frac{i\pi}{4}} H_1 H_2 Z_2 + \frac{1}{2} e^{\frac{i\pi}{4}} H_1 H_2 Z_1 + \frac{i}{2} H_1 H_2 Z_1 Z_2 \right) |++\rangle. \quad (2.10)$$

We now apply our merge on the first and fourth states, and the second and third states, to get

$$T_2 T_1 |++\rangle = \frac{1}{\sqrt{2}} S_1 H_2 |G\rangle + \frac{1}{\sqrt{2}} e^{\frac{\pi i}{4}} H_1 Z_1 |G\rangle, \quad (2.11)$$

where G is the complete graph on two vertices, so $|G\rangle$ is $CZ |++\rangle$. We obtain a decomposition into 2 stabilizer states, which is optimal since $T_1 T_2 |++\rangle$ is not a stabilizer state.

We return to the discussion of magic states in Appendix A, which is connected to results introduced in the next chapter.

2.7 Proof of merging formula

In this section, we give a proof of Equation (2.2) from Theorem 2.5.2. The outline for the proof structure is to show that the two states on either side of Equation (2.2) have the same set of stabilizers and the same global phase. The proof itself is quite technical.

Let g_u be the canonical stabilizer generator of graph G associated with vertex u as given in Definition 2.4.2. We have that $g_u = X_u \prod_{w \in N(u)} Z_w$. Let σ and ζ be shorthand for the CS and CZ products in Equation (2.2). We have that $\sigma = \prod_{u, w \in A} CS_{u, w}^k$ and $\zeta = \prod_{u \in A, w \in B} CZ_{u, w}$.

Let the unitary U be the operation $U = H_v Z_v \sigma \zeta$. We wish to show that

$$\frac{1}{\sqrt{2}} \left(I + i^k \prod_{u \in B} Z_u \right) |G\rangle = U |G\rangle. \quad (2.12)$$

Since any g_u stabilizes $|G\rangle$, we have that $U g_u U^\dagger$ stabilizes $U |G\rangle$. It thus remains to show that this new stabilizer $g'_u = U g_u U^\dagger$ stabilizes the left-hand side of Equation (2.2).

We first consider the case for g'_v . For simplicity, we will denote an expression of the form $\prod_{w \in S} Z_w$ as Z_S . We have the following derivation. Here, we use the commutation rules that $CZ_{u,w}X_u = X_uZ_wCZ_{u,w}$ as well as that $S^kX = X(iZ)^k$. We also recall that $A = N(v) \cup \{v\}$.

$$g'_v = Ug_vU^\dagger \quad (2.13)$$

$$= H_vZ_v\sigma\zeta X_vZ_{N(v)}\zeta\sigma^\dagger Z_vH_v \quad (2.14)$$

$$= H_vZ_v\sigma Z_vX_vZ_AZ_BZ_{N(v)}Z_v\sigma^\dagger Z_vH_v \quad (2.15)$$

$$= H_vS_v^k X_vZ_{N(v)}^k Z_vZ_B S_v^{-k} H_v \quad (2.16)$$

$$= H_vX_v(iZ_v)^k Z_{N(v)}^k Z_vZ_B H_v \quad (2.17)$$

$$= Z_v(iX_v)^k Z_{N(v)}^k Z_{B \setminus \{v\}} \quad (2.18)$$

$$= Z_{N(v)}^k Z_B(iX_v)^k \quad (2.19)$$

Now, we need to check that g_v stabilizes the state on other side of our equation, which we denote as the state $|\psi\rangle = \frac{1}{\sqrt{2}}(I + i^k Z_B)|G\rangle$. We have the following.

$$g'_v|\psi\rangle = \frac{1}{\sqrt{2}}Z_{N(v)}^k Z_B(iX_v)^k (I + i^k Z_B)|G\rangle \quad (2.20)$$

$$= \frac{1}{\sqrt{2}}Z_{N(v)}^k (Z_B + (-1)^k i^k I)(iX_v)^k |G\rangle \quad (2.21)$$

$$= \frac{1}{\sqrt{2}}Z_{N(v)}^k (i^k Z_B + I) Z_{N(v)}^k |G\rangle \quad (2.22)$$

$$= \frac{1}{\sqrt{2}}(I + i^k Z_B)|G\rangle = |\psi\rangle \quad (2.23)$$

We now need to show the same is true for an arbitrary vertex $u \neq v$. We introduce two indicator functions $\mathbb{1}_A$ and $\mathbb{1}_B$ which are equal to 1 if $u \in A$ or $u \in B$, respectively, and are 0 otherwise. We then have the following.

$$g'_u = Ug_uU^\dagger \quad (2.24)$$

$$= H_vZ_v\sigma\zeta X_uZ_{N(u)}\zeta\sigma^\dagger Z_vH_v \quad (2.25)$$

$$= H_v\sigma X_u(-1)^{\mathbb{1}_A\mathbb{1}_B} Z_A^{\mathbb{1}_B} Z_B^{\mathbb{1}_A} Z_{N(u)}\sigma^\dagger H_v \quad (2.26)$$

$$= (-1)^{\mathbb{1}_A\mathbb{1}_B} H_v(S_u)^{\mathbb{1}_A k} X_u Z_{A \setminus \{v\}}^{\mathbb{1}_A k} Z_A^{\mathbb{1}_B} Z_B^{\mathbb{1}_A} Z_{N(u)}(S_u)^{-\mathbb{1}_A k} H_v \quad (2.27)$$

$$= (-1)^{\mathbb{1}_A\mathbb{1}_B} H_v X_u(iZ_u)^{\mathbb{1}_A k} Z_{A \setminus \{v\}}^{\mathbb{1}_A k} Z_B^{\mathbb{1}_A} Z_A^{\mathbb{1}_B} Z_{N(u)} H_v \quad (2.28)$$

$$= (-1)^{\mathbb{1}_A\mathbb{1}_B} i^{\mathbb{1}_A k} X_u(X_v Z_{A \setminus \{v\}})^{\mathbb{1}_A k} (X_v Z_{B \setminus \{v\}})^{\mathbb{1}_A} (X_v Z_{A \setminus \{v\}})^{\mathbb{1}_B} (X_v Z_v)^{\mathbb{1}_A} Z_{N(u)} \quad (2.29)$$

$$= i^{\mathbb{1}_A k} Z_B^{\mathbb{1}_A} (X_v Z_{N(v)})^{\mathbb{1}_A k + \mathbb{1}_B} X_u Z_{N(u)} \quad (2.30)$$

$$= (i^k Z_B)^{\mathbb{1}_A} g_v^{\mathbb{1}_A k + \mathbb{1}_B} g_u \quad (2.31)$$

All that remains for us to show is that $g'_u|\psi\rangle = |\psi\rangle$. We note that g_u and g_v are stabilizers of $|G\rangle$.

$$g'_u |\psi\rangle = \frac{1}{\sqrt{2}} (i^k Z_B)^{\mathbb{1}_A} g_v^{\mathbb{1}_A k + \mathbb{1}_B} g_u (I + i^k Z_B) |G\rangle \quad (2.32)$$

$$= \frac{1}{\sqrt{2}} (i^k Z_B)^{\mathbb{1}_A} g_v^{\mathbb{1}_A k + \mathbb{1}_B} (I + i^k (-1)^{\mathbb{1}_B} Z_B) g_u |G\rangle \quad (2.33)$$

$$= \frac{1}{\sqrt{2}} (i^k Z_B)^{\mathbb{1}_A} (I + i^k (-1)^{\mathbb{1}_A k} Z_B) g_v^{\mathbb{1}_A k + \mathbb{1}_B} |G\rangle \quad (2.34)$$

$$= \frac{1}{\sqrt{2}} \left((i^k Z_B)^{\mathbb{1}_A} + (i^k Z_B)^{1 - \mathbb{1}_A} \right) |G\rangle \quad (2.35)$$

$$= \frac{1}{\sqrt{2}} (I + i^k Z_B) |G\rangle = |\psi\rangle \quad (2.36)$$

This proves that both sides of Equation (2.2) have the same stabilizers. We now show that they have the same global phase.

Let $c = \frac{1}{\sqrt{2^n}}$. Let the co-vector $\langle \mathbf{0} |$ be defined as $\langle \mathbf{0} | = \langle 0 |^{\otimes n}$. We apply $\langle \mathbf{0} |$ to both sides of Equation (2.2). We also define $\langle \mathbf{1}_v | = \langle \mathbf{0} | X_v$. On the left-hand side of the equation, the product of Z terms acts on the $\langle \mathbf{0} |$ trivially, since $|0\rangle$ is a $+1$ eigenstate of Z_u for all u . Furthermore, since $|G\rangle = \prod_{(u,w) \in E} CZ_{u,w} |+\rangle^{\otimes n}$ where E is the edge set of G , and since $CZ_{u,w}$ stabilizes $\langle \mathbf{0} |$ and $\langle \mathbf{1}_v |$, we obtain the inner products below.

$$\langle \mathbf{0} | \prod_{(u,w) \in E} CZ_{u,w} |+\rangle^{\otimes n} = \langle \mathbf{0} | + \rangle^{\otimes n} = c \quad (2.37)$$

$$\langle \mathbf{1}_v | \prod_{(u,w) \in E} CZ_{u,w} |+\rangle = \langle \mathbf{1}_v | + \rangle^{\otimes n} = c \quad (2.38)$$

Thus, $\langle \mathbf{0} | G \rangle = \langle \mathbf{1}_v | G \rangle = c$. Since B contains v , we get the following.

$$\left\langle \mathbf{0} \left| \frac{1}{\sqrt{2}} \left(I + i^k \prod_{u \in B} Z_u \right) \right| G \right\rangle = \frac{1 + i^k}{\sqrt{2}} \cdot c \quad (2.39)$$

$$\left\langle \mathbf{1}_v \left| \frac{1}{\sqrt{2}} \left(I + i^k \prod_{u \in B} Z_u \right) \right| G \right\rangle = \frac{1 - i^k}{\sqrt{2}} \cdot c \quad (2.40)$$

For the right-hand side, we note that $|\mathbf{0}\rangle$ is a $+1$ eigenstate of Z , CZ , and CS . The inner products with the diagonal terms in our equation are given by the following.

$$\left\langle \mathbf{0} \left| Z_v \prod_{u,w \in A} CS_{u,w}^k \prod_{u \in A, w \in B} CZ_{u,w} \right| G \right\rangle = c \quad (2.41)$$

$$\left\langle \mathbf{1}_v \left| Z_v \prod_{u,w \in A} CS_{u,w}^k \prod_{u \in A, w \in B} CZ_{u,w} \right| G \right\rangle = i^k \cdot c \quad (2.42)$$

This is since $|\mathbf{1}_v\rangle$ is a -1 eigenstate of Z_v , a $+i$ eigenstate of S_v , and a $+1$ all the other operators in the expression. Note that there are two Z_v 's in the above product, of which one appears as $CZ_{v,v}$. Similarly, $CS_{v,v}$ is S_v . Thus we have the following.

$$\begin{aligned} & \left\langle \mathbf{0} \left| H_v Z_v \left(\prod_{u,w \in A} CS_{u,w}^k \right) \left(\prod_{u \in A, w \in B} CZ_{u,w} \right) \right| G \right\rangle \\ &= \frac{\langle \mathbf{0} | + \langle \mathbf{1}_v |}{\sqrt{2}} \left(Z_v \left(\prod_{u,w \in A} CS_{u,w}^k \right) \left(\prod_{u \in A, w \in B} CZ_{u,w} \right) \right) |G\rangle = \frac{1+i^k}{\sqrt{2}} \cdot c \end{aligned} \quad (2.43)$$

$$\begin{aligned} & \left\langle \mathbf{1} \left| H_v Z_v \left(\prod_{u,w \in A} CS_{u,w}^k \right) \left(\prod_{u \in A, w \in B} CZ_{u,w} \right) \right| G \right\rangle \\ &= \frac{\langle \mathbf{0} | - \langle \mathbf{1}_v |}{\sqrt{2}} \left(Z_v \left(\prod_{u,w \in A} CS_{u,w}^k \right) \left(\prod_{u \in A, w \in B} CZ_{u,w} \right) \right) |G\rangle = \frac{1-i^k}{\sqrt{2}} \cdot c. \end{aligned} \quad (2.44)$$

In summary, we proved that applying $\langle \mathbf{0} |$ or $\langle \mathbf{1}_v |$ to both sides gives the same result. If k is 0 or 2, one of these terms can equal 0, not allowing us to confirm that the phases are equal, but the expressions cannot be 0 simultaneously, which proves that the global phases are equal. This proves the correctness of our algorithm.

2.8 Runtime

Consider the action of a \mathcal{C}_3 gate $C \in \mathcal{S}$ on stabilizer state $|\psi\rangle = U|G\rangle$. The full steps of our algorithm are as follows.

- (1) Express C as $C = C_1 + C_2$, a sum of operations involving Pauli projectors and \mathcal{C}_2 gates, as shown in Table 2.1.
- (2) For each term of the form $I + P$ in C_1 that we wish to apply to $|\psi\rangle$, first compute $P' = U^\dagger P U$. Now, we seek to compute $U(I + P')|G\rangle$.
- (3) Convert all X 's and Y 's in P' to Z 's on neighbouring vertices in G through the graph stabilizers of $|G\rangle$.
- (4) Apply the merging algorithm given by Equation (2.2) to turn the expression $U(I + P')|G\rangle$ into a single graph state with local Cliffords.
- (5) Repeat steps (2)-(4) for each $I + P$ remaining in C_1 .
- (6) Repeat steps (2)-(5) for C_2 .

The main contributor to the runtime are steps (3) and (4). If n is the number of qubits and d is the average degree of $|G\rangle$, we claim that our average runtime is $O(nd)$. The only other step that takes non-constant time is step (2), which requires $O(n)$ time to compute P' . Converting an X or Y to Z 's might need to be done for each of n qubits, requiring d updates on per qubit. Hence step (3) has $O(nd)$ runtime. Lastly, applying the gates in the algorithm takes time $O(|A| \cdot |A| + |A| \cdot |B|)$. However, on average we have $|A| = d$ and $|B| = n$, so we get $O(d^2 + dn)$. Since $d < n$, we have proven our runtime $O(nd)$.

2.9 Conclusion

In this chapter, we showed how to simulate \mathcal{C}_3 circuits on stabilizer states. We use a decomposition of \mathcal{C}_3 operators into a sum of projectors and a merging algorithm that combines two states. We showed the robustness of our algorithm with circuit identities and we also derived a decomposition of the magic state $TT|++\rangle$ into two stabilizer states.

Future work can examine how our algorithm performs when computing higher-qubit magic states. We can also look to derive more cases where merging two states is possible besides the ones we found. Additionally, we can look at the implications of our \mathcal{C}_3 circuit simulation algorithm for universal quantum computation. Another future research direction is to examine the application of \mathcal{C}_3 gates to stabilizer codes in addition to their effect on stabilizer states. Lastly, we can consider ways to develop the graph formalism further and see what statements we can make about stabilizer states expressed as graphs with local Cliffords. We investigate this in the next chapter.

Chapter 3

Quantum States from Graphs

3.1 Introduction

As we saw in the previous chapter, the stabilizer formalism has important applications to quantum error correction and fault tolerant quantum computation [20, 28] and to the classical simulation of quantum circuits [29, 32–37].

The general classical simulation of quantum circuits to be exponentially slow, yet simulating stabilizer circuits can be done in polynomial time by the Gottesman-Knill Theorem [1]. As we discussed in the previous chapter, the addition of certain non-Clifford gates makes stabilizer circuits universal, able to approximate any unitary operation arbitrarily well. When applying such gates to a stabilizer state, the state becomes a linear combination of multiple stabilizer states, as shown in Section 2.5. Applying non-Clifford gates can be performed with by circuits consisting of Clifford gates, a magic state, and a post-selective measurement. The circuit then becomes equivalent to a Clifford circuit applied to a certain non-stabilizer state, which is important since Clifford operations can be implemented fault tolerantly [1]. By expressing this magic state as a linear combination of stabilizer states, any quantum circuit can be simulated [32]. In order to do so by using as few stabilizer states as possible, it is important to study additive properties of stabilizer states, such as their linear dependence. This chapter will explore ways in which we can represent this linear dependence using graphs.

In Chapter 2, we saw how graph states can be used to represent the application of gates to stabilizer states. Graph states, just like the stabilizer formalism, have many applications, such as in measurement based quantum computing [38], where they are prepared and inputted to the one-way quantum computer. Graph states are also used to construct codes in quantum error-correction [39, 40].

Furthermore, graph states can be extended to represent all stabilizer states by applying local Clifford operators to each of the qubits [30]. In fact, only a single layer of either Hadamard or phase gates needs to be applied to a graph state to result in an arbitrary stabilizer state [41, 42]. By representing stabilizer states in terms of graph states and local Clifford operations, graph states were used to classically simulate stabilizer circuits in [43]. Graph states can simulate certain classes of circuits an order of magnitude faster than stabilizer tableau methods can [35, 43].

Informally, our main results in this chapter can be summarized as follows. We derive

a unique canonical form for expressing any stabilizer state as a graph state with certain local Clifford operations applied to the vertices. By applying various restrictions to the set of allowable local Clifford operations, we achieve the uniqueness of our canonical form. Additionally, we give various algorithms for working with stabilizer states in this graph formalism, such as computing inner products and manipulating them using Clifford gates. We calculate the runtime of our algorithm and show a worst-case runtime of $O(nd^2)$, where n is the number of qubits and d is the degree of the graph. We also compute exact conditions on when a linear combination of two stabilizer state yields a third, or alternatively, when three stabilizer states are linearly dependent.

In Section 3.2, we give key definitions for this chapter. In the following three sections, we describe in detail three new contributions to the study of quantum states through graphs.

In Section 3.2, we show that graph states provide us with a new canonical form for stabilizer states, which is unique and phase sensitive. Also, this canonical form can be directly converted to a canonical circuit that prepares stabilizer states from a computational basis state. This circuit has only four blocks of Clifford gates, which is fewer than other canonical forms [44]. This chapter extends upon work done in [39, 41, 42], which show how to simplify stabilizer graphs, graph states with at most 2 layers of Hadamard and phase operators applied to them, to a reduced form. We show how to simplify *extended graph states*, a generalization of stabilizer graphs where each qubit can have an arbitrary local Clifford operator applied to it, to canonical form, and we also analyze the runtime of this compilation.

In Section 3.4, we present a simpler algorithm for graph state simulation. While the algorithm introduced in [43] for applying controlled-Pauli Z gates to extended graph states has many cases and does not provide insight about the updated state, we develop a formula that easily yields the updated state. Using our formula, we prove the near-impossibility of improving the theoretical runtime of applying controlled-Phase Z gates. Our results give further evidence for the fact that graph state simulation is most useful in circuits where neighbouring qubits have few interactions [35, 43].

In Section 3.5, we study the additive properties of stabilizer states by fully examining the special case of the linear dependence of three stabilizer states. We extend the work of García, Markov, and Cross [45] by finding two new cases of linearly dependent triplets. Our characterization enables efficient algorithms for detecting linear dependence between three stabilizer states and for computing stabilizer states that are in the span of two given stabilizer states. Additionally, we improve on the algorithm we saw in Chapter 2 for the merging of two stabilizer states related by a Pauli operator.

Appendix A contains a discussion of improving upper bounds on the stabilizer rank of magic states as well as a representation of a few optimal decompositions in the graph formalism. Appendix B contains proofs for the graph state transformation rules derived in this chapter.

3.2 The stabilizer and graph formalisms

Let us start by refreshing various key definitions and notations used throughout the chapter.

As in Definition 2.2.1, let a *Pauli operator* P on n qubits be of the form $i^k \bigotimes_{i=1}^n P_i$ where

$k \in \{0, 1, 2, 3\}$ and $P_i \in \{I, X, Y, Z\}$ is a Pauli matrix. The Pauli matrices are defined as $I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, and $Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Let the set of all Pauli operators be \mathcal{P} , the *Pauli group*.

Recall that for some gate U , we let $CU_{a,b}$ denote the *controlled- U gate* with control qubit a and target qubit b . For example, $CX_{a,b}$ denotes the *controlled- X gate* with control qubit a and target b , and we define $CY_{a,b}$ and $CZ_{a,b}$ similarly. We place subscripts on single-qubit operators to turn them into n -qubit operators where that operator is applied to the particular qubit referred to by the subscript, and n is contextual. For example, Z_1 would be the Pauli Z gate on qubit 1.

As in Definition 2.2.3, let a *Clifford operator* C on n qubits be a unitary operator on 2^n dimensional state space such that for all Pauli operators P on n qubits, $CPC^\dagger \in \mathcal{P}$. Let the set of all Clifford operators be \mathcal{C} , the *Clifford group*, which is generated by the *Hadamard gate* $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, the *phase gate* $S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, and any controlled-Pauli gate [28]. Additionally, applying certain controlled gates that modify phases in the computational basis to the same pair of qubits, we use the gate without a control. In particular, we have $CZ_{v,v} = Z_v$ and $CS_{v,v} = S_v$.

In Definition 2.2.6 we defined the Clifford operators C acting on a single qubit as *local Clifford operators*, and these operators are generated by H and S .

We introduce the shorthand $[n] := \{1, 2, \dots, n\}$. Recall from Definition 2.3.1 that an n -qubit state $|\psi\rangle$ is a *stabilizer state* if there exists a set of n commuting independent Pauli operators, $\{g_1, g_2, \dots, g_n\}$, such that for all $i \in [n]$, $g_i^2 = I$ and $g_i|\psi\rangle = |\psi\rangle$. We call the operators g_i *stabilizers*. A stabilizer state $|\psi\rangle$ is equivalently defined as a state resulting from the action of a Clifford operator C on a computational basis state [34].

For a graph G , we let $E(G)$ refer to the set of edges of G and $V = [n]$, where vertex i and qubit i are synonymous. We assume our graphs are undirected and do not have loop edges or multiple edges between two qubits. Let $N(i)$ be the set of neighbours of i in G not including i , where G is contextual. In this chapter, we will make use of several new graph operations.

Definition 3.2.1. The *local complementation about a vertex* (LCV) of a graph G at qubit v , $L_v(G)$, be a graph with the same number of vertices as G . The edges of G and $L_v(G)$ are identical with the following exception. For each unordered pair of vertices $u, w \in N(v)$, the edge (u, w) is present in $L_v(G)$ if and only if the edge (u, w) is not in G .

Definition 3.2.2. The *local complementation about an edge* (LCE) of a graph G is defined as follows. If (u, v) is an edge in graph G , the local complementation about the edge (u, v) is constructed from G by toggling several sets of edges. Specifically, we consider the three sets of vertices $N(u) \setminus (N(v) \cup \{v\})$, $N(v) \setminus (N(u) \cup \{u\})$, and $N(u) \cap N(v)$. For any pair of vertices (p, q) , if p and q each belong to a different set out of the three above, the edge (p, q) is toggled in G . Additionally, the adjacencies of u and v are swapped, meaning a vertex w is connected to u in the resulting graph if and only if it was connected to v in G and vice versa. We note that the resulting graph is equal to each of $L_u(L_v(L_u(G)))$ and $L_v(L_u(L_v(G)))$.

As defined in Definition 2.4.2, the *graph state* of a graph G , $|G\rangle$, is the stabilizer state

with stabilizers $g_v := X_v \prod_{u \in N(v)} Z_u$ for $v \in [n]$ [30]. An equivalent definition of graph states is

$$|G\rangle := \left(\prod_{(u,v) \in E(G)} CZ_{u,v} \right) |+\rangle^{\otimes n}, \quad (3.1)$$

where $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ [30]. When $|G\rangle$ is expressed as a state vector, the global phase is fixed by assuming the amplitude of $|0\rangle^{\otimes n}$ is positive and real.

We define our terminology for stabilizer states represented as applications of local Clifford operators to graph states, which is enabled by a theorem proved in [30].

Definition 3.2.3. An *extended graph state* is a stabilizer state written as a graph state with local Clifford operators applied to it in the form $C|G\rangle$ where C is a tensor product of local Clifford operators.

This definition formalizes the application of Clifford operations to graph states used in Chapter 2. Lastly, we let the *support* of a quantum state $|\psi\rangle$ be the number of non-zero amplitudes it has when written as a state vector, and let the *support set* be the set of vectors corresponding to the computational basis states with non-zero amplitudes in $|\psi\rangle$.

These definitions enable us to begin examining stabilizer states from the perspective of graph states.

3.3 Canonical forms for stabilizer states

When expressing a stabilizer state as a set of stabilizers, we have many choices for how to pick and order our set of stabilizer generators. This means that the task of deciding whether two stabilizer states are equal by considering their tableaus can be difficult to do by hand. Some attempts have been made to find a more canonical form for stabilizer presentation to make this task easier.

3.3.1 Canonical generator matrix

The binary representation of the stabilizer formalism [1] associates a binary vector with each Pauli operator generator. The generators of an n -qubit stabilizer state are stored in an $n \times 2n$ generator matrix. The rows of the generator matrix are linearly independent, and a shifted inner product can be defined so that it is 0 for all pairs of distinct rows of the generator matrix. Swapping rows corresponds to swapping generators, adding a row to another corresponds to multiplying generators, and switching columns corresponds to swapping qubits. These operations can transform a generator matrix into a *canonical form*,

$$\left(\begin{array}{cc|cc} I & A & B & 0 \\ 0 & 0 & A^T & I \end{array} \right), \quad (3.2)$$

where B is a symmetric matrix. However, this canonical form is not unique because of the freedom in choosing how to swap qubits. Furthermore, this canonical form can be converted into the *reduced form* for extended graph states [41].

Definition 3.3.1. Let an extended graph state $C|G\rangle$ be in *reduced form* if there exist n -tuples $c := (c_1, \dots, c_n)$ and $z := (z_1, \dots, z_n)$ with $c_v \in \{I, S, H\}$ and $z_v \in \{I, Z\}$ such that $C = \bigotimes_{v=1}^n c_v z_v$, and for all $(u, v) \in E(G)$, either $c_v \neq H$ or $c_u \neq H$.

The reduced form provides an elegant graphical representation of stabilizer states, but multiple extended graph states in reduced form can refer to the same quantum state. In this chapter we extend the conditions of the reduced form to find a description of a truly canonical form, meaning that each stabilizer state has a *unique* representation in this form.

3.3.2 A unique canonical form

To define our canonical form, we extend the definition of the reduced form.

Definition 3.3.2. Let an extended graph state in reduced form be in *canonical form* if for all $(u, v) \in E(G)$ such that $c_v = H$, we have $v < u$.

In subsequent chapters, we will refer to extended graph states expressed in this canonical form as diagrams in HK form, or HK diagrams.

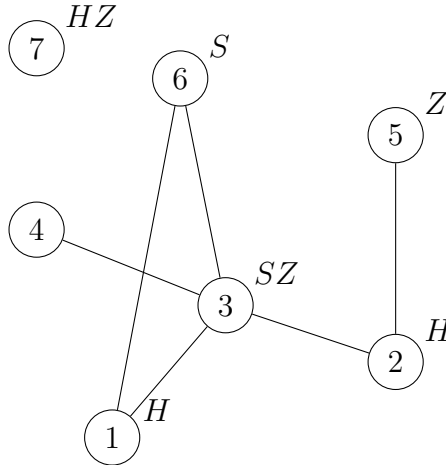


Figure 3.1: An illustration of the stabilizer state $|\psi\rangle$ in canonical form. Here, $|\psi\rangle = H_1 H_2 S_3 Z_3 Z_5 S_6 H_7 Z_7 |G\rangle$, where G is a 7-vertex graph with the edges $(1, 3)$, $(1, 6)$, $(2, 3)$, $(2, 5)$, $(3, 4)$, and $(3, 6)$. The vertices are ordered by their vertical position in the figure. Note that no H operations are on vertices adjacent to lower-numbered vertices.

An example of a state in canonical form is shown in Figure 3.1. The following result relates the number of H 's to the support and helps us prove the canonical form is unique.

Lemma 3.3.3. Let $|\psi\rangle = \left(\bigotimes_{v=1}^n c_v z_v \right) |G\rangle$ be in reduced form. Let k be the number of c_i that are equal to H . Then the support of $|\psi\rangle$ is 2^{n-k} .

Proof. Let $A := \{v \in [n] | c_v = H\}$, where $k = |A|$. We use the identity $H_v \cdot CZ_{u,v} = CX_{u,v} \cdot H_v$. We also define single-qubit Pauli operators p_i as $p_i := c_i z_i c_i^\dagger$. Then

$$\begin{aligned}
\left(\bigotimes_{v=1}^n c_v z_v \right) |G\rangle &= \left(\bigotimes_{v=1}^n p_v \right) \left(\prod_{v \in [n] \setminus A} (c_v)_v \right) \left(\prod_{v \in A} H_v \right) |G\rangle \\
&= \left(\bigotimes_{v=1}^n p_v \right) \left(\prod_{v \in [n] \setminus A} (c_v)_v \right) \left(\prod_{\substack{(u,v) \in E(G) \\ u,v \notin A}} CZ_{u,v} \right) \left(\prod_{v \in A} \left(H_v \prod_{u \in N(v)} CZ_{u,v} \right) \right) |+\rangle^{\otimes n} \\
&= \left(\bigotimes_{v=1}^n p_v \right) \left(\prod_{v \in [n] \setminus A} (c_v)_v \right) \left(\prod_{\substack{(u,v) \in E(G) \\ u,v \notin A}} CZ_{u,v} \right) \left(\prod_{\substack{v \in A \\ u \in N(v)}} CX_{u,v} \right) \left(\prod_{v \in A} H_v \right) |+\rangle^{\otimes n}. \quad (3.3)
\end{aligned}$$

$\prod_{i \in A} H_i |+\rangle^{\otimes n}$ has support 2^{n-k} because it consists of a tensor product of k $|0\rangle$'s and $n-k$ $|+\rangle$'s. The rest of Equation (3.3) is a product of phase operators, Pauli operators, and controlled-Pauli operators, which do not change the support of $|\psi\rangle$. \square

The main advantage of our canonical form is that it uniquely represents a stabilizer state.

Theorem 3.3.4. *If $|\psi\rangle = |\psi'\rangle$ up to global phase, and $|\psi\rangle := \bigotimes_{v=1}^n c_v z_v |G\rangle$ and $|\psi'\rangle := \bigotimes_{v=1}^n c'_v z'_v |G'\rangle$ are both in canonical form, then $G = G'$, $c = c'$, and $z = z'$. The representation of a state in canonical form is unique.*

Proof. Let $A := \{v \in [n] | c_v = H\}$ and $A' := \{v \in [n] | c'_v = H\}$. The supports of $|\psi\rangle$ and $|\psi'\rangle$ are equal, so by Lemma 3.3.3, $|A| = |A'|$. Let $k := |A| = |A'|$. Now let $A = \{a_1, a_2, \dots, a_k\}$ and $A' = \{a'_1, a'_2, \dots, a'_k\}$ where $a_1 < a_2 < \dots < a_k$, $a'_1 < a'_2 < \dots < a'_k$. Having defined these quantities, we will need several important definitions to continue the proof.

Definition 3.3.5. For a binary string s and a subset $B \subseteq [n]$ of the same size, let $|s\rangle\langle s|_B$ be a n -qubit projector onto the subspace of n -qubit state space spanned by the basis of computational basis states that agree with s on the qubits in B . We can think of $|s\rangle\langle s|_B$ as stretching the bits in s out in a n dimensional vector to occupy the slots corresponding to qubits in B , and we let s_v denote the bit in s in the slot corresponding to qubit v .

Definition 3.3.6. For a single-qubit state $|\varphi\rangle$ and a subset $B \subseteq [n]$, let $|\varphi\rangle_B$ be a tensor product of $|B|$ $|\varphi\rangle$'s, in the registers corresponding to the qubits in B .

Now, suppose for the sake of contradiction $a_1 < a'_1$. We will apply projectors of the form $|s\rangle\langle s|_{[n] \setminus A}$ and $|s\rangle\langle s|_{[n] \setminus A'}$ to $|\psi\rangle$ and $|\psi'\rangle$ to derive a contradiction. Letting $Q := |s\rangle\langle s|_{[n] \setminus A}$, we write

$$Q \left(\bigotimes_{v=1}^n c_v z_v \right) |G\rangle = \left(\bigotimes_{v=1}^n c_v z_v \right) \left(\prod_{(u,v) \in E(G)} CZ_{u,v} \right) Q |+\rangle^{\otimes n} \quad (3.4)$$

$$= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c_v z_v \right) \left(\prod_{(u,v) \in E(G)} CZ_{u,v} \right) |+\rangle_A \otimes |s\rangle \quad (3.5)$$

$$= \frac{1}{\sqrt{2^{n-|A|}}} \left(\bigotimes_{v=1}^n c_v z_v \right) \left(\prod_{(u,v) \in E(G)} Z_u^{s_v} \right) |+\rangle_A \otimes |s\rangle \quad (3.6)$$

$$= \frac{1}{\sqrt{2^{n-|A|}}} \left(\bigotimes_{v=1}^n p_v \right) \left(\prod_{v \in [n] \setminus A} (c_v)_v \right) |0\rangle_A \otimes |s\rangle. \quad (3.7)$$

Here, Equation (3.4) uses the fact that Q commutes with diagonal operators such as S , Z , and CZ . Equation (3.5) applies Q to the state vector of supported equally on all computational basis states, which sets the bits in $[n] \setminus A$ to match s . Equation (3.6) follows from assuming without loss of generality that $v \notin A$ due to there being no edges in G between qubits in A , so at least one of u and v is not in A . Equation (3.7) is derived by conjugating the Z operators to form Pauli operators p_i . We then observe the following.

Lemma 3.3.7. *For all binary strings s of length $n - k$, $|s\rangle \langle s|_{[n] \setminus A} |\psi\rangle$ and $|s\rangle \langle s|_{[n] \setminus A'} |\psi'\rangle$ are computational basis states.*

Proof. By Equation (3.7), $|s\rangle \langle s|_{[n] \setminus A} |\psi\rangle$ is a single computational basis state because it consists of Pauli and phase operators applied to a computational basis state, and similarly $|s\rangle \langle s|_{[n] \setminus A'} |\psi'\rangle$ is as well. \square

We consider $Q_1 := |s\rangle \langle s|_{[n] \setminus A'}$, where $s_{a_1} = 1$ and the rest of the s_v equal 0, note that by our assumption that $a_1 < a'_1$, we have $a_1 \in ([b] \setminus A')$. If we also set $Q_2 := |0\rangle \langle 0|_{[n] \setminus A'}$, we have the following claim.

Claim 3.3.8. *$Q_1 |\psi'\rangle$ and $Q_2 |\psi'\rangle$ are computational basis states that differ only in qubit a_1 .*

Proof. By Equation (3.6),

$$\begin{aligned}
Q_1 |\psi'\rangle &= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c'_v z'_v \right) \left(\prod_{(u,v) \in E(G')} Z_u^{s_v} \right) |+\rangle_{A'} \otimes |s\rangle \\
&= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c'_v z'_v \right) \left(\prod_{u \in N_{G'}(a_1)} Z_u \right) |+\rangle_{A'} \otimes |s\rangle \\
&= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c'_v z'_v \right) |+\rangle_{A'} \otimes |s\rangle \\
&= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n p'_v \right) \left(\prod_{v \in [n] \setminus A'} (c'_v)_v \right) |0\rangle_{A'} \otimes |s\rangle. \tag{3.8}
\end{aligned}$$

Here, the third step follows by the fact that no neighbours of a_1 in G' can be in A' since $a_1 < a'_1$ and $|\psi'\rangle$ is in canonical form, so vertices where $c_v = H$ cannot be connected to lower numbered vertices such as a_1 . Thus, Z_u must act on the register $|s\rangle$, which is equal to $|0\rangle$ on all qubits other than a_1 . Again, the final expression must be a computational basis state as the state is only transformed by Pauli and phase operators.

We also have

$$\begin{aligned}
Q_2 |\psi'\rangle &= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c'_v z'_v \right) \left(\prod_{(u,v) \in E(G')} Z_u^0 \right) |+\rangle_{A'} \otimes |0\rangle_{[n] \setminus A'} \\
&= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n c'_v z'_v \right) |+\rangle_{A'} \otimes |0\rangle_{[n] \setminus A'} \\
&= \frac{1}{\sqrt{2^{n-k}}} \left(\bigotimes_{v=1}^n p'_v \right) \left(\prod_{v \in [n] \setminus A'} (c'_v)_v \right) |0\rangle_{A'} \otimes |0\rangle_{[n] \setminus A'}. \tag{3.9}
\end{aligned}$$

Once again, this must be a computational basis state. Since the support of s only contains a single qubit, we have proven our claim that $Q_1 |\psi'\rangle$ and $Q_2 |\psi'\rangle$ are basis-states differing only in qubit a_1 . \square

Let s' be the unique binary string such that $|s'\rangle \langle s'|_{[n] \setminus A} Q_1 |\psi'\rangle = Q_1 |\psi'\rangle$. Equivalently, s' is the string of bits of the basis state $Q_1 |\psi'\rangle$ on $[n] \setminus A$. By Claim 3.3.8, $|s'\rangle \langle s'|_{[n] \setminus A} Q_2 |\psi'\rangle = Q_2 |\psi'\rangle$ since $a_1 \notin [n] \setminus A$. Then, the support of $|s'\rangle \langle s'|_{[n] \setminus A} |\psi'\rangle$ is at least 2, with at least one term coming from each of Q_1 and Q_2 . However, the support of $|s'\rangle \langle s'|_{[n] \setminus A} |\psi\rangle$ is 1 by Lemma 3.3.7. Since $|\psi\rangle = |\psi'\rangle$, this produces the desired contradiction.

This has merely shown that $a_1 = a'_1$. We cancel H_{a_1} from both sides and repeat this procedure. Each time we do this, we reduce k by 1 until k is 0. Now, for all v , we have $c_v z_v \in \{I, S, Z, SZ\}$. If $c_v \neq c'_v$ or $z_v \neq z'_v$ for some v , then the amplitudes of $|0\rangle^{\otimes(v-1)} \otimes |1\rangle \otimes |0\rangle^{\otimes(n-j)}$ in $|\psi\rangle$ and $|\psi'\rangle$ would differ by some positive power of i . Therefore, $c = c'$ and $z = z'$, and we have $|G\rangle = |G'\rangle$. If $(u, v) \in E(G)$ but $(u, v) \notin E(G')$ or vice versa, the amplitudes of

$|1\rangle_{\{i,j\}} \otimes |0\rangle_{[n]\setminus\{i,j\}}$ would differ. Since $|\psi\rangle = |\psi'\rangle$, we also have that $G = G'$. This completes the proof of the theorem stating the uniqueness of our canonical form. \square

We show that any stabilizer state can be expressed in our canonical form by a counting argument. In [34], it is proven that the number of n -qubit stabilizer states is

$$2^n \prod_{k=1}^n (2^k + 1). \quad (3.10)$$

Since our canonical form is unique, it suffices to show the following result.

Theorem 3.3.9. *There are $2^n \prod_{k=1}^n (2^k + 1)$ n -qubit extended graph states in canonical form.*

Proof. We wish to count all possible c, z , and G such that $c_v \in \{I, S, H\}$ and $z_v \in \{I, Z\}$ for all $v \in [n]$ and whenever $c_v = H$, all the edges in G incident to v connect to higher numbered qubits. For each qubit k , we choose c_k, z_k , and all the edges of the form (v, k) where $v < k$. If we decide to select none of the (v, k) to add to $E(G)$, then there are no restrictions on c_k and z_k , yielding 6 possibilities. Otherwise, the only restriction is $c_k \neq H$, and there are $2^{k-1} - 1$ possible choices for the edges, yielding $4(2^{k-1} - 1)$ possibilities. In total, there are $2^{k+1} + 2$ ways to choose c_k, z_k , and all the edges of the form (v, k) where $v < k$, and doing so for each $1 \leq k \leq n$ yields all possible extended graph state in canonical form. Thus, there are $\prod_{k=1}^n (2^{k+1} + 2) = 2^n \prod_{k=1}^n (2^k + 1)$ n -qubit extended graph states in canonical form. \square

3.3.3 Simplifying extended graph states

We demonstrate how to simplify extended graph states to canonical form. As in [41], we repeatedly apply two transformation rules. The first rule relates $|L_v(G)\rangle$ to $|G\rangle$.

Theorem 3.3.10 (Hein, Eisert, and Briegel [31]). *For any graph state $|G\rangle$ and qubit v ,*

$$|G\rangle = H_v S_v^\dagger H_v \left(\prod_{u \in N(v)} S_u \right) |L_v(G)\rangle. \quad (3.11)$$

The second transformation, discovered by [41], allows us to simplify extended graph states to reduced form by eliminating pairs of H 's applied to connected qubits and also allows us to simplify to canonical form by sliding remaining H 's down to lower-numbered qubits.

Theorem 3.3.11 (Elliott, Eastin, and Caves [41]). *Let (u, v) be an edge in $E(G)$. Let $A = N(u) \cup \{u\}$ and $B = N(v) \cup \{v\}$. Then,*

$$H_u H_v |G\rangle = Z_u Z_v \left(\prod_{p \in A, q \in B} CZ_{p,q} \right) |G\rangle. \quad (3.12)$$

Remark 3.3.12. Note that the transformation applied to the graph G in Equation (3.12) is precisely a local complementation about the edge (u, v) . Specifically, this refers to the edges toggled with CZ gates and not the factors of Z_w from a term of the form $CZ_{u,w}$ or the other local Clifford operations in the expression.

Additionally, as discussed in Section 2.5, the action on a graph of a product of the form $\prod_{p,q \in R} CS_{p,q}$ will precisely toggle every edge in the set R , in addition to apply several local operations. This means that if we set $R = N(v)$ to be a neighbourhood of a vertex v , we can use the CS product to perform a local complementation about the vertex v . This allows us to express Equation (3.11) in terms of CS gates.

The runtime of the graph state simplification algorithm, though cubic in the worst case, can be much quicker.

Theorem 3.3.13. *There exists an algorithm to simplify an arbitrary extended graph state, $|\psi\rangle := \left(\bigotimes_{v=1}^n C_v \right) |G\rangle$, into canonical form, that runs in $O(nd^2)$, where d is the maximum degree in G encountered during the calculation.*

Proof. Multiplying both sides of Equation (3.11) by $S_v H_v$, we obtain

$$S_v H_v |G\rangle = H_v \left(\prod_{u,w \in N(v)} CS_{u,w} \right) |G\rangle. \quad (3.13)$$

Equivalently,

$$H_v S_v H_v |G\rangle = \left(\prod_{u,w \in N(v)} CS_{u,w} \right) |G\rangle. \quad (3.14)$$

Multiplying both sides of Equation (3.13) by $H_x S_x H_x S_x^\dagger$, we obtain

$$\begin{aligned} H_v S_v |G\rangle &= H_v S_v H_v S_v^\dagger H_v \left(\prod_{u,w \in N(v)} CS_{u,w} \right) |G\rangle \\ &= \frac{1+i}{\sqrt{2}} S_v^3 \left(\prod_{u \in N(v)} Z_u \right) \left(\prod_{u,w \in N(v)} CS_{u,w} \right) |G\rangle. \\ &= \frac{1+i}{\sqrt{2}} \left(\prod_{u \in N(v) \cup \{v\}} S_u^3 \right) |L_v(G)\rangle. \end{aligned} \quad (3.15)$$

Since $C_v \in \langle H, S \rangle$, each C_v is equivalent to a product of H 's and S 's. Since $HH = I$ and $SS = Z$ are both Pauli operators, C_v is equivalent to a global phase and a Pauli operator applied to an alternating product of H 's and S 's, which we define as D_v . Thus we can write $|\psi\rangle = \alpha P \left(\bigotimes_{v=1}^n D_v \right) |G\rangle$ for some phase α and some Pauli operator P . In what follows, we do not mention Pauli operators or global phases because we can automatically keep track of them by conjugating them through and updating α and P accordingly. We define the following useful monovariant and describe an algorithm to decrease it.

Definition 3.3.14. Let M be the sum of the total number of H 's among all D_v for $1 \leq v \leq n$ as well as the number of vertices v such that D_v ends in SH .

Our goal will be to reduce M as much as possible until all terms D_v consist of at most one Clifford operation.

Lemma 3.3.15. *If D_v has length at least 2, we can update D_v and all D_u for $u \in N(v)$ so that M decreases.*

Proof. If D_v ends in HS , we apply Equation (3.15) on qubit v , which effectively removes HS from D_v and appends S onto the ends of D_v and all D_u where $u \in N(v)$. This move does not increase the number of terms that end in SH but does decrease the number of H 's in D_v . If this transformation cannot be performed, then D_v ends in SH since it has length at least 2. In this case, we apply Equation (3.13) to vertex v . This replaces the SH in D_v with H , which decreases M by 1. This also adds S gates to $N(v)$, which does not increase M . This proves the claim. \square

We can apply the updates in Lemma 3.3.15 a finite number of times until all products D_v have length at most 1, in which case $D_v \in \{I, S, H\}$ for all v . Rearranging Equation (3.12) and assuming $u > v$, we have

$$H_v |G\rangle = H_u Z_v Z_u \left(\prod_{p \in A, q \in B} CZ_{p,q} \right) |G\rangle, \quad (3.16)$$

which we repeatedly apply on qubits u with D_u ending in H whenever u has a neighbour v in G with $v < u$. If v already contained a local H operation, the two H gates cancel out. This procedure must terminate after a finite number of steps since the total index of all H gates can only decrease. After this terminates, we conjugate P through the remaining local Clifford operations. Using the fact that $X_v |G\rangle = \left(\prod_{u \in N(v)} Z_u \right) |G\rangle$, and $Y = -iZX$, we can turn all Y 's and X 's into Z 's and phases. Now, we have transformed $|\psi\rangle$ into our canonical form.

Every time we apply Theorem 3.3.11, Equation (3.13), or Equation (3.15), we perform $O(d^2)$ edge toggles where d is the maximum degree of G . Initially, $M = O(n)$ because any local Clifford operator can be represented with a finite number of H 's. Then, shortening the lengths of all the D_v terms to 1 takes $O(nd^2)$ operations. Next, we only need to apply Equation (3.16) at most $n - 1$ times by applying it for $v = n, n - 1, n - 2, \dots, 2$ in that order. Since the H 's move to lower numbered qubits or are eliminated, the only way an H could still exist on a qubit i after the algorithm passes through i the first time is if right before the algorithm passes through v , all $u \in N(v)$ satisfy $u > i$. In that case, $N(i)$ cannot change once $v < i$, because i is not connected to any lower-numbered qubits. Therefore, after v reaches 2, none of the H 's can be moved to lower numbered qubits. Thus, moving the H 's to the lowest possible numbered qubits takes $O(nd^2)$ operations. Removing all D_v that end in SH using Equation (3.13) takes $O(nd^2)$ operations, and simplifying the Pauli operators takes $O(nd)$ operations, so the total runtime is $O(nd^2)$. \square

3.4 Graph state stabilizer simulation

3.4.1 Algorithm

Graph state simulators of stabilizer circuits are advantageous in that local Clifford gates such as S and H can be applied trivially in $O(1)$ time. The bottleneck of a graph state simulator is the application of controlled-Pauli gates, such as CZ gates, which currently can be done in $O(d^2)$ time where d is the maximum degree of the graph encountered during the calculation.

To apply a gate $CZ_{u,v}$ to an extended graph state $|\psi\rangle = \left(\bigotimes_{v=1}^n C_v\right) |G\rangle$, we use the identity

$$CZ_{u,v} = \frac{1}{2} ((I + Z_u) + (I - Z_u)Z_v).$$

If we conjugate this expression through the C_i , it suffices to apply operators of the form $\frac{1}{2}((I + P_u)I_v + (I - P_u)Q_v)$ to graph states $|G\rangle$ where P_u and Q_v are Hermitian Pauli operators. This motivates the following definition.

Definition 3.4.1. For Hermitian Pauli operators P and Q , let $|\psi_{PQ}\rangle$ be the extended graph state obtained from simplifying the expression

$$|\psi_{PQ}\rangle = \frac{1}{2} ((I + P_u) + (I - P_u)Q_v) |G\rangle. \quad (3.17)$$

For example, $|\psi_{ZZ}\rangle$ is $CZ_{u,v} |G\rangle$, so updating G takes $O(1)$ time. The values of u and v are contextual for ψ_{PQ} .

Our expressions for $|\psi_{PQ}\rangle$ and the update times based on the expressions are depicted in Table 3.1.

The formulas for $|\psi_{ZX}\rangle$ and $|\psi_{XX}\rangle$ were derived by Elliott, Eastin, and Caves [42]. The rest of the formulas are computed by applying Theorem 2.5.2 and Theorem 3.5.1. Since all the proofs are similar, they can be found in Appendix B.

3.4.2 Discussion

To apply a CZ gate to qubits u and v of the extended graph state $|\psi\rangle = \left(\prod_{w=1}^n C_w\right) |G\rangle$, the original graph state simulation algorithm described in [33, 43] performs local complementations on u , v , or neighbouring qubits of u and v , changing C_u and C_v until they are both diagonal. Local complementations run in $\Omega(d^2)$, where d is the degree of the vertex at which it was applied. When applying a CZ gate using our algorithm, if $P = \pm Z$ or $Q = \pm Z$, then it takes $O(d)$ time and runs faster than the original algorithm would have. For example, when $C_u = HSH = \sqrt{X}$ and $C_v = I$, the original algorithm would perform a local complementation at qubit u , whereas our algorithm would update $|\psi\rangle$ more efficiently, based on the expression in Table 3.1 for $|\psi_{YZ}\rangle$.

In order to perform CZ updates in under quadratic time, we must find efficient update rules for $|\psi_{PQ}\rangle$ for all pairs $(P, Q) \in \{(X, X), (Y, Y), (X, Y)\}$. We show that the runtime for such update rules cannot be improved further.

(P, Q)	$ \psi_{PQ}\rangle$	Runtime
(Z, Z)	$CZ_{u,v} G\rangle$	$O(d)$
(Z, X)	$\left(\prod_{w \in N_v} CZ_{u,w} \right) G\rangle$	
(Y, Z)	$S_v Z_v \left(\prod_{w \in M_u} CZ_{v,w} \right) G\rangle$	
$(X, X), (u, v) \in E$	$H_u H_v CZ_{u,v} \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) G\rangle$	$O(d^2)$
$(X, X), (u, v) \notin E$	$\left(\prod_{p \in N_u, q \in N_v} CZ_{p,q} \right) G\rangle$	
$(Y, X), (u, v) \in E$	$\frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_u \Delta N_v} CZ_{u,w} \right) L_u(G)\rangle$	
$(Y, X), (u, v) \notin E$	$\left(\prod_{w \in M_u \Delta N_v} Z_w \right) \left(\prod_{p, q \in M_u \Delta N_v} CS_{p,q} \right) \left(\prod_{p, q \in M_u} CS_{p,q} \right) G\rangle$	
$(Y, Y), (u, v) \in E$	$-i \left(\prod_{p, q \in M_u} CS_{p,q} \right) \left(\prod_{p, q \in M_v} CS_{p,q} \right) G\rangle$	
$(Y, Y), (u, v) \notin E$	$\frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_2} CZ_{u,w} \right) L_u(G)\rangle$	

Table 3.1: A table of formulas for $|\psi_{PQ}\rangle$ as defined in Definition 3.4.1, where $d = \max(\deg(u), \deg(v))$. With this data, we can compute $|\psi_{PQ}\rangle$ for all possible unordered pairs (P, Q) since $|\psi_{PQ}\rangle$ and $|\psi_{QP}\rangle$ are equal with the roles of qubits u and v flipped, and changing the sign of P changes $|\psi_{PQ}\rangle$ by Q . Note that $|\psi_{PQ}\rangle$ is not necessarily in canonical form. Also, we define the shorthands $N_w := N(w)$ and $M_w := N_w \cup \{w\}$. The operand Δ denotes the symmetric difference of two sets. Note that for $(P, Q) \in \{(Z, Z), (Z, X), (Y, Z)\}$, $|\psi_{PQ}\rangle$ consists of $O(d)$ CZ operators applied to $|G\rangle$, whereas for $(P, Q) \in \{(X, X), (Y, X), (Y, Y)\}$, $|\psi_{PQ}\rangle$ consists of $O(d^2)$ CZ operators and $O(d)$ local Clifford operators applied to $|G\rangle$, hence the $O(d^2)$ update time. Additionally, we split the latter expressions into cases based on whether or not the graph G contains the edge (u, v) . The proofs of these statements are found in Appendix B.

Theorem 3.4.2. *There exists a family of extended graph states such that applying a CZ gate requires $\Omega(n^2)$ edges of G to be toggled.*

Proof. Let A and B be disjoint sets such that $A, B \subset [n]$, $|A| = \Omega(n)$, and $|B| = \Omega(n)$. We select vertices $u \in A$, $v \in B$. The following graphs are used in this proof.

Definition 3.4.3. Let $W_{p,q}$, where $p \in A$ and $q \in B$, be the graph consisting solely of the following edge set E .

1. $(p, q) \in E$
2. For all $w \in A \setminus \{p\}$, $(p, w) \in E$
3. For all $w \in B \setminus \{q\}$, $(q, w) \in E$

Let graph $K_{A,B}$ be the complete bipartite graph with edges between each vertex in A and each vertex in B . Let K_A (respectively, K_B) be the graph union of K together with all the edges between vertices in A (B). Let $K_{A,w}$ ($K_{B,w}$) be the graph where all the vertices in A (B) are connected to each other, and vertex w is connected to every other vertex. Let G be the graph that has all possible edges, except those between vertex v and the vertices in A .

With these definitions, we can state the following lemma.

Lemma 3.4.4. *Let R be the set of all graphs G' that are local Clifford equivalent to $|W_{u,v}\rangle$. Then*

$$R = \{K_{A,B}, K_A, K_B\} \cup \{K_{A,w} | w \in B\} \cup \{K_{B,w} | w \in A\} \cup \{W_{p,q} | p \in A, q \in B\}. \quad (3.18)$$

Proof. By a theorem proved in [30], the local Clifford equivalence of the graph states $|G'\rangle$ and $|W_{u,v}\rangle$ is equivalent to the existence of a sequence of local complementation operations taking G' to $W_{u,v}$. If we let \mathcal{G} be the orbit of $W_{u,v}$ under local complementation, then $R = \mathcal{G}$. \mathcal{G} is depicted in Figure 3.2. The rest of the proof details traversing \mathcal{G} . For all $i \in A$ and $j \in B$,

- We consider all the edges in \mathcal{G} emanating from $W_{i,j}$. For all $k \in [n] \setminus \{i, j\}$,

$$L_i(W_{i,j}) = K_{A,j} \quad L_j(W_{i,j}) = K_{B,i} \quad L_k(W_{i,j}) = W_{i,j} \quad (3.19)$$

- We consider all the edges in \mathcal{G} emanating from $K_{A,j}$. The case for $K_{B,i}$ is analogous. For all $k \in B \setminus \{j\}$,

$$L_i(K_{A,j}) = W_{i,j} \quad L_j(K_{A,j}) = K_B \quad L_k(K_{A,j}) = K_{A,j} \quad (3.20)$$

- We consider all the elements of \mathcal{G} reachable from $K_{A,B}$, K_A , or K_B in a single local complementation.

$$\begin{aligned} L_i(K_A) &= K_{B,i} & L_j(K_A) &= K_{A,B} \\ L_i(K_B) &= K & L_j(K_B) &= K_{A,j} \\ L_i(K_{A,B}) &= K_B & L_j(K_{A,B}) &= K_A \end{aligned} \quad (3.21)$$

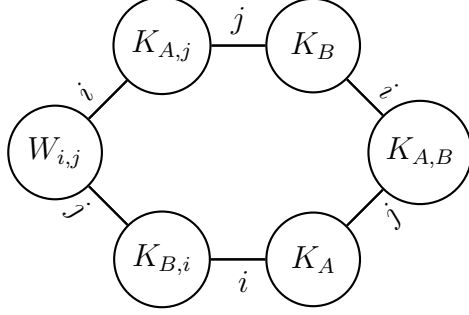


Figure 3.2: A depiction of \mathcal{G} in the proof of Lemma 3.4.4, with undirected edges labelled with the vertex that local complementation is applied to and loop edges omitted. To generate \mathcal{G} in its entirety, let i and j range over all vertices in A and in B respectively.

- The graph $W_{u,v}$ is in the same orbit as $W_{i,j}$ in \mathcal{G} .

$$L_j(L_v(L_i(L_u(W_{u,v})))) = W_{i,j} \quad (3.22)$$

This completes the proof. \square

We show that $|E(G) \Delta E(G')| = \Omega(n^2)$ for any $G' \in R$. Suppose without loss of generality that $\frac{1}{2}n \leq |A| \leq cn$ where c is some fixed constant less than 1. Then K_A has $\binom{n}{2} - \binom{|B|}{2}$ edges, which is the most number of edges out of all graphs in R .

$$|E(G) \Delta E(G')| \geq |E(G)| - |E(G')| \geq \binom{n}{2} - |A| - \left(\binom{n}{2} - \binom{|B|}{2} \right) \geq \binom{|B|}{2} - |A|. \quad (3.23)$$

Thus, $|E(G) \Delta E(G')| = \Omega(n^2)$ since $|B| \geq (1-c)n = \Omega(n)$. \square

3.5 Additive properties of stabilizer states

3.5.1 Graph merging

We now consider the case of two states related by a Pauli operator. The case when the Pauli operator acts on a single qubit was explored in [31], and the case when the Pauli operator acts on multiple qubits was explored in [42] as well as in Chapter 2. We restate Theorem 2.5.2 here. In [42] a related theorem is proven but without the case where k is odd.

Let $A = N(1) \cup \{1\}$, and let B be a set including 1. Let k be an integer. Then

$$\frac{1}{\sqrt{2}} \left(I + i^k \prod_{u \in B} Z_u \right) |G\rangle = H_v Z_v \left(\prod_{u,w \in A} C S_{u,w}^k \right) \left(\prod_{u \in A, w \in B} C Z_{u,w} \right) |G\rangle. \quad (3.24)$$

Here we provide an alternative formula for when k is odd that is more concise than previous formulas.

Theorem 3.5.1. *Let $k = 2m + 1$. Let A be an arbitrary set. Then*

$$\frac{1}{\sqrt{2}}(I + i^{2m+1} \prod_{u \in A} Z_u) |G\rangle = \frac{1 + i^{2m+1}}{\sqrt{2}} \left(\prod_{u \in A} Z_u^{m+1} \right) \left(\prod_{u,v \in A} CS_{u,v} \right) |G\rangle. \quad (3.25)$$

Proof. Let $|z\rangle$ be some computational basis state, and let r be the number of values i in A where the i^{th} bit in z is 1. Let indicator functions f and g be defined as $f(r) = 1$ when $r \equiv 2 \pmod{4}$ or $r \equiv 3 \pmod{4}$ and 0 otherwise and $g(r) = 1$ when r is odd and 0 otherwise. Then,

$$\begin{aligned} & \langle z | \frac{1}{\sqrt{2}} (I + i^{2m+1} \prod_{p \in A} Z_p) |G\rangle \\ &= \frac{1}{\sqrt{2}} (\langle z | G\rangle + i^{2m+1} (-1)^r \langle z | G\rangle) \\ &= \frac{1}{\sqrt{2}} (1 + i^{2m+1} (-1)^r) \langle z | G\rangle, \end{aligned} \quad (3.26)$$

and

$$\begin{aligned} & \langle z | \frac{1 + i^{2m+1}}{\sqrt{2}} \prod_{p \in A} Z_p^{m+1} \prod_{p,q \in A} CS_{p,q} |G\rangle \\ &= \frac{1 + i^{2m+1}}{\sqrt{2}} (-1)^{f(r)} (-1)^{(m+1)r} i^r \langle z | G\rangle \\ &= \frac{1 + i^{2m+1}}{\sqrt{2}} i^{g(r)} (-1)^{(m+1)r} \langle z | G\rangle. \end{aligned} \quad (3.27)$$

The two expressions are equal for all parities of m and r . \square

The merging formulas, Theorem 2.5.2 and Theorem 3.5.1, can be used to compute measurements of Pauli operators on extended graph states, by conjugating Pauli projectors through the local Clifford operators. These formulas can also be used to prove the correctness of the expressions for $|\psi_{PQ}\rangle$ in Table 3.1, which we do in Appendix B.

Considering ways to merge stabilizer states that are not related by a Pauli operator, an interesting formula arises when u and v are not connected in Theorem 3.3.11.

Theorem 3.5.2. *Let u and v be two vertices of graph G such that $(u, v) \notin E(G)$. Let sets M_u and M_v be defined as $M_u = N(u) \cup \{u\}$ and $M_v = N(v) \cup \{v\}$. Then*

$$H_u H_v |G\rangle = Z_u Z_v |G\rangle + \left(\prod_{w \in N(u)} Z_w \right) \left(\prod_{w \in N(v)} Z_w \right) \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) |G\rangle. \quad (3.28)$$

Proof. We start by defining the states $|\psi\rangle$, $|\phi_1\rangle$, and $|\phi_2\rangle$ as $|\psi\rangle = H_u H_v |G\rangle$, $|\phi_1\rangle = Z_u Z_v |G\rangle$, and $|\phi_2\rangle = \left(\prod_{w \in N(u)} Z_w \right) \left(\prod_{w \in N(v)} Z_w \right) \left(\prod_{p \in A, q \in B} CZ_{p,q} \right) |G\rangle$. For any bit string s , we seek to show that $\langle s | \psi\rangle = \langle s | \phi_1\rangle + \langle s | \phi_2\rangle$.

We start by computing $\langle s|\psi\rangle$. Let s_i be the bit in the i^{th} position of s and let s_R be the number of 1's in s at the indices denoted by set R , or equivalently, the sum of s_i over $i \in R$. We proceed by applying the H operations in $|\psi\rangle$ to $\langle s|$ and producing a sum of four states, one for each possibility for the values of s_u and s_v . We denote these states as s with X_u and X_v applied with appropriate exponents. We also make use of the stabilizers of a graph.

$$\langle s|\psi\rangle = \langle s|H_u H_v|G\rangle \quad (3.29)$$

$$= \frac{1}{2} \sum_{i,j \in \{0,1\}} (-1)^{s_u i + s_v j} \langle s|X_u^{s_u+i} X_v^{s_v+j}|G\rangle \quad (3.30)$$

$$= \frac{1}{2} \sum_{i,j \in \{0,1\}} (-1)^{s_u i + s_v j} \left\langle s \left| \left(\prod_{w \in N(u)} Z_w^{s_u+i} \right) \left(\prod_{w \in N(v)} Z_w^{s_v+j} \right) \right| G \right\rangle \quad (3.31)$$

$$= \frac{1}{2} \sum_{i,j \in \{0,1\}} (-1)^{s_u i + s_v j + (s_u+i)s_{N(u)} + (s_v+j)s_{N(v)}} \langle s|G\rangle \quad (3.32)$$

$$= \frac{1}{2} \sum_{i,j \in \{0,1\}} (-1)^{(s_u+s_{N(u)})i + (s_v+s_{N(v)})j + s_u s_{N(u)} + s_v s_{N(v)}} \langle s|G\rangle \quad (3.33)$$

If either $s_u + s_{N(u)}$ or $s_v + s_{N(v)}$ are odd, the entire expression will be 0. If that is not the case, the expression will be $2(-1)^{s_u+s_v} \langle s|G\rangle$.

We also see that $\langle s|\phi_1\rangle = (-1)^{s_u+s_v} \langle s|G\rangle$. All that remains is to compute $\langle s|\phi_2\rangle$.

$$\langle s|\phi_2\rangle = \left\langle s \left| \left(\prod_{w \in N(u)} Z_w \right) \left(\prod_{w \in N(v)} Z_w \right) \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) \right| G \right\rangle \quad (3.34)$$

$$= (-1)^{s_{N(u)} + s_{N(v)} + s_{M_u} s_{M_v}} \langle s|G\rangle \quad (3.35)$$

$$= (-1)^{s_{N(u)} + s_{N(v)} + (s_u + s_{N(u)})(s_v + s_{N(v)})} \langle s|G\rangle \quad (3.36)$$

If $s_u + s_{N(u)}$ is odd, we have the following.

$$\langle s|\phi_1\rangle + \langle s|\phi_2\rangle = (-1)^{s_u+s_v} \langle s|G\rangle + (-1)^{s_{N(u)} + s_{N(v)} + (s_u + s_{N(u)})(s_v + s_{N(v)})} \langle s|G\rangle \quad (3.37)$$

$$= (-1)^{s_u+s_v} \langle s|G\rangle + (-1)^{s_{N(u)} + s_v} \langle s|G\rangle \quad (3.38)$$

$$= (-1)^{s_v} ((-1)^{s_u} + (-1)^{s_{N(u)}}) \langle s|G\rangle = 0 \quad (3.39)$$

Analogously, the same is true if $s_v + s_{N(v)}$ is odd. If both $s_u + s_{N(u)}$ and $s_v + s_{N(v)}$ are even, we simplify our expression further.

$$\langle s|\phi_1\rangle + \langle s|\phi_2\rangle = (-1)^{s_u+s_v} \langle s|G\rangle + (-1)^{s_{N(u)} + s_{N(v)} + (s_u + s_{N(u)})(s_v + s_{N(v)})} \langle s|G\rangle \quad (3.40)$$

$$= (-1)^{s_u+s_v} \langle s|G\rangle + (-1)^{s_{N(u)} + s_{N(v)}} \langle s|G\rangle = (-1)^{s_u+s_v} \langle s|G\rangle \quad (3.41)$$

This shows that $\langle s|\psi\rangle$ is always equal to $\langle s|\phi_1\rangle + \langle s|\phi_2\rangle$, which completes our proof. \square

3.5.2 Linearly dependent triplets

We now turn our attention to characterizing linearly dependent triplets of stabilizer states. The following theorem shows that there are three types.

Theorem 3.5.3. *Let $\mathcal{S} := \{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ be a set of linearly dependent stabilizer states that are not all parallel. Then, up to global phase, one of the three cases must be true*

1. *For some stabilizer state $|\phi\rangle$ and some Pauli operator P ,*

$$\mathcal{S} = \{|\phi\rangle, P|\phi\rangle, \frac{I+P}{\sqrt{2}}|\phi\rangle\}. \quad (3.42)$$

2. *For some Clifford operator C , $1 \leq v \leq n$, an extended graph state in reduced form $|\psi\rangle$ such that v is the only vertex u such that $c_u \neq H$, and $z_u = I$ whenever $c_u = H$,*

$$\mathcal{S} = \{C|0^n\rangle, C|\psi\rangle, C(S_x|\psi)\}. \quad (3.43)$$

3. *For some Clifford operator C , $1 \leq u < v \leq n$, an extended graph state in reduced form $|\psi\rangle$ such that u and v are the only two vertices w such that $c_w \neq H$, and $z_w = I$ whenever $c_w = H$,*

$$\mathcal{S} = \{C|0\rangle^{\otimes n}, C|\psi\rangle, C(Z_u Z_v C Z_{u,v} |\psi)\}. \quad (3.44)$$

Proof. Let U be a Clifford operator such that $|\psi_1\rangle = U|0\rangle^{\otimes n}$. Let $|\psi\rangle := U^\dagger|\psi_2\rangle$ and $|\varphi\rangle := U^\dagger|\psi_3\rangle$. Any stabilizer state can be represented up to global phase as

$$\frac{1}{\sqrt{|V|}} \sum_{x \in V} i^{\ell(x)} (-1)^{q(x)} |x\rangle,$$

where V is an affine subspace of \mathbb{F}_2^n , $\ell(x)$ is a linear binary function on n bits, and $q(x)$ is a quadratic binary function on n bits. Let $(V, \ell(x), q(x))$ be the corresponding triple for $|\psi\rangle$. Without loss of generality let the first non-zero amplitudes in $|\psi\rangle$ and $|\varphi\rangle$ be positive real numbers. The linear dependence of the state vectors in \mathcal{S} is equivalent to the existence of $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ such that

$$\frac{1}{\sqrt{|V|}} |0\rangle^{\otimes n} + \alpha |\psi\rangle = \beta |\varphi\rangle.$$

Note that $|V|$ is a power of 2. If $|V|=1$, $|\psi\rangle$ is a non-zero computational basis state. Since the non-zero amplitudes in stabilizer states differ from each other by powers of i , α must be a power of i , $\alpha|\psi\rangle$ and $|0^n\rangle$ are Pauli related, and $|\varphi\rangle = \frac{|0^n\rangle + \alpha|\psi\rangle}{\sqrt{2}}$.

From now on assume $|V| > 1$. Then $0^n \in V$ or else $|\varphi\rangle$ would have $|V|+1 \neq 2^m$ non-zero amplitudes and could not be a stabilizer state. Also note the support set of $|\varphi\rangle$ is either V or $V \setminus \{0^n\}$, and $|V|-1 \neq 2^m \quad \forall m \geq 2$. Therefore, the only case when the support set of $|\varphi\rangle$ is $V \setminus \{0^n\}$ is if $|V|=2$ and $\alpha = -1$, in which case $|\varphi\rangle$ is a computational basis state, related by a Pauli operator to $|0\rangle^{\otimes n}$.

From now on the support set of $|\varphi\rangle$ is V . Then, $\beta = 1 + \alpha$ and by comparing non-zero amplitudes of the left and right hand sides, $\frac{\alpha}{1+\alpha} = i^k$ for some $k \in \{1, 2, 3\}$.

Claim 3.5.4. *If $|V| \geq 8$ and $k = 2$, it is not possible for $|\varphi\rangle$ to be a stabilizer state.*

Proof. Suppose $|\varphi\rangle$ was a stabilizer state. We consider the stabilizer state $|\phi\rangle$ with support set V and quadratic and linear functions equal to the difference of the quadratic and linear functions of $|\varphi\rangle$ and $|\psi\rangle$. The un-normalized amplitudes of $|\phi\rangle$ are equal to the ratios of the amplitudes of $|\varphi\rangle$ and $|\psi\rangle$, which are i^k for all non-zero computational basis states and 1 for $|0^n\rangle$. We use the following proposition to derive a contradiction.

If we write $|\phi\rangle = C|0^n\rangle$ for some Clifford operator C . Then, for some Pauli operator P' , $\langle\phi|P|\phi\rangle = \langle 0^n|C^\dagger P C|0^n\rangle = \langle 0^n|P'|0^n\rangle \in \{0, 1, i, -1, -i\}$.

That $0^n \in V$ implies V is a subspace of \mathbb{F}_2^n . Let $e := e_1 e_2 \dots e_n$ be a basis vector of V . Let $P := \bigotimes_{i=1}^n X_i^{e_i}$. Then $P|\phi\rangle = \frac{1}{\sqrt{|V|}} \left(|e\rangle - \sum_{x \in V \setminus \{e\}} |x\rangle \right)$, so $\langle\phi|P|\phi\rangle = \frac{|V|-4}{|V|} \notin \{0, 1, i, -1, -i\}$, which is impossible. This completes the proof of the claim. \square

Claim 3.5.5. *If $|V| \geq 4$ and $k \in \{1, 3\}$, it is not possible for $|\varphi\rangle$ to be a stabilizer state.*

Proof. As in Claim 3.5.4, define $|\phi\rangle$ equal to the stabilizer state whose un-normalized amplitudes are the ratios of the amplitudes of $|\varphi\rangle$ and $|\psi\rangle$, in which case $|\phi\rangle \propto |0^n\rangle \pm i \sum_{x \in V \setminus \{0^n\}} |x\rangle$.

It is known that in a stabilizer state with its first non-zero amplitude positive and real, the number of pure imaginary amplitudes must be 0 or half of the support. $|\phi\rangle$ does not satisfy this condition, which proves the claim. \square

By Claim 3.5.4 and Claim 3.5.5, the remaining cases either satisfy $|V|=2$ or $|V|=4$ and $k=2$. If $|V|=2$, then $|\psi\rangle$ and $|\varphi\rangle$ are of the form $|\psi\rangle = \frac{|0^n\rangle + i^h |s\rangle}{\sqrt{2}}$ and $|\varphi\rangle = \frac{|0^n\rangle + i^{k+h} |s\rangle}{\sqrt{2}}$ for some h and computational basis state $|s\rangle$. Also, $|0^n\rangle = -\sqrt{2}\alpha|\psi\rangle + \sqrt{2}(1+\alpha)|\varphi\rangle$. If $k=2$, then $\alpha = -\frac{1}{2}$ and $-2\alpha|\psi\rangle$ and $2(1+\alpha)|\varphi\rangle$ are Pauli-related stabilizer states such that their sum divided by $\sqrt{2}$ is $|0^n\rangle$. If $k=1$, then $\alpha = \frac{i-1}{2}$. If we express $|\psi\rangle$ in reduced form, then $n-1$ of the c_u are equal to H by Lemma 3.3.3, and we can let v be the unique index u such that $c_u \neq H$. By Proposition 3.5.8, since $\langle 0^n|\psi\rangle \neq 0$, for each $c_u = H$, we have $z_u = I$. Note that $s_v = 1$ by Lemma 3.3.7, so $S_v|\psi\rangle = |\varphi\rangle$, and we have

$$|0^n\rangle = \frac{1-i}{\sqrt{2}}|\psi\rangle + \frac{1+i}{\sqrt{2}}S_v|\psi\rangle, \quad (3.45)$$

which corresponds to Case 2. If $k=3$, then similar arguments yield the same result with the roles of $|\psi\rangle$ and $|\varphi\rangle$ swapped.

If $|V|=4$ and $k=2$, then $\alpha = -\frac{1}{2}$ and $\beta = \frac{1}{2}$. If we express $|\psi\rangle$ in reduced form, then $n-2$ of the c_i are equal to H by Lemma 3.3.3, and we can let u and v be the indices w such that $c_w \neq H$. By Proposition 3.5.8, since $\langle 0^n|\psi\rangle \neq 0$, for each $c_w = H$, we have $z_w = I$. By Lemma 3.3.7, we can write the computational basis states in $|\varphi\rangle$ and $|\psi\rangle$ as $|i\rangle_u \otimes |j\rangle_v \otimes |s_{ij}\rangle$ for $i, j \in \{0, 1\}$ and binary strings s_{ij} of length $n-2$. We compute

$$\langle i|_x \otimes \langle j|_y \otimes \langle s_{ij}| Z_x Z_y C Z_{x,y} |\psi\rangle = (-1)^{1-(1-i)(1-j)} \langle i|_x \otimes \langle j|_y \otimes \langle s_{ij}| |\psi\rangle, \quad (3.46)$$

so we have

$$|0\rangle^{\otimes n} = |\psi\rangle + Z_x Z_y C Z_{x,y} |\psi\rangle, \quad (3.47)$$

which corresponds to Case 3. \square

Example 3.5.6. We show small illustrative examples of each of the three cases in Theorem 3.5.3. Each of the stabilizer states is in canonical form with vertex 1 being the lowest node in the diagram and vertex 3 being the highest.

$$\left| \begin{array}{c} \textcircled{H} \\ \textcircled{H} \textcircled{H} \end{array} \right\rangle = \frac{1}{\sqrt{2}} \left| \begin{array}{c} \textcircled{H} \\ \textcircled{I} \textcircled{H} \end{array} \right\rangle + \frac{1}{\sqrt{2}} \left| \begin{array}{c} \textcircled{H} \\ \textcircled{Z} \textcircled{H} \end{array} \right\rangle \quad (3.48)$$

$$\left| \begin{array}{c} \textcircled{H} \\ \textcircled{H} \textcircled{H} \end{array} \right\rangle = \frac{1-i}{\sqrt{2}} \left| \begin{array}{c} \textcircled{I} \\ \textcircled{H} \textcircled{H} \end{array} \right\rangle + \frac{1+i}{\sqrt{2}} \left| \begin{array}{c} \textcircled{S} \\ \textcircled{H} \textcircled{H} \end{array} \right\rangle \quad (3.49)$$

$$\left| \begin{array}{c} \textcircled{H} \\ \textcircled{H} \textcircled{H} \end{array} \right\rangle = \left| \begin{array}{c} \textcircled{I} \\ \textcircled{H} \textcircled{I} \end{array} \right\rangle + \left| \begin{array}{c} \textcircled{Z} \\ \textcircled{H} \textcircled{Z} \end{array} \right\rangle \quad (3.50)$$

We take a closer look at Case 2 and Case 3 of Theorem 3.5.3 by considering inner products, revealing the symmetries in non-Pauli-related triplets of linearly dependent stabilizer states.

Theorem 3.5.7. *If two stabilizer states $|\psi_1\rangle$ and $|\psi_2\rangle$ satisfy $\langle\psi_1|\psi_2\rangle \in \{\frac{i-1}{2}, -\frac{1}{2}\}$, then $|\psi_3\rangle$, defined as $|\psi_3\rangle := -(|\psi_1\rangle + |\psi_2\rangle)$, is a stabilizer state and satisfies $\langle\psi_2|\psi_3\rangle = \langle\psi_3|\psi_1\rangle = \langle\psi_1|\psi_2\rangle$.*

Proof. Let $|\psi_1\rangle = C|0^n\rangle$ and $|\psi_2\rangle := C^\dagger|\psi\rangle$ for some Clifford operator C . If $\langle 0^n|\psi\rangle = \frac{i-1}{2}$, then $|\psi\rangle$ is of the form $\frac{i-1}{2}|0^n\rangle + i^k\frac{i-1}{2}|s\rangle$ for some non-zero computational basis state $|s\rangle$ and integer k . Then, $|\psi_3\rangle$, which is equal to $C(-\frac{i+1}{2}|0^n\rangle - i^k\frac{i-1}{2}|s\rangle)$, is a stabilizer state and satisfies $\langle\psi_2|\psi_3\rangle = \langle\psi_3|\psi_1\rangle = \frac{i-1}{2}$. Likewise, if $\langle 0^n|\psi\rangle = -\frac{1}{2}$, then $|\psi\rangle$ is of the form $-\frac{1}{2}(|0^n\rangle + i^{k_1}|s_1\rangle + i^{k_2}|s_2\rangle + i^{k_3}|s_3\rangle)$ for some distinct computational basis states $|s_1\rangle, |s_2\rangle, |s_3\rangle$ and some integers k_1, k_2, k_3 , so $|\psi_3\rangle$ similarly is a stabilizer state and satisfies $\langle\psi_2|\psi_3\rangle = \langle\psi_3|\psi_1\rangle = -\frac{1}{2}$. \square

3.5.3 Inner product algorithm

We now turn our attention to computing inner products between extended graph states. Our inner product algorithm has cubic worst-case runtime, same as the current best algorithm based on generator matrices [44]. Our algorithm is more direct in implementation due to the correspondence between an extended graph state and the gates required to produce it and is also naturally global phase sensitive. Our algorithm uses the following observation.

Proposition 3.5.8. *Let $|\psi\rangle := \left(\bigotimes_{i=v}^n c_v z_v\right) |G\rangle$ be in reduced form, and let $A := \{v|c_v = H\}$.*

Then

$$\langle 0|^{\otimes n} |\psi\rangle = \begin{cases} 0 & \text{if } \exists v \in A, z_v = Z \\ \frac{1}{\sqrt{2^{n-|A|}}} & \text{otherwise} \end{cases}. \quad (3.51)$$

Proof. Note that

$$\langle 0|^{\otimes n} \left(\bigotimes_{v=1}^n c_v z_v\right) |G\rangle = \langle 0|^{\otimes n} \left(\prod_{v \in A} H_v(z_v)_v\right) |+\rangle^{\otimes n} = \frac{\langle 0|_A \left(\prod_{v \in A} (x_v)_v\right) |0\rangle^{\otimes n}}{\sqrt{2^{n-|A|}}}, \quad (3.52)$$

where $x_v = X$ when $z_v = Z$ and $x_v = I$ when $z_v = I$. If $x_v = X$ for some $v \in A$, then $\langle 0 |^{\otimes n} |\psi\rangle = 0$ and otherwise $\langle 0 |^{\otimes n} |\psi\rangle = \frac{1}{\sqrt{2^{n-|A|}}}$. \square

We present our algorithm in the proof of the following theorem.

Theorem 3.5.9. *Let $|\psi\rangle := \left(\bigotimes_{v=1}^n C_v\right) |G\rangle$ and $|\psi'\rangle := \left(\bigotimes_{v=1}^n C'_v\right) |G'\rangle$ be two extended graph states. Then $\langle \psi | \psi' \rangle$ can be computed in $O(nd^2)$ time, where d is the maximum degree in G and G' encountered during the calculation.*

Proof. First we apply C_v^\dagger to C'_v for each v . It suffices to take the inner product of $|G\rangle$ and $\left(\bigotimes_{v=1}^n D_v\right) |G'\rangle$ for local Clifford operators D_i . We do so by taking the inner product of $|0\rangle^{\otimes n}$ and $|\varphi\rangle := \langle 0 |^{\otimes n} \left(\bigotimes_{v=1}^n H_v\right) \left(\prod_{(u,v) \in E(G)} CZ_{u,v}\right) \left(\bigotimes_{v=1}^n D_v\right) |G\rangle$. We first simplify the layer of CZ operators.

Definition 3.5.10. A *star operation* on qubit v is a product of operators $CZ_{u,v}$ for various u 's.

For each $v \in [n]$, we apply star operations of the form $\prod_{u \in N(v), v < u} CZ_{u,v}$ to $\left(\bigotimes_{w=1}^n D_w\right) |G'\rangle$.

We perform updates in $O(d^2)$ time as follows. If D_v takes Z to $\pm Z$ upon conjugation, then for each neighbour u of v we apply $CZ_{u,v}$ by the method described in Section 3.4, conjugating it through D_v and D_u and either applying a normal CZ gate to G' or the appropriate operation from Table 3.1. After updating the local Clifford operations D_w and the graph G' , D_v still takes Z to $\pm Z$ upon conjugation since D_v is changed by a diagonal Clifford, so we can repeat the same update process for all qubits u in the star operation. If D_v takes Z to $\pm X$ upon conjugation, we apply Equation (3.12) to qubit v and some neighbour u of v , which changes D_v to $D_v H$. We proceed as before because D_v now takes Z to $\pm Z$ upon conjugation. If qubit v does not have a neighbour, then the application of the X operator to qubit v does not change $|G'\rangle$, so applying $CZ_{u,v}$ becomes equivalent to applying some Pauli operator on qubit u , which can be done in constant time. If D_v takes Z to $\pm Y$ upon conjugation, then we apply Equation (3.11) to qubit v , which changes D_v to $D_v H S^\dagger H$. We proceed as in the first case since D_v takes Z to $\pm Z$.

Next, we append H to D_v for all v and simplify $\left(\bigotimes_{v=1}^n D_v\right) |G'\rangle$ to reduced form, following the algorithm described in Theorem 3.3.13. The inner product $\langle \psi | \psi' \rangle$ is equal to the product of the result of Proposition 3.5.8 applied to $|\varphi\rangle$ and the global phase factors produced during the calculation. The total runtime of the algorithm is $O(nd^2)$. \square

3.6 Conclusion

In this chapter, we explored various operations on Clifford states through the lens of the graph formalism. We created a canonical form for expressing extended graph states in a concise and unique way that improves upon previous reduced forms [1, 41, 42]. We developed

efficient simplification and inner product algorithms, and the connections between stabilizer states and the properties of their corresponding graphs when expressed in canonical will be explored in later chapters.

We applied our merging formulas to discover new rules that describe the action of controlled- Z gates on arbitrary extended graph states. Our transformation rules enable us to improve the algorithm for applying controlled-Pauli operators to graph states [33, 43] and also to prove that under certain assumptions, it is impossible to update extended graph states in under quadratic time in the number of qubits upon the application of a controlled-Pauli gate. Therefore, in order to improve graph state simulation, we should consider algorithms that do not simply apply one gate at a time. Whenever multiple CZ gates can be applied consecutively, we can potentially apply star operations following the method described in the proof of Theorem 3.5.9 to spread out the $O(d^2)$ update time over multiple CZ gates, improving performance. Future work to improve graph state simulation could study the relationship between the circuit and the runtime, as well as design more efficient algorithms for simulating certain types of circuits. We discuss the simulation of quantum circuits and error-correcting codes in later chapters.

Chapter 4

Quantum Codes from Graphs

4.1 Introduction

As we saw in previous chapters, stabilizer codes are the quantum analogue of linear codes for classical computing. More precisely, a $[[n, k]]$ stabilizer code encodes k logical qubits to n physical qubits by embedding 2^k logical degrees of freedom into a subspace defined as the simultaneous $+1$ eigenspace of $n - k$ n -qubit Pauli operators, known as the stabilizers. Stabilizers comprise a considerably large class of quantum codes, including all CSS codes [46, 47].

Generally, a stabilizer code is specified by the *stabilizer tableau*, the $n - k$ Pauli operator strings which define the code space. This description is simple and elegant, and has led to remarkable results such as the Gottesman-Knill theorem [34], which efficiently simulates any Clifford operation classically, and the quantum Gilbert-Varshamov bound [1], which proves by a probabilistic technique that asymptotically good stabilizer codes exist. At the same time, the stabilizer tableau representation is prohibitive in many other ways. Without further structure, it is unclear as to how one might construct desirable codes by simply writing down a clever collection of $n - k$ Pauli strings, or how one might devise and analyze coding algorithms for a given tableau. For this reason, much of the constructive effort in quantum coding theory has relied on developing sophisticated CSS-type product operations that generate CSS codes from nice classical codes, and relying on classical algorithm analysis for inspiration [47–50].

In this chapter, we argue that a different approach based on graphs to represent stabilizer codes may also prove useful for the development and analysis of quantum codes. The employment of graphs in code construction has a rich history in coding theory. Classically, Tanner graphs, which encode a classical linear code into a bipartite graph, built the bridge between expander graphs and classical codes and significantly contributed to modern classical coding [51]. In the quantum realm, graph reasoning, specifically the topological structure of Euclidean lattices with periodic boundary conditions, motivated the development of the toric and other surface codes [52, 53]. The toric code was even shown to be efficiently decoded by way of classical graph algorithms, in particular Edmonds’ minimum weight perfect matching [54, 55]. Outside of quantum coding, tensor networks have played a key role in quantum simulation and algorithm design.

We have already seen what graphs can do to represent certain non-Clifford operations and stabilizer states. It is natural to believe that these representations can be extended to quantum circuits and codes. The critical contributions of graphs in both classical and quantum coding in many specific constructive cases naturally lead to the questions of (a) what the most general graph techniques on stabilizer codes are and (b) how useful such a representation is for a variety of important coding tasks. This graph-based approach can likely be extended for studying non-Clifford logical operations on stabilizer codes as well.

4.1.1 Contributions, scope, and conjectures

The following chapters take a first step in answering both such questions. Our first contribution, in the direction of the first question, is the development of a simple graph representation of all stabilizer codes. The general structure of the graph is known as an *encoder-respecting form*, which has the structure of a semi-bipartite graph that maps k input-representing nodes to n output-representing nodes. By semi-bipartite, we mean that inputs may not be connected but outputs generically may. Informally, our result may be stated as the following.

Theorem 4.1.1 (Informal). *Every stabilizer code is essentially uniquely represented by an encoder-respecting graph satisfying some rules, and conversely every such graph essentially uniquely represents a stabilizer code. There is an efficient compilation algorithm that maps tableaus to graphs in $O(n^3)$ time and vice versa in $O(n^2)$ time.*

The precise version of Theorem 4.1.1 is given in Section 4.2 and Section 4.4. These results establish that our graph representation is sufficiently general to universally represent all stabilizer codes. We use the compilation algorithm from tableaus to graphs in part for the study of graph properties of well-known codes. As examples, we compile the famous 5-qubit, 7-qubit, and 9-qubit quantum codes and show that each take simple geometric forms respectively of a cone, cube, and tree-star. Conversely, Theorem 4.1.1 enables us to essentially transform any semi-bipartite graph into a stabilizer code, in such a way that (a) any stabilizer code can be constructed this way and (b) the properties of the code are tied to the properties of the graph. As a consequence, we can leverage the tools of graph theory and graph algorithms to study stabilizer codes. We show that the key properties of a stabilizer code are controlled in a unified way, namely by the corresponding graph's degree.

Theorem 4.1.2 (Informal). *Let G be a graph and $C(G)$ the corresponding code. The following hold.*

- (1) *The distance of $C(G)$ is bounded above by the min-degree of G .*
- (2) *The stabilizer tableau produced by the algorithm in Theorem 4.1.1 has weights bounded by a quadratic function of the degree of certain nodes in G .*
- (3) *There exists an efficient algorithm which produces an encoding circuit for $C(G)$ whose depth is bounded by (up to a small additive constant) twice the maximum degree of G .*
- (4) *Every constant-depth diagonal gate and the \sqrt{X} can be implemented logically in $C(G)$ with a circuit of depth, respectively, about (up to an additive constant) twice the max-degree and the max-degree.*

The formal versions of these statements are given in Section 4.4.

To further strengthen the connection between graphs and codes, we next define a simple, one-player optimization-type game on a graph which we call quantum lights out (QLO), in Section 4.4. We prove that QLO unifies many important tasks in quantum coding, which opens a path towards the study of coding algorithms via their correspondence to approximately optimal QLO strategies.

Theorem 4.1.3 (Informal). *Many coding algorithms such as distance approximation, stabilizer weight reduction, and decoding are all approximately optimal strategies for QLO games.*

The above results demonstrate that graphs in many senses unify various aspects of stabilizer coding in a simple manner. Overall, we give four pieces of evidence that graphs serve as a useful representation. In the first, which we discussed above, we show that graphs enable efficient algorithms which produce encoding circuits and logical-operators whose depths and weights are controlled by the degree. Specifically, we give a procedure for transforming a graph into an encoding circuit for a code, such that the circuit’s depth is linear in the degree of the graph. Similarly, we show that the logical operators of the code have a weight linear in the graph’s degree. Later on, when we study decoding, we are able to bound the depths directly by the distance of the code for graphs which satisfy a certain property.

In the second aspect, we explore the geometric and topological properties of graphs as tools for building codes. Noticing that simple geometric solids realize celebrated quantum codes, we construct codes based on other such solids, including platonic solids and topological transformations of them. For simpler constructions, we are able to calculate the distance by direct computation. As an example, we produce a non-CSS stabilizer code from a dodecahedron, which has parameters $J16, 4, 3K$. We also construct a $J54, 6, 5K$ code by lifting the icosahedron to a covering space. For more complicated constructions, we use more indirect analytical techniques based on decoding. The main advantage of graphs as a constructive tool is their flexibility: we show that graphs enable us to more easily produce codes that have a desired numerical distance, by finding graphs which have a similar degree. Graphs also can be chosen to immediately satisfy desired experimental constraints based on locality, geometric structure, etc. Thus, the graph representation may prove helpful tools for code construction at constant-size scales fit for experimental use.

Our third avenue is decoding. In general, we believe that the graph representation serves as an excellent guide for the design of decoding algorithms. Historical evidence of minimum-weight perfect matching on the surface code suggests that graphs are indeed helpful. In this chapter, we take a first step in that direction by designing a decoder that employs a simple greedy strategy on the QLO game. We give a general condition on graphs, which we call its *sensitivity*, that sufficiently characterizes a graph’s amenity to be decoded well greedily. The sensitivity is the size of the largest intersections of vertex neighbourhoods in the graph. For concreteness, we also design a simple family of $J\frac{m2^m}{m+1}, \frac{2^m}{m+1}K$ codes, which we call the hypercube codes. Their distance is provably at most m , but we show that the decoder can correct at least $m/4$ errors on it, so that the distance is also at least $m/2$ (up to a ± 1 additive constant). We conjecture, however, that a more careful analysis can prove that the distance is actually m . Assuming this conjecture, a small case of the hypercube code family is $J112, 16, 7K$. Moreover, our results imply a lower bound on the distance in terms of

the degree, which in turn lead to bounds on encoding circuit depth, logical operator circuit depth, and stabilizer weight entirely in terms of distance.

Theorem 4.1.4 (Informal). *Many coding algorithms such as distance approximation, stabilizer weight reduction, and decoding are all approximately optimal strategies for QLO games.*

Theorem 4.1.5 (Informal). *If the graph of a code on n qubits has degree d vertices whose neighbourhoods share at most B vertices, there exists efficient greedy decoder as a QLO game instance that will correct at least $\frac{d}{2B}$ errors, putting a lower bound on the code's distance.*

Finally, we exploit the structure of graphs to give a more fine-grained argument about random codes. By randomly connecting edges of our graphs, we give a large class of codes for which almost all members satisfy a trade-off between rate, distance, and stabilizer weight. This extends the result of the quantum Gilbert-Varshamov bound, which shows by a coarse-grained probabilistic stabilizer tableau analysis a similar result with a rate-distance trade-off but always large stabilizer weight. Such a result further exemplifies that graphs enable greater flexibility in code analysis.

Theorem 4.1.6 (Informal). *There exists a large family of random graphs which form codes on n qubits with rate R , distance d and stabilizer weight no greater than $4Rd^2 \log^2 n$. This is an extension over the quantum Gilbert-Varshamov bound for arbitrary random codes, which have linear stabilizer weight.*

We present our results at a very general scope, namely at the level of all stabilizer codes. The universality of these results therefore has limitations that do not exist for highly specific quantum low-density parity check (qLDPC) constructions. In particular, even when optimized as much as possible with known techniques, code properties such as check weight, encoding circuit depth, and logical operator circuit depth, will scale with the degree and therefore the code parameters, though not necessarily by a great deal (logarithmic, for example). Thus, our intention is not to use the graph representation as a means for continued study into asymptotically good qLDPC codes with very large constants [56–59]. Rather, we consider our results to be complementary to qLDPC in the sense that we give general insight into stabilizer codes and new flexible ways to construct codes that may be tailored specifically for a given experimental implementation. As an example, a future quantum long-term memory device may seek a particular large numerical distance threshold but care little for comparably large check weights if the measurement error is sufficiently small. This philosophy underpins our explicit construction of codes which have desirable properties at small scales. We believe also that further applications of graph theoretical techniques may further improve the techniques used this chapter to build increasingly practical recipes for code constructions that flexibly adapt to experimental constraints.

More generally, we argue that graph theory provides a promising path forward *generally* across avenues of quantum coding theory. Recent breakthroughs in qLDPC codes, for example, have relied on graphs in their construction to generalize the use of surface code lattices [53]. Perhaps further generalizations of these specific types of constructive techniques, as well as less universal but more fine-grained (i.e. finding certain graph constructions which map to codes in such a way that some properties scale favourably or not at all with parameters) refinements of the universal graph representation will lead to new constructions of and insights

into quantum codes. Additionally, the ability to perform logical non-Clifford operations is of great interest when trying to perform universal, fault-tolerant quantum computation. Future work can also adapt techniques from Chapter 2 to study the effects of both logical and physical non-Clifford gates on codes by using linear combinations of graphs.

4.1.2 Related work

Graph forms have been exploited in many ways in the quantum computation literature, most generally via tensor network representations. One simple case of a graph representation is a graph state. In Chapter 3, we discussed a generalized graph state representation of stabilizer *states*, i.e. a stabilizer code with 0 logical qubits. Our reduction from tableau to graph utilizes insights from Chapter 3, and in the special case of codes with no inputs we find a transformation that reduces our tableau-to-graph map to the canonical form from Chapter 3. We remark that McElvanney and Backens [60], building upon results from Chapter 3 which were published previously, derived a different unique canonical form for stabilizer states that are particularly convenient for measurement-based quantum computation. Independently, Yu, Chen, and Oh [61] also utilized graph theory in quantum coding, albeit at a much more general level (including non-stabilizer codes) for constructive and classification purposes.

Parts of this chapter, particularly the reduction from stabilizer tableaus to graphs shown in Section 4.2, use rules and notation from the ZX-calculus. The ZX-calculus is a graphical language used for expressing quantum operations in a fundamental way. It represents quantum states, circuits, codes, and operations as tensor networks containing just two types of tensors. The ZX-calculus is imbued with a handful of rewrite rules which are useful for manipulating such diagrams. An introduction to the ZX-calculus and a list of rewrite rules is included in Appendix C.

Recent works have also explored the use of the ZX-calculus to diagrammatically express quantum codes. A recent paper of Kissinger [62] also constructs diagrammatic forms for *CSS codes* specifically. The ZX normal forms used in that work are substantially different from ours and serve a different purpose. Primarily, they are used to establish a correspondence between CSS codes and ZX diagrams by non-uniquely mapping CSS codes to such diagrams and mapping *phase-free* ZX diagrams to CSS codes. The tableau-to-graph map in Section 4.2 extends the conceptual idea of diagrammatic forms inspired by the ZX-calculus to all stabilizer codes, but takes a significantly different approach and utilizes the result for constructive and algorithmic purposes. We will examine extensions of our results with a focus on CSS codes in a subsequent chapter.

More generally, ZX-calculus approaches to quantum error correction have been considered in various ways. Two relatively recent works which use the ZX-calculus exemplify these different approaches. In the first, Wu, Cheng, and Zeng [63] represent specifically graph codes with ZX-calculus diagrams. This approach, while not general to stabilizer or CSS codes, has shown promise in code analysis. The second, due to Chancellor *et al.* [64], uses the ZX-calculus specifically to quantize classical codes in the spirit of CSS code construction. Both of these works give evidence that graphs enable new insights into quantum coding, both in their construction and analysis, and thus motivate our completely general theory of graph representations. Moreover, aside from our tableau-to-graph reduction algorithm which does use elements of the ZX-calculus, our results build everything from just the standard

definition of graphs. We emphasize that the graphical diagrams of the ZX-calculus require additional structure. Therefore, graph representations further simplify related previous works that also devise similar representations based on the ZX-calculus. The specific motivations, applications, and analysis in such works are also distinct from those pertinent to our results.

4.2 From tableaux to graphs

We begin by constructing the general graph form for a code and compiling any stabilizer tableau into such a graph. More precisely, we will compile an equivalence class of encoding Clifford circuits corresponding to an equivalence class of stabilizer tableaux, and at the end of this section we discuss how to compile starting with a tableau [19]. As a starting point, we appeal to the ZX-calculus, a graph language for vectors that has become of great interest in quantum information research [62, 65–69]. The ZX-calculus produces visual diagrams that represent quantum states, circuits, and more. As with any formal logical system, the ZX-calculus has a set of rules which may be iteratively applied to transform diagrams into equivalent diagrams. These rules are representations of identities in quantum circuits. The ZX-calculus has become of more interest than ever in fault tolerant quantum computation and quantum compiler theory because it can explicitly visualize quantum properties such as entanglement in an intuitive manner. It has recently been applied to a host of quantum computation problems, including lattice surgery [70] and quantum optimization [71]. Importantly, the ZX-calculus is, for stabilizer tableaux, complete (equalities of tableaux can be derived from corresponding ZX diagrams), sound (vice versa), and universal (every quantum operation can be expressed in the ZX-calculus) [65, 72].

We are consequently motivated to leverage the ZX-calculus as an intermediate step in the development of a graph representation. Ultimately, our graphs will be simple graphs and not the more complicated and structured diagrams in the ZX-calculus. The diagrams that we map our circuits into are a subset of ZX diagrams that are equivalent by a simple transformation to graphs. To more clearly elucidate the transformation from tableau to graph, we construct the map from a composition of simpler maps. In particular, we first convert the tableau into a circuit. Next we show that up to an equivalence relation, we can efficiently biject the circuits into a class of ZX diagrams of a certain form that satisfies four rules. We thus denote these diagrams *ZX canonical forms* (ZXCFs). Lastly, we remove unnecessary structure from ZXCFs to obtain a graph representation of the code. This is pictorially represented by the following maps.

$$\text{Tableau} \longleftrightarrow \text{Encoder} \longleftrightarrow \text{ZXCF} \xleftrightarrow{\text{LE}} \text{Graph}. \quad (4.1)$$

In absence of the last step, everything is completely invertible and has an interpretation as a unique compiler. For the last step, the map between ZXCFs and graphs is invertible modulo *local equivalence*; that is, modulo local (1-qubit) Clifford operations on the outputs. An immediate consequence for this ZXCF compiler is a diagrammatic method of testing equality between stabilizer codes.

We begin the formalism by noting that properties of a code depend only on the codespace, and thus there is a unitary degree of freedom on the logical space. In particular, encoding

circuits for a given stabilizer tableau will produce the same stabilizer code if and only if they differ by an image. We therefore make the following definition.

Definition 4.2.1. Two circuits are equivalent as *Clifford encoders* if they have the same image over all possible input states. Equivalently, \mathcal{C}_1 and \mathcal{C}_2 are equivalent encoders if there exists a unitary U acting on the inputs of the circuit such that $\mathcal{C}_1 = \mathcal{C}_2 U$ or $\mathcal{C}_2 = \mathcal{C}_1 U$.

Any reference we make to encoding circuits will either implicitly or explicitly refer to them up to this equivalence, and indeed they all map to the same stabilizer code.

4.2.1 ZX canonical form construction

In the intermediate steps using ZX-calculus rules, we follow the standard notation of ZX-calculus graph diagrammatics, specified by Backens [72]. An introduction to the ZX-calculus, its notations, key definitions, and rewrite rules is included in Appendix C.

A ZX diagram is a graph with additional structure. In particular, nodes may be either red or green, nodes may be decorated with local Clifford operators, and edges may be Hadamarded. Additionally, nodes may have a “free edge”, an edge connected only to one node and dangling on the other side. Green nodes are associated with Z operators, and red with X . Each node may be associated with a local Clifford operator (which may be expressed as a phase which is a multiple of $\pi/2$), and each edge may have a Hadamard gate on it. We colour an edge blue if it has a Hadamard gate on it [73] (alternatively, we can instead use an edge with a yellow box, such as in [72]). The circuit takes k input qubits to n output qubits, for $k \leq n$.

The specific structure of our graphs will be those in the following form.

Definition 4.2.2. An *encoder-respecting form* \mathcal{D} has only Z (green) nodes and is structured as a *semi-bipartite graph*. A semi-bipartite graph has a left and right cluster, such that left-cluster nodes may have edges only to right-cluster nodes, but right-cluster nodes have no such restrictions. In our case, the left and right cluster are denoted as the input and output clusters, respectively. The input cluster \mathcal{I} has k nodes associated with the k input qubits of the corresponding encoder, and the output cluster $\tilde{\mathcal{O}}$ has n nodes. Each input node has a free (not connected to any other nodes) edge, the input edge. Similarly, each output node also has a free output edge. The output edges are numbered from 1 to n , in order from left to right on a stabilizer tableau or top to bottom on Clifford circuit output wires. For convenience, we refer to the node connected to an output edge numbered v as the output node or qubit numbered v .

The design of the encoder-respecting form graphically illustrates how information propagates from input to output (which edges connect \mathcal{I} to $\tilde{\mathcal{O}}$) as well as the entanglement structure (which edges connect $\tilde{\mathcal{O}}$ to $\tilde{\mathcal{O}}$) of the underlying encoder. We emphasize that this idea is only for intuition, as there exists equivalence transformation rules on ZX diagrams that appear to change the connectivity in nontrivial ways but nonetheless represent the same tensor. Note that the structure of \mathcal{D} gives rise to a natural binary “partial adjacency matrix” $M_{\mathcal{D}}$ of size $k \times n$, which describes the edges between \mathcal{I} and $\tilde{\mathcal{O}}$ akin to the standard graph adjacency matrix.

Although this structure appears intuitively appealing, it is insufficient because there exists several equivalence transformations in the ZX-calculus that yield an equivalent (but not obviously so) diagram. We therefore constrain an encoder-respecting form into a ZX canonical form (ZXCF) via four additional rules. For notational convenience, we will interchangeably refer to applying an operation on a node's free edge as applying an operation on the node.

Definition 4.2.3. A ZX diagram in encoder-respecting form said to be in *ZX canonical form (ZXCF)* if it satisfies the following rules.

- (1) *Edge Rule:* The ZXCF must have exactly one Z -node per free edge and every internal edge must have a Hadamard on it.
- (2) *Hadamard Rule:* No output node v may both have a Hadamard gate on its output edge and have edges connecting v to lower-numbered nodes or input nodes.
- (3) *RREF Rule:* $M_{\mathcal{D}}$ must be a full rank matrix in reduced row-echelon form (RREF).
- (4) *Clifford Rule:* Let $\mathcal{P} \subseteq \tilde{\mathcal{O}}$ be the nodes associated with the pivot columns of the RREF matrix $M_{\mathcal{D}}$, so that $|\mathcal{P}| = k$. The only local Cliffords allowed on nodes are the set $\{I, S, Z, SZ, H, HZ\}$, but there can only be identity operations on input and pivot nodes. There can be no input-input edges or pivot-pivot edges.

In subsequent chapters, we will also refer to diagrams in ZXCF as defined in Definition 4.2.3 as diagrams in KLS form, diagrams in KLS canonical form, or KLS diagrams. This is done to disambiguate this particular canonical form from other canonical forms constructed through the ZX-calculus.

The notion of a *pivot node* from the Clifford rule is incredibly important to the results that follow.

Definition 4.2.4. For any code or diagram in ZXCF, or more generally obeying the RREF rule, we define the *pivot nodes* of the diagram as follows. The adjacencies between the input and output nodes determine the $k \times n$ matrix $M_{\mathcal{D}}$, where the inputs correspond to rows of $M_{\mathcal{D}}$ and outputs correspond to columns. Since $M_{\mathcal{D}}$ is in RREF, k of its columns are the *pivot columns*, meaning they each contain exactly one non-zero entry and that entry is the first non-zero entry in its row. Each row is thus associated with a pivot column. This gives a bijection between inputs and a special subset of k outputs. We call these output nodes *pivot nodes* and make frequent use of their properties that each is connected to a distinct unique input node.

We have elected for emphasis to include the constraints on only using Z -nodes and not using input-input edges constraint in the Edge and Clifford rules, respectively, even though these are redundant with the constraints of the encoder-respecting form.

To provide some visual intuition on these 4 rules, Figure 4.1 depicts a generic example of some possible violations to the rules. We define the four rules such that the ZXCF is as homogeneous as possible in its node type (Z or X) and generically prefers not including edges where possible. It can be shown that each of these rules corresponds to certain equivalence transformations [72, 74]. For example, row operations on $M_{\mathcal{D}}$ correspond to

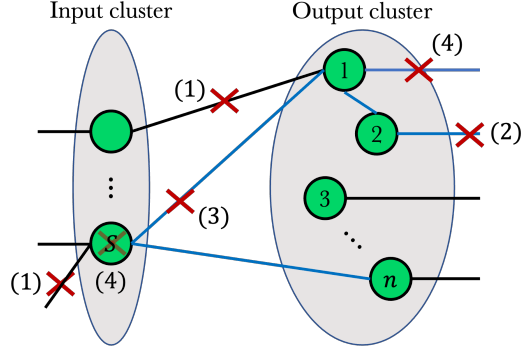


Figure 4.1: Example of an encoder-respecting form and some ways it might violate the 4 rules. The violations are as follows. Rule (1): an internal edge does not have a Hadamard gate on it and a node does not have exactly one free edge. Rule (2): a free edge with a Hadamard gate is connected to a lower-numbered node or output node. Rule (3): the partial adjacency matrix $M_{\mathcal{D}}$ is not in RREF. Rule (4): there is a non-identity local operation on a pivot node and on an input node.

unitary controlled- X operations on the input qubits. To show the uniqueness of the ZXCF, we devise a map from an encoder to a ZXCF and prove that such a map is efficient and bijective.

Theorem 4.2.5. *Any Clifford encoder has a unique equivalent ZXCF satisfying the Edge, Hadamard, RREF, and Clifford rules. There exists an algorithm, running in worst-case $O(n^3)$ time, that on an input of a description of a Clifford encoder outputs the corresponding ZXCF. This map is bijective.*

We briefly sketch the proof idea of Theorem 4.2.5 but defer the details to Appendix D. The proof involves a series of transformations via ZX equivalence rules.

Proof Sketch. In the first step, we apply an isomorphism between circuits and states, and proceed to apply the result of Theorem 3.3.4 to preliminarily represent the circuit as the ZX diagram of a corresponding state. We then transform the diagram into one representing a circuit, and carefully choose a series of equivalence transformations that iteratively force the diagram to satisfy a rule above without at the same time violating a different rule that has previously been satisfied. The resulting product is precisely a ZXCF.

In fact, since the steps are equivalence transformations, distinct encoders map to distinct ZXCFs. The only remaining aspect of the proof of Theorem 4.2.5 is whether this one-to-one map is bijective. We prove this claim in Section 4.2.3.

4.2.2 Tableau to encoder

There are numerous algorithms for mapping a stabilizer tableau into a Clifford encoding circuit [1]. If we quotient out operations which leave the code space invariant, then any such map is also bijective. We describe one such algorithm, which can be summarized as follows. For a $(n - k) \times n$ stabilizer tableau, we begin by drawing n output wires. At each step,

we first simplify the tableau by applying a Clifford operation and then measure out one of the qubits to remove one row and column from the tableau. Repeating inductively yields a Clifford circuit that takes k qubits to n qubits.

To build an encoding circuit from a tableau, we apply the following sequence of operations. We start with a circuit containing n wires. We then apply the following procedure $n - k$ times, as many times as there are generators in the stabilizer tableau.

We consider a generator in our tableau, g . Let v be the index of a non-identity Pauli in g . We find any Clifford operation C such that $gC = CZ_v$. Such an operation can be built up as follows.

We start with a candidate $C' = I$ and repeatedly evaluate $P = C'gC'^{\dagger}$ until P becomes Z_1 . If P_v is equal to Y , we left-multiply C' by S_v to turn the Y into an X , transforming $C' \rightarrow S_v C'$. If P_v is now equal to X , we multiply C' by H_v to turn the X into a Z . We do the same for all other non-identity terms in P . If the sign of P is negative, we multiply C' by X to correct the sign. For each Z remaining in P at position $u \neq v$, we multiply C' by $CX_{u,v}$, which turns the Z_u into the identity in P . What remains now is $P = Z_v$. Now our candidate C' is a valid choice for C . We apply the operation C to our wires. Lastly, we apply the post-selected measurement $\langle 0|$ on qubit v , capping it off. Now, there are 1 fewer wires in our diagram and we can ignore the column of the stabilizer tableau corresponding to v . We can also ignore the generator g . Effectively, our tableau's height and width both shrank by 1 and we reindex our rows and columns to match our remaining wires.

After applying the above subroutine $n - k$ times, our tableau has 0 rows in it and we have k wires remaining. At this point, we simply read our circuit in the reverse direction. The k remaining wires become k input wires and the n original input wires become outputs. Any post-selected measurement $\langle 0|$ now becomes $|0\rangle$, an initialization of a work qubit. Any operation C applied to our wires becomes C^{\dagger} when applied backwards. Since the only post-selected states allowed by the circuit we built were those stabilized our tableau, all states produced by this encoder must be as well.

Going backwards from an encoder to a stabilizer tableau is much simpler. Every time an ancilla qubit v is initialized in the $|0\rangle$ state, this adds a stabilizer generator of the form Z_v . Every time a Clifford operation U is applied in the encoder, all existing generators are conjugated by U , with generator g turning into UgU^{\dagger} .

4.2.3 Proof of canonicity

We next prove that our proposed ZXCF is indeed canonical. In other words, two equivalent stabilizer tableaus, generators of the same subspace of the n -qubit Hilbert space, will map to the same ZXCF. We proceed by counting the number of stabilizer tableaus and ZXCFs. For notational convenience, we will let m be the number of rows of the stabilizer tableau, so $m = n - k$.

Claim 4.2.6. *The number of stabilizer tableaus with m stabilizers on n qubits is*

$$\frac{\prod_{i=1}^m (2 \cdot 4^n / 2^{i-1} - 2 \cdot 2^{i-1})}{\prod_{i=1}^m (2^m - 2^{i-1})} = \prod_{i=1}^m \frac{2^{2n-i+2} - 2^i}{2^m - 2^{i-1}}. \quad (4.2)$$

Proof. For each row i , there are $2 \cdot 4^n$ possible Pauli strings (including the sign) for that row's stabilizer, but the requirement that they commute with previous rows divides the count by 2^{i-1} . Of these $2 \cdot 4^n / 2^{i-1}$ valid strings, 2^{i-1} strings are linear combinations of previous strings. Another 2^{i-1} strings are exactly the negation of a linear combination of previous strings.

We have overcounted, however, since there are many ways to find a set of stabilizer generators for a particular tableau. In particular, when choosing a set of generators for a Clifford encoder, we have $2^m - 1$ choices for the first generator (subtracting the identity). There are then $2^m - 2$ ways of choosing the next element, as we cannot pick anything in the span of the elements chosen so far. This product counts the multiplicity by which we have overcounted the number of ways to represent each encoder. Repeating inductively gives the denominator above. \square

Next, the number of ZXCF diagrams with k inputs and n outputs can be expressed by the following fourfold recursive function f evaluated at $p = o = 0$, where we still have $m = n - k$.

$$f(n, m, p, o) = \begin{cases} 1 & \text{if } n = m = 0 \\ A_{n,m,p,o} + B_{n,m,p,o} & \text{else} \end{cases} \quad (4.3)$$

where we have

$$A_{n,m,p,o} = \begin{cases} 0 & \text{if } n = m \\ 2^o f(n-1, m, p+1, o) & \text{else} \end{cases} \quad (4.4)$$

$$B_{n,m,p,o} = \begin{cases} 0 & \text{if } m = 0 \\ (2^{2p+o+2} + 2)f(n-1, m-1, p, o+1) & \text{else} \end{cases}. \quad (4.5)$$

This function is computed with a base case of an empty tableau when $n = m = 0$. Derivation of this function is left to Appendix E. We solve for an explicit form to obtain

$$f(n, m, p, o) = 2^{o(n-m)} \prod_{i=1}^m \frac{(2^{n+1} - 2^i)(2^{n-i+1+2p+o} + 1)}{2^m - 2^{i-1}}. \quad (4.6)$$

It can be verified by induction that f satisfies the conditions of Equation (4.3) and that $f(n, m, 0, 0)$ gives the same expression as in Equation (4.2), proving that the ZXCF is indeed canonical.

4.2.4 ZXCF to graph

In the final step, we reduce a ZXCF directly to a graph. We remark that any local Clifford operation must, by the Clifford rule, be placed only on non-pivot output nodes. However, local Cliffords do not change the weights of the set of correctable errors. Thus, local Cliffords do not change the code distance or any other code parameters. If we also quotient out this equivalence, we may remove all local Cliffords entirely. Since all internal edges have Hadamards, we can remove those as well and simply remember that they exist for inversion. Similarly, we can remove all free edges. The remaining diagram is identical to a graph, specified entirely by a collection of nodes and edges. As a consequence, we have completed the map sequence from Equation (4.1), except for the graph to ZXCF map. We have also thus proved the following theorem.

Theorem 4.2.7. *For any stabilizer code, there exists at least one equivalent code that has a representation as a semi-bipartite graph with no local Clifford operations.*

A well-studied family of stabilizer codes are the CSS codes, which can be formed by using two classical codes obeying certain orthogonality properties. CSS codes are named after Calderbank, Shor, and Steane [46, 47].

Definition 4.2.8. A CSS code is a stabilizer code which can be expressed as a set of stabilizer generators S obeying the following property. There exists a way to partition S into two sets, S_X and S_Z such that the only non-identity Pauli matrices in each set of generators are X and Z , respectively. The S_X measurements detect Z errors and vice versa. CSS codes generally make decoding a code easier as the decoding of X and Z errors can be done completely independently.

From experimental testing we can make the following observation.

Theorem 4.2.9. *Bipartite graph correspond to CSS codes. Specifically, the graph of any CSS code will be bipartite and any bipartite graph can be turned into a CSS code.*

We prove this theorem fully in the next chapter, which focuses more heavily on CSS codes.

Proof Sketch. We sketch the proof of one of the directions of the theorem. If a graph is bipartite, its vertices can be split into two sets, V_1 and V_2 . The graph is invariant under the operation of applying an X operation to a node v and Z operations to all of v 's neighbours. If we apply Hadamard gates to V_1 , producing a locally equivalent code, then for all vertices $v \in V_1$ or $v \in V_2$, the invariants will only contain Z or X operations, respectively.

4.3 Application to quantum codes

It is illuminating to observe the graph representation of well-known quantum codes. Not only does it inform of geometric structure embedded in the code, but it also provides a guide as to how such codes may be generalized. We provide three examples for study. Consider first the nine-qubit code, due to Shor [18], which uses 9 physical qubits to encode 1 logical qubit. The Shor code may be represented by the stabilizer tableau

$$\begin{bmatrix} Z & Z & I & I & I & I & I & I & I \\ Z & I & Z & I & I & I & I & I & I \\ I & I & I & Z & Z & I & I & I & I \\ I & I & I & Z & I & Z & I & I & I \\ I & I & I & I & I & I & Z & Z & I \\ I & I & I & I & I & I & Z & I & Z \\ X & X & X & X & X & X & I & I & I \\ X & X & X & I & I & I & X & X & X \end{bmatrix}. \tag{4.7}$$

In Figure 4.2, we give the graph representation in (a) and the ZXCF in (b). In the ZXCF, the input node is denoted by \mathbf{I} and free edges are dashed for emphasis. In the graph representation, the input node is blue and the outputs are black. Let us first examine the ZXCF. There are

three identical sectors of the outputs, two with Hadamarded outputs and one without. This resembles our expectations from examination of the unnormalized qubit representation of the Shor code, $(|000\rangle \pm |111\rangle)^{\otimes 3}$. The graph, on the other hand, is a star-shaped tree. It is easy to imagine how one might extend the Shor code into an infinite family of graphs, namely by applying several iterations of recursively giving every outer (leaf) node several child nodes.

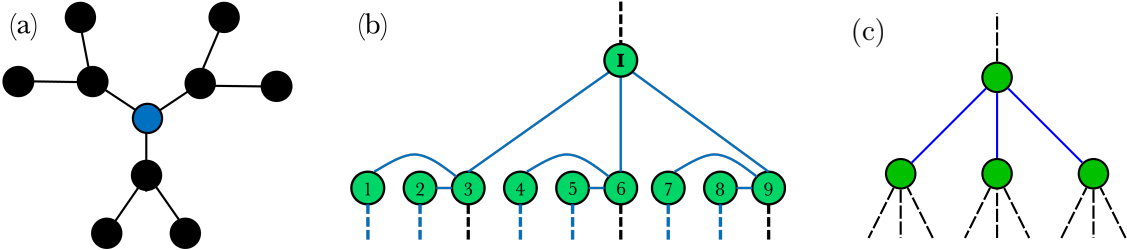


Figure 4.2: (a) Graph representation and (b) ZXCF of the 9-qubit code. The input in the graph is shown in blue. Note that the graph encoder uses a slightly different basis as since its output edges do not contain Hadamard gates. (c) A simpler representation of the 9-qubit code, formed by applying the identity removal and Hadamard cancellation rules from Definition C.1.

Next, we compile Steane’s seven-qubit code, a central construction in many fault tolerant quantum computation schemes [46]. The code is represented by the following tableau:

$$\left[\begin{array}{cccccc} I & I & I & X & X & X & X \\ I & X & X & I & I & X & X \\ X & I & X & I & X & I & X \\ I & I & I & Z & Z & Z & Z \\ I & Z & Z & I & I & Z & Z \\ Z & I & Z & I & Z & I & Z \end{array} \right]. \tag{4.8}$$

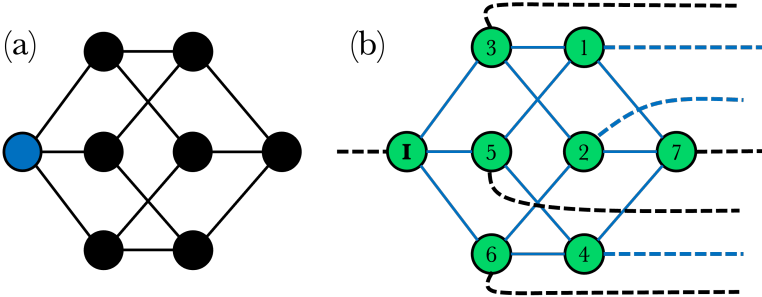


Figure 4.3: (a) Graph representation and (b) ZXCF of the 7-qubit code. The input in the graph is shown in blue. Note that the graph encoder uses a slightly different basis as since its output edges do not contain Hadamard gates.

In our ZXCF, this code takes the form given in Figure 4.3. In particular, the nodes of the diagram are simply the corners of a cube. A similar picture has been given in a different context by Duncan and Lucas [75]. Several generalizations of the Steane code come

to mind. One involves using graphs for polyhedra other than the cube and another involves constructing hypercubes of arbitrary dimension. We explore precisely such generalizations in Section 4.5.

We observe that the X and Z operations in the stabilizers of the 7-qubit code are positioned at exactly the 1-indices in the binary representation of the qubit's index. We can start to see some elegant symmetries in Figure 4.3 with the positions of the nodes and their expressions in binary.

As a final example we consider the five-qubit code, which is the smallest code one can achieve for correction of an arbitrary single-qubit error and has been studied experimentally [19, 76]. Its tableau representation is given by

$$\begin{bmatrix} X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \\ Z & X & I & X & Z \end{bmatrix}. \quad (4.9)$$

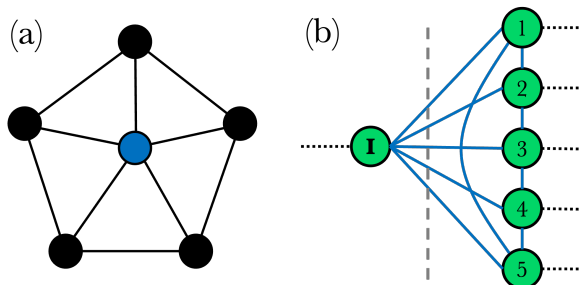


Figure 4.4: (a) Graph representation and (b) ZXCF of the 5-qubit code. The input in the graph is shown in blue.

Our construction produces the ZXCF shown in Figure 4.4. The 5-qubit code takes the shape of either a pentagon with an input in the middle or a cone, depending on how one sets up the graph. Consequently, a simple generalization of such a code would be to use a n -gon, or equivalently add more nodes to the circle in the cone.

Such elegant and simple structure in the 5, 7, and 9-qubit codes suggest that other graphs with similar elegant structure may yield interesting quantum codes, either of constant size or in family. We explore this idea in Section 4.5.

4.4 The inverse map: from graphs to stabilizer codes

The bijective relation between stabilizer codes and graphs, particularly those in the ZX canonical form, give justification that graphs are at least as powerful as stabilizer tableaus for the expression of codes. In this section, we lay the foundation for the use of graphs as *constructive tools* for code design. Such a mapping from graphs to stabilizer tableaus can be viewed as an inverse map to the algorithm given in Section 4.2.3, with some caveats relating to the fact that not all graphs can be equivalently represented by ZXCFs and therefore not all graphs can be mapped into codes.

Let G be a graph with $n + k$ nodes, partitioned into k input nodes \mathcal{I} , a choice of k pivot nodes \mathcal{P} , and $n - k$ output nodes \mathcal{O} . To ensure that our operations are well-defined, there must exist equivalence operations that map G into a ZXCF. The only nontrivial restriction this requirement poses is on the choice of pivots, whose conditions are given in Definition 4.2.4. The RREF rule ensures that every distinct pivot is connected to exactly one distinct input; in other words, \mathcal{P} and \mathcal{I} are perfectly matched.

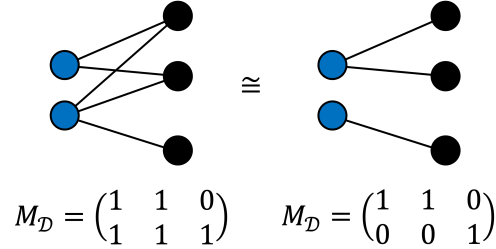


Figure 4.5: A simple example for which the third output node is necessarily a pivot. The inputs are blue and outputs are black. An example graph code is given on the left, and an equivalent graph is given on the right.

Since row operations on the partial adjacency matrix are equivalences, it suffices to choose pivots such that there exists a row-reduced partial adjacency matrix $M_{\mathcal{D}}$ for which the chosen k pivot nodes correspond to the k pivot columns of $M_{\mathcal{D}}$. A simple example of this subtlety is shown in Figure 4.5. Here, it is impossible to choose the first two outputs to be the pivots because the third output is forced to be a pivot when we row-reduce. Note, however, that this subtle restriction poses no issue if every distinct pivot we choose is already connected to exactly one distinct input (as in the case in Section 4.5.6) or if we can observe directly that the pivots we have chosen do correspond to the pivot columns after row reduction. Henceforth, we will denote G as a graph for which a set of valid pivots \mathcal{P} have been specified alongside a set of input nodes \mathcal{I} .

Assuming the choice of \mathcal{P} is valid, G will be equivalent to a ZXCF by a series of equivalence transformations. First, we place a free edge on every node and place a Hadamard on all internal edges, satisfying the edge rule. The Hadamard rule is vacuously satisfied, as we will not place any Hadamard on output nodes. We can row-reduce the partial adjacency matrix to satisfy the RREF rule. Next, we strip input-input edges, which are unitary controlled- Z operations on the inputs and thus represent equivalent encoders. Lastly, as discussed in Appendix D, there is an equivalence relation that strips pivot-pivot edges. This procedure results in a ZXCF with no local Clifford on nodes at all. While there exist encoders that can only be expressed with local Clifford operations that this map cannot produce, the map can always produce a locally equivalent encoder, and is otherwise completely general.

In practice, we never transform our graphs into a ZXCF. The only transformation we shall make is endow every node with a free edge. This endowment enables a simpler description of operator actions on the graph. However, in our diagrams we omit the free edges to reduce clutter. We can also strip input-input edges and pivot-pivot edges if desired for convenience. Aside from that, knowing that the graph is equivalent to a ZXCF, we can write down the stabilizer generators of its corresponding ZXCF directly. To do so, we first establish notation.

Let $\bigtriangleup_{i=1}^n A_i = A_1 \Delta \cdots \Delta A_n$ for sets A_1, \dots, A_n , where Δ is the symmetric difference. The symmetric difference is both commutative and associative, so this iterative procedure is well-defined.

Consider some vertex v in our graph. We define $i(v) = \{w \in \mathcal{I} \mid w \sim v\}$ the inputs connected to v and $p(v) = \{w \in \mathcal{P} \mid w \sim v\}$ the pivots connected to v , which each consist of only one vertex if v is a pivot or an input, respectively. For later use we similarly define $o(v) = \{w \in \mathcal{O} \mid w \sim v\}$, the set of non-pivot outputs connected to v . We also define $N_o(v) = \{w \in \mathcal{O} \cup \mathcal{P} \mid w \sim v\} = o(v) \cup p(v)$ the non-input neighbours of $v \in \mathcal{O}$, and more generally $N_o(A) = \bigtriangleup_{v \in A} N_o(v)$ and similarly for $i(A)$, $p(A)$, and $o(A)$. The symmetric difference is useful for correctly counting the parities of Pauli operations applied to certain nodes, i.e. if a Pauli is applied twice in the set, it is effectively not applied at all.

Let X_w be a Pauli on (the free edge of) node w , and $X_A = \bigotimes_{v \in A} X_v$. Pauli Z operators are defined analogously. Note that we may only directly apply operators to (the free edge of) *output* nodes because these are physical operators and not logical ones. With this notation, we define the following map $\mathcal{S} : G \mapsto S$ from graph to stabilizer tableau, the output of which we call the *canonical stabilizers* of the code represented by G .

$$\mathcal{S} := \{X_v Z_{N_o(v)} X_{p(i(v))} Z_{N_o(p(i(v)))}\}_{v \in \mathcal{O}}. \quad (4.10)$$

Denote each stabilizer S_v for $v \in \mathcal{O}$. (Note that we are not using local Clifford operations, so S refers to a Pauli stabilizer and not a phase gate.) These stabilizers are readily seen to be a valid generating set. There are exactly $n - k$ generators, and all are independent because only S_v contains the term X_v . Every pair of stabilizers S_u and S_v also have even X - Z overlap, and thus commute, because the graphs are undirected and if $u \in N_o(v)$, then $v \in N_o(u)$ and vice versa. In principle, one could disregard the entirety of the previous section, *define* Equation (4.10) as a map from graphs to stabilizers, and explore their properties. However, it is not immediately clear from this approach how expressive such a class of stabilizers would be and the motivation behind such an assertion would be obscure.

We next show that such a map generates precisely the stabilizer group of the encoder that the corresponding ZXCF of G represents. Since graphs do not have local Clifford operations associated to them, we can treat \mathcal{S} as the inverse map from a graph to a ZXCF, up to local equivalence. To do so, we appeal to the two most fundamental equivalence rules of the ZX-calculus, the merging/unmerging rule and the π -copy rule from Definition C.1. We will use both of these rules many times in the course of our calculations. More details on the ZX-calculus and its rules can be found in Appendix C.

Lemma 4.4.1 (ZX-calculus fundamental equivalences). *Let v be a Z -node in a ZX diagram. Operators may be placed on edges and associated with the vertex on either side of the edge.*

- (1) *If an operator placed on an internal edge (u, v) is associated with u , it can be equivalently associated with v instead. However, if the internal edge is Hadamarded, the operator is flipped $X \leftrightarrow Z$ during this change of association. An operator placed on a free edge of v is vacuously associated with v .*

- (2) If an X operator is placed on an edge associated with v , it can be equivalently commuted through v into X 's on every other edge (including the free edge) connected to v , with each new X still associated with v .
- (3) If a Z operator is placed on an edge associated to v , it may be equivalently commuted through as a Z on any one other edge associated to v , remaining associated to v .

The rules provided in Lemma 4.4.1 give a prescription for generating stabilizers. Fix $v \in \mathcal{O}$. First, place a X on the free edge of v . By rule (2), this X equivalently transforms into X on all other edges connected to v , associating with v . For edges connecting v to a non-input node u , we re-associate them by rule (1) to u , and since all internal edges are Hadamarded, these operators become Z . They commute through by rule (3) to the free edge of u and remain there as Z . We perform a similar transformation except that we do not commute the Z 's to the free edges of inputs because these correspond to operations on inputs (i.e. logical operations) rather than operations on outputs (i.e. physical operations). Instead, we commute them through canonically to the pivot associated with that input, turning the Z back into the X as we re-associate the operator with the pivot. Finally, we commute the X through the pivot. Since the X was on an internal edge between the input and pivot, a X appears on the free edge of the pivot. The remaining X 's become Z 's associated with the output neighbours of the pivot and commute through to their free edges by rule (3). To reverse all these operations and achieve the identity, thereby creating a stabilizer, we apply all these operations in reverse, precisely $X_v Z_{N_o(v)} X_{p(i(v))} Z_{N_o(p(i(v)))}$. Therefore, we have proven the following theorem.

Theorem 4.4.2 (Inversion). *Given a graph G with a feasible choice of pivots \mathcal{P} , the stabilizer tableau associated with the ZXCF equivalent to G is given by Equation (4.10).*

Note that the sets on which the X and Z operations are applied are not necessarily disjoint, so pairs of Y terms can appear if v is adjacent to both an input and its pivot. The Y operations will appear on v and on the respective pivot. As stated, the expression in Equation (4.10) is correct, but the order of the terms matters as they do not necessarily commute.

From here, we can also easily write down a canonical set of *logical* Pauli operations for a given graph, by using the same two transformation rules from above. For each input node $v \in \mathcal{I}$ corresponding to the v^{th} logical qubit, construct \overline{X}_v by placing X_v , which is by definition a logical X , on the v^{th} logical qubit. To obtain the physical operator, we commute X_v to the (free edges of the) output nodes, where X_v commutes through to become $Z_{N_o(v)}$. Hence, $\overline{X}_v = Z_{N_o(v)}$. Similarly, $\overline{Z}_v = X_p Z_{N_o(p)}$, where p is the pivot associated with v . We place an X on p to canonically define logical Z , but any neighbour of v would suffice. In this way, we have used the equivalence rules on every possible node: on \mathcal{O} , they create stabilizers; on \mathcal{I} , they create logical X 's; and on \mathcal{P} , they create logical Z 's. We have proven the following.

Theorem 4.4.3 (Logical operations). *Given a graph G , the logical operations associated with the ZXCF equivalent to G are given by the following. If v is an input vertex with a neighbour u , $\overline{X}_v = Z_{N_o(v)}$ and $\overline{Z}_v = X_u Z_{N_o(u)}$.*

As a consequence of our canonical logical operator construction, we observe that the degree of G controls the upper bound of the distance as well as the stabilizer weights of $\mathcal{S}(G)$.

Corollary 4.4.4. *The distance of the code with stabilizers $\mathcal{S}(G)$ is at most the minimum degree of any vertex in $\mathcal{I} \cup N_o(\mathcal{I})$.*

Proof. We use the logical operators from Theorem 4.4.3. For each input vertex $v \in \mathcal{I}$, $X_v = Z_{N_o(v)}$ is a logical operation. The weight of this operation is equal to the degree of v . Similarly, for each vertex $u \in N_o(\mathcal{I})$ which neighbours some input v , we have the operation $Z_u = X_v Z_{N_o(v)}$. This size of this set is equal to $|N_o(u)| + 1$, which is at most the degree of u , since u neighbours v . The construction of these logical operations proves the desired upper bound on the distance. This also shows that the statement of the corollary could be strengthened slightly by replacing the degree of input neighbours u by $|N_o(u)| + 1$. \square

Corollary 4.4.5. *Given a graph G , define*

$$\delta_{\mathcal{O}}^* = \max_{v \in \mathcal{O}} \deg(v), \quad \delta_{\mathcal{O}\mathcal{I}}^* = \max_{v \in \mathcal{O}} |i(v)|, \quad \delta_{\mathcal{P}\mathcal{O}}^* = \max_{v \in \mathcal{P}} |N_o(v)|. \quad (4.11)$$

Then $\max_{S \in \mathcal{S}(G)} |S| \leq 1 + \delta_{\mathcal{O}}^ + \delta_{\mathcal{O}\mathcal{I}}^* \delta_{\mathcal{P}\mathcal{O}}^*$, where $|S|$ is the weight of a stabilizer S . Moreover, if every path between every pair of nodes $v, w \in \mathcal{I}$ is of length at least 3, so that every node $u \in \mathcal{O}$ is connected to at most one node in \mathcal{I} , then $\max_{S \in \mathcal{S}(G)} |S| \leq \delta_{\mathcal{O}}^* + \delta_{\mathcal{P}\mathcal{O}}^*$.*

This result is a direct consequence of Equation (4.10).

In the next section, we will show that another important property, encoding depth, is also bounded above by the degree. We make two remarks regarding the utility of such degree bounds. First, for a general stabilizer code it is unclear as to how one may give a nontrivial upper bound on properties like distance and circuit depth. The degree allows us to algorithmically do so by compiling a stabilizer tableau into a graph and then examining the degree. Second, it is possible, at least in certain cases, to upper bound the degree itself by some function of the code parameters. We show bounds of this type in Section 4.5.5 and Section 4.5.6. When such a bound is possible, it provides nontrivial bounds on code properties in terms of functions of other parameters.

4.4.1 Encoding circuit with degree-bounded depth

A particularly appealing quality of the graph formalism is that it enables us to efficiently and canonically construct encoding circuits which are bounded by a small linear function of the *degree* of the graph. This construction can be taken advantage of in two ways. If we already have a stabilizer code and would like to construct a nice encoding circuit, we can compile the code's tableau into a graph and then apply the procedure below. Note that Theorem 4.4.6 assumes a graph representation, so if the ZXCF has local Cliffords, they are not included in the encoding circuit. They can be appended to the encoding circuit produced by the theorem, at the cost of increasing the depth by 1, since all local Cliffords are single-qubit operations. Alternatively, if we have a graph which represents a stabilizer code, we can directly write down this encoding circuit for the code and have a guarantee of its depth.

Theorem 4.4.6. *Suppose that one may initialize qubits to the $|+\rangle$ state. Given a graph G with maximum degree δ^* , there exists an efficient algorithm which outputs an encoding circuit \mathcal{C} for the code with stabilizers $\mathcal{S}(G)$, such that $\text{depth}(\mathcal{C}) \leq 2\delta^* + 3$.*

Proof. We construct explicitly the transformation from the graph to its encoding circuit. An informal description is as follows. A graph with $|\mathcal{I}| = k$ and $|\mathcal{O} \cup \mathcal{P}| = n$ requires a circuit taking k input and $n - k$ ancillary qubits to n output qubits. We choose to send the k inputs to the k pivots on the output side. Edges in G will generally become controlled- Z gates in the encoding circuit, with the exception of edges from \mathcal{I} to \mathcal{P} , which become a layer of Hadamards. More precisely, we construct the circuit \mathcal{C} as follows.

- (1) *Initialization.* Create n wires, one for each node in $\mathcal{O} \cup \mathcal{P}$. Label the output side of the wires by the index of the node. For each wire associated to a pivot v , label the input side of the wire by the input corresponding to v . The remaining $n - k$ wires unlabelled on the input side are the ancillary qubits. Initialize these unlabelled wires to $|+\rangle$.
- (2) *Input-output edges.* For each input $u \in \mathcal{I}$ and $v \in \mathcal{O}$, if $v \in o(u)$ then add a $CZ_{u,v}$ to the circuit. The order does not matter since all CZ gates commute.
- (3) *Input-pivot edges.* For each input $u \in \mathcal{I}$ apply H_u . These will correspond to the edges between each input and its corresponding pivot.
- (4) *Output-output edges.* For each pair of non-input vertices $u, v \in \mathcal{O} \cup \mathcal{P}$ where the edge (u, v) is in G , apply $CZ_{u,v}$.

There are two claims to show: (a) this construction correctly yields an encoding circuit for the code described by $\mathcal{S}(G)$, and (b) $\text{depth}(\mathcal{C}) \leq 2\delta^* + 3$. The first claim is a direct consequence of the rules of the ZX-calculus and the form of the ZXCF. By turning the encoding circuit into a ZX diagram and merging Z nodes together, we recover the ZXCF of the code. Examples of this transformation are shown in Section 4.5.2 and Appendix H.

Specifically, the initialization of qubits in the state $|+\rangle$ in step (1) is represented by a Z node with a single free edge in ZX-calculus. In turn, CZ gates in steps (2) and (4) are applied by a pair of Z nodes connected by a Hadamarded edge. The Hadamard gate in step (3) is applied as a Hadamard gate. Now, we simplify the ZX diagram. Every Z node along each wire initialized as $|+\rangle$ is merged into a single node. All Z nodes along each input wire are merged into two nodes, an input and a pivot, with one cluster on each side of the central Hadamard gate. The Hadamard gate on the wire between each input and its pivot now becomes exactly the Hadamarded edge we desired.

Note that the gates are ordered in this particular way because of the causal structure of the ZX diagram. First, input edges must propagate information to the output edges, so the associated input wires must have their CZ gates to establish their interaction with the ancilla wires. Next, the circuit completes the interactions from input to output via the input-pivot Hadamards. Finally, the output edges interact, so the output-output CZ gates are placed on the ancillary wires. This completes the proof of the first claim, correctness.

For the second claim, we observe that since all CZ gates commute, the depth is given by the minimum number of groupings of CZ gates which act on disjoint sets of qubits. Such a problem reduces to finding the optimal *edge colouring* of G , i.e. the minimum number of colours needed to colour every edge, such that no two edges which share a node have the same colour. Although finding the optimal edge colouring is known to be **NP**-complete, Vizing's edge colouring theorem guarantees that the minimal colouring is at most $\delta^* + 1$, and

moreover there exists an efficient algorithm which finds such a colouring [77, 78]. Thus, step (1) does not require any depth, steps (2) and (4) each has depth at most $\delta^* + 1$, and step (3) has depth 1, so the total depth is at most $2\delta^* + 3$ as claimed. \square

Although encoding in practice is often performed by a method to prepare the logical zero state, e.g. repeatedly measuring the stabilizers until they are all +1, Theorem 4.4.6 shows that for codes that have sufficiently small degree, it may be possible to have a much stronger guarantee, namely to efficiently encode any state directly via an encoding circuit.

This construction is also described in Appendix H with some minor variations as well as step-by-step illustrations for an example graph code. Additionally, Section 4.5.2 gives an example of such an encoding circuit for one of our constructed codes and discusses how the depth may actually be substantially smaller in practice by solving small cases of minimal edge colouring. Moreover, in Section 4.5.5, we will show that the degree, and thus the encoding circuit depth, can be bounded above by code parameters for certain families of codes. This result will thus directly upper bound the degree of the encoding circuit by code parameters.

4.4.2 Logical non-Pauli gates on graph codes

Earlier, we showed that the logical Pauli operations can be extracted immediately from the graph representation. Specifically, \bar{X}_v and \bar{Z}_v for $v \in \mathcal{I}$ are implemented respectively by $Z_{N_o(v)}$ and $X_{p(v)}Z_{N_o(p(v))}$. We derived these logical Paulis by placing a Pauli on the free edge of a particular input node, and then applying ZX equivalence rules to push the Pauli through the node into the output.

For a completely general logical unitary operation \bar{U} and graph code G , the only algorithm to physically implement \bar{U} is to unencode, apply U , and then re-encode. Such a technique is typically undesirable, since the encoding circuit is necessarily high-depth to achieve a good distance, which implies that the logical operation's implementation strongly propagates errors and therefore resists fault tolerance. Nonetheless, if the encoding circuit has a depth which is sufficiently small, it is conceivable that in some cases this generic procedure may be of use. Moreover, we already have a generically optimized encoding circuit from Section 4.4.1, which in turn implies the following general result.

Theorem 4.4.7 (Generic logical operation). *Let G be a graph code with maximum degree δ^* , and let U be a unitary which can be implemented in depth d_U . Then there is an efficient algorithm which constructs a circuit \mathcal{C}_U that logically implements U on G , such that $\text{depth}(\mathcal{C}_U) \leq 4\delta^* + 6 + d_U$.*

Conceivably, if a depth of δ^* is not immediately prohibitive, an additional factor of 4 significantly reduces the likelihood of practical utility. However, we will show that many important gates, including diagonal Clifford, non-diagonal Clifford, and diagonal non-Clifford gates, can be implemented generically with a reduction on the constant factor.

Theorem 4.4.8. *For any graph code G with maximum degree δ^* , every diagonal gate U can be implemented logically on G with depth at most $2\delta^* + 5$.*

Proof. The circuit is still simply the unencode-apply-reencode operation, but with cancellations due to the diagonal structure. Let E be the encoding circuit from Theorem 4.4.6. The circuit is of depth at most $2\delta^* + 3$ because it is of the form $CZ_V H_V CZ_V$, i.e. a layer of CZ 's acting

on all the nodes V in the graph, a layer of H 's, then another layer of CZ 's. These respectively contribute at most $\delta^* + 1$, 1, and $\delta^* + 1$ to the encoding circuit depth. The logical operation is given by $CZ_V H_V CZ_V U CZ_V H_V CZ_V = CZ_V H_V U H_V CZ_V$ since U commutes with all CZ operations. This circuit has a reduced depth of $(\delta^* + 1) + (1) + (1) + (1) + (\delta^* + 1) = 2\delta^* + 5$. \square

As a corollary, the controlled- Z (CZ), phase (S), and $\frac{\pi}{8}$ (T) gates can all be generically applied with a reduction by a factor of 2 from Theorem 4.4.7.

For a certain non-diagonal Clifford gate, the \sqrt{X} gate, we are able to even further reduce the constant to just 1. This improvement relies on a specific ZX equivalence relation involving a purely-based graph transformation, a local complementation about a vertex (LCV) as defined in Definition 3.2.1. In Definition 3.2.2, we showed how three local complementations about a pair of adjacent vertices create a local complementation about an edge (LCE). We have already seen the effect of an edge local complementation on a graph state in Equation (3.12). Local complementations are defined for any graph and has been presented under various guises in the literature [72, 74].

We have already seen the LCV used in the proof of Lemma 3.4.4, in the expressions in Table 3.1, and in Appendix D to enforce the Clifford rule of the ZXCF.

Below, we fix a vertex set V and consider different graphs which can be made with the nodes in V . Given a graph $G = (V, E)$, let $N(u) = \{v \in V : (u, v) \in E\}$ be the neighbours of $u \in V$ in G . As always, we can assume that G does not permit self-edges; that is, $\forall u \in V, (u, u) \notin E$.

Another way to express local complementations about a vertex is as follows. Let V be fixed and $G = (V, E)$ be a graph. A *local complementation about a vertex* $v \in V$ is a graph transformation $\text{LCV} : \mathcal{G} \times V \rightarrow \mathcal{G}$ given by $(V, E) \mapsto (V, E \Delta K(N(v)))$, where $K(S)$ is the edge set of a complete graph formed by nodes in $S \subseteq V$. As before, we denote the resulting graph $\text{LCV}(G, v)$ as $L_v(G)$.

A LCV about a vertex v can thus be described as follows. Consider the edges of the complete graph built from $N(v)$, and then toggle all these edges in G . That is, if $e \in E \cap K(N(v))$, then remove e from E , and if $e \in K(N(v)) \setminus E$, add e to E .

The LCV builds a bridge between unitary operations on graph codes and inherent graph transformations. Suppose we have a graph $G = (\mathcal{I} \cup \mathcal{O} \cup \mathcal{P}, E)$ and we wish to apply a logical unitary \bar{U} ; that is, \bar{U}_v for $v \in \mathcal{I}$. Generically, if we attempt to use the ZX equivalence rules to push \bar{U}_v to the output, the rules will add more local operators and change edges, resulting in \bar{U} applied to the output \mathcal{O} of a *different graph*, which corresponds to a different code. To make this distinction clearer, let $U_v(G)$ be the operator U applied to $v \in V$ on G . If $v \in \mathcal{I}$, then $U_v(G)$ is a logical operator; otherwise, $U_v(G)$ is a physical operator. For brevity, if $U = U^{(1)} \dots U^{(m)}$, we denote $U_v(G) = U^{(1)} \dots U_v^{(m)}(G)$. We also denote $U_{v_1}(G) \otimes \dots \otimes U_{v_m}(G) = U_{\{v_1, \dots, v_m\}}(G)$.

The specific connection between the LCV and the $\sqrt{X} = HSH$ gate is given in Theorem 3.3.10 and Equation (3.14), which we restate here. Proofs of this relation in the ZX-calculus are given by Backens [72] and Wetering [74].

Claim 4.4.9. *Let $G = (V, E)$ be a graph. Then $\sqrt{X}_v(G) = HSH_v(G) = S_{N(v)}(L_v(G))$.*

Therefore, in order to apply a logical \sqrt{X} on some input vertex $v \in \mathcal{I}$, we apply the LCV about v , and then apply a S gate on all nodes in $N(v)$. Since $N(v) \subseteq \mathcal{O} \cup \mathcal{P}$, all the S gates

are physical.

Lemma 4.4.10. *Given a graph G representing a code, the graph transformation $L_v(G)$ for input vertex $v \in \mathcal{I}$ can be implemented with a quantum circuit of depth at most $\deg(v)$. There is an efficient algorithm outputting this circuit.*

Proof. The graph $L_v(G)$ is constructed from G by applying $CZ_{u,w}$ for all $(u, w) \in K(N(v))$. Since $|N(v)| = \deg(v)$, each node in $K(N(v))$ has degree $\deg(v) - 1$. By Vizing’s theorem, there is an efficient algorithm to arrange the CZ gates to have depth at most $(\deg(v) - 1) + 1 = \deg(v)$. \square

Theorem 4.4.11. *Let G be a graph. There is an efficient algorithm which finds a circuit that implements the logical $\sqrt{X} = HSH$ gate on an input node u with depth at most $\deg(u) + 1$.*

The proof is a direct consequence of Claim 4.4.9 and Lemma 4.4.10.

In general, it seems difficult completely reduce the implementation depth of an arbitrary Clifford circuit because the Hadamard gate does not appear amenable to further optimization. To have a complete set of Clifford operations which can be implemented in depth strictly better than that of Theorem 4.4.7, one solution is to start with a self-dual CSS code, which admits a transversal Hadamard. In this case, the local complementation simplifications that push a H gate through to the output will cancel out in just the precise way as to produce H ’s on all output nodes while preserve the graph structure. $\{H, \sqrt{X}, CZ\}$ is a generating set of the Clifford group, and thus the above results imply that any self-dual CSS code implements logical Cliffords at a depth that is reduced by at least a factor of 2 from the generic procedure of Theorem 4.4.7.

4.4.3 Unification of stabilizer coding algorithms

Thus far, given a graph, we have described its corresponding stabilizers, given a set of logical operators, and provided a simple upper bound on the distance. To complete our fully graph formalism of stabilizer codes, we will show that important code algorithms, distance calculation or approximation, stabilizer weight reduction, and decoding, can all be expressed in a unified graph manner, namely by a single class of one-player games on the graph.

We begin by mentioning an existing game known as “Lights Out”. In Lights Out, a player aims to turn all lights off on a grid with some lights initially on. Each cell in the grid contains both a light and a button or a switch. The player uses moves consisting of pressing a button or toggling a switch at a given cell, thereby *toggling* all of the adjacent cells’ lights as well as the light in the cell. Note that this might cause some lights that were previously off to turn off. The game ends when all lights are off.

Definition 4.4.12 (Quantum lights out). An instance of a quantum lights out (QLO) game on a graph G is described as follows. The graph G consists of both input nodes \mathcal{I} , pivot nodes \mathcal{P} and non-pivot output nodes \mathcal{O} , as usual. However, the notion of a free edge is not needed for QLO and will be discarded. Every node is endowed with both a light and a switch, both of which are binary (i.e. on or off) and which are both initially off. Flipping a switch at node v both (a) permanently destroys the light at v if $v \notin \mathcal{I}$ and (b) toggles all intact (i.e. non-destroyed) lights on the neighbours of v . Let Alice be the player. The graph begins with some initial configuration of lights. The game consists of two rounds:

- (1) Depending on the instance of the game, Alice may be allowed to flip switches of input nodes \mathcal{I} .
- (2) Alice chooses a set of s nodes $v_1, \dots, v_s \in \mathcal{O} \cup \mathcal{P}$, subject to some instance-dependent constraints. For each node v_i , in order, Alice chooses whether to toggle and destroy the switch at v_i or only to destroy the light on v_i . The game ends when the lights reach an instance-specific desired final configuration, usually with all non-input lights off or destroyed.

The specific instance of the QLO game specifies the initial light configuration, whether round (1) exists, the constraints in round (2), and the desired final configuration, e.g. all lights are turned off. Regardless of instance, Alice must make at least one move in round (2). We say that Alice wins in s moves if she makes s choices that lead to the desired final configuration of the game.

By correctly choosing the instance of the game, we can represent many important stabilizer coding algorithms as strategies for QLO games. We begin by showing that finding the distance of a code is QLO. Note that the distance is invariant under unitary operations on inputs, and hence every equivalent Clifford encoder has the same distance.

Theorem 4.4.13 (Distance is QLO). *Given a graph G , denote the distance of the code represented by $d(G)$, which is calculated by the following QLO instance. Initially, all lights are off. In round (1), Alice may flip any number s of switches in \mathcal{I} , the input nodes of G . In round (2), Alice has no constraints and may flip any non-input switch or destroy any non-input light. The final configuration consists of all non-input lights off or destroyed. Additionally, we require that either at least one input light is on or that $s \geq 1$. Under this instance,*

$$d(G) = \min_{\mathcal{A}} m_D(\mathcal{A}, G), \tag{4.12}$$

where \mathcal{A} is Alice's strategy and $m_D(\mathcal{A}, G)$ is the number of moves she made in round (2). As a consequence, every distance approximation algorithm on G which is correct up to a multiplicative error of $1 + \epsilon$ yields a strategy in the distance QLO game instance that is optimal up to a factor of $1 + \epsilon$ in the number of steps.

Proof. Each of the switches flipped on the v^{th} input corresponds to \overline{X}_v , i.e. logical X on logical qubit v . If the game allowed for flipping a single light at a node, this would correspond to applying a Z on the node. There is no point to applying a Z operator multiple times to the same output node, as they will cancel (and we can order them so that no phase occurs). Hence, instead we simplify by destroying the light altogether as a reminder that re-toggling this light does not increase an operator's weight. Next, toggling lights on all neighbours of a node v corresponds to applying X_v . There is no additional Pauli weight if we apply both X_v and Z_v , so for convenience we also destroy the light on v when we flip the switch. Thus, destroying lights and flipping switches correspond to physical Z and X operators. Lights turned on at inputs after all lights on outputs have been extinguished are logical Z operators. Input lights that would have been on had they not been destroyed are logical Y operators. Consequently, the entire distance QLO game consists of applying some logical X operators and translating them into physical operators and logical Z operators. In other words, the

physical operator represented by the n moves apply the logical product of the initial logical X 's and the final logical Z 's, which is a nontrivial logical operator if at least one of the two is not vacuous, i.e. if at least one input light is left on or $s \geq 1$. Since each move in round (2) increases the physical operator's weight by exactly 1, the minimum number of moves is precisely the distance. \square

Since finding the distance of a stabilizer code is **NP**-complete [79], we may immediately conclude that optimally playing QLO on arbitrary graphs is also **NP**-complete.

Theorem 4.4.14 (Weight reduction is QLO). *Let $\{S_i\}$ be the canonical stabilizer generators of G . Without loss of generality, let S_1 be the first stabilizer. Then the minimum-weight stabilizer S'_1 which can replace S_1 in the tableau, i.e. that remains independent of S_2, \dots, S_{n-k} is given by the following QLO game instance. Initially, all lights are off. There is no round (1). In round (2), Alice may freely flip switches on any non-input node except v_1 , the vertex in \mathcal{O} corresponding to S_1 . Specifically, she must flip the switch at v_1 exactly once. The final configuration consists of all lights destroyed or off, including those at inputs. Under this game instance,*

$$|S'_1| = \min_{\mathcal{A}} m_{WR}(\mathcal{A}, G), \quad (4.13)$$

where \mathcal{A} is Alice's strategy and $m_{WR}(\mathcal{A}, G)$ is the number of moves she made in round (2). Thus the minimum weight is equal to the minimum number of moves to end the game.

We formulate the weight reduction theorem in terms of the canonical stabilizers in the graph representation. We observe that an analogous result applies for a different set of stabilizers, so long as they are independent.

Proof. Initially, we apply X_{v_1} when Alice toggles the switch at v_1 in round (2). The canonical stabilizer represents the trivial strategy of flipping pivot switches to remove lights from inputs, and then destroying all remaining lights. However, any sequence of moves that turns all lights off, i.e. effectively applies the identity on the graph, is also a stabilizer. Since we prohibit Alice from either not flipping the switch at v_1 at all or flipping it more than once, the resulting stabilizer is both nontrivial (i.e. not the identity) and independent from all other S_i , since S'_1 is still the only stabilizer containing X_{v_1} . Hence, the minimum number of moves represents the new weight as claimed. \square

By examining the proof, we also observe that the act of writing down the canonical stabilizers and the canonical logical operators are also instances of substantially simpler QLO instances.

Theorem 4.4.15 (Decoding is QLO). *Suppose that after the application of a noisy channel to a codeword, we measure the canonical (or more generally, any known set of) stabilizer generators of the graph of our code, G . We thereby obtain syndrome bits $s_1, \dots, s_{n-k} \in \{\pm 1\}$. Then, the recovery map that should be applied is given by a QLO game instance. Initially, the light at each vertex $v_i \in \mathcal{O}$ corresponding to stabilizer S_i is turned on if $s_i = -1$. All remaining lights start off. In round (1), Alice may flip any number of switches in \mathcal{I} . In round*

(2), Alice has no constraints aside from only being able to act on nodes in $\mathcal{O} \cup \mathcal{P}$, as usual. The final configuration consists of all non-input lights off or destroyed. Under this instance,

$$r(S, G) = \min_{\mathcal{A}} m_{DC}(\mathcal{A}, S, G), \quad (4.14)$$

where S is the set of syndromes, r is the number of moves in the optimal recovery map, \mathcal{A} is Alice's strategy and $m_{DC}(\mathcal{A}, S, G)$ is the number of moves she made in round (2). We note that input lights being on does not affect anything in round (2) or in the minimization condition. This means that, where convenient, input lights can be completely ignored.

Proof. We show that at each step of the decoding procedure, the current syndromes s_i (corresponding to v_i) are given by $(-1)^{\eta_i}$, where η_i is the parity of the number of lights that are currently on in certain sets $\mathcal{T}_i := \{v_i\} \cup p(i(v_i))$. We proceed by casework on each possible type of error, and the stabilizers that they affect.

- (1) $E = Z_v$ for $v \in \mathcal{O}$. E anticommutes with stabilizers which contain X_v . The unique canonical generator which contains X_v is S_v . Thus, applying a Z to a node in \mathcal{O} toggles its light.
- (2) $E = Z_v$ for $v \in \mathcal{P}$. E anticommutes with stabilizers which contain X_v . These are the stabilizers associated with the *non-pivot output neighbours* of the *input* associated with v , i.e. S_u for all $u \in o(i(v))$. Applying a Z to a node in $v \in \mathcal{P}$ negates the syndromes of *all* stabilizers of the vertices $o(i(v))$, and therefore should toggle all lights in $o(i(v))$. We can either view the action of the Z as toggling the lights $o(i(v))$ or, equivalently, as just toggling the light at v , since this will also negate all of the desired syndromes. The reason for this is that $v \in \mathcal{T}_i$ for all v_i in $o(i(v))$. Toggling the lights $o(i(v)) \cup \{v\}$ can be done in round (1) by toggling the switch at $i(v)$, so this equivalence is justified. This means that toggling the light at v is equivalent to toggling the lights of $o(i(v))$. Thus, applying a Z to a node in \mathcal{P} toggles its light.
- (3) $E = X_v$ on any $v \in \mathcal{O} \cup \mathcal{P}$. E anticommutes with stabilizers which contain Z_v . These are S_u for $u \in o(v)$ as well as $w \in o(i(p(v)))$ due to the presence of Z 's in S_u on $o(p(i(u)))$ (note that the order of i and p is reversed when we consider stabilizers affected by a node). Applying an X to a node $v \in \mathcal{O} \cup \mathcal{P}$ toggles all lights in $o(v) \Delta o(i(p(v)))$, or equivalently, $o(v) \cup p(v)$. As shown previously, $X(v)$ is equivalent to Z on all neighbours of v , some of which may be pivots. Applying an X to v flips the switch at v , and thereby toggles the lights on $N_o(v)$, its non-input neighbours. This is equivalent to toggling the lights $o(v)$ and then toggling $o(i(p(v)))$. Thus, applying an X to a node in $\mathcal{O} \cup \mathcal{P}$ toggles all neighbouring lights.

A decoding procedure involves turning off lights by acting on nodes in $\mathcal{O} \cup \mathcal{P}$ (corresponding to physical recovery operators), using the fewest number of moves possible. For $v \in \mathcal{O}$, let S_v be the canonical stabilizer associated with v . The moves in round (1) do not change the syndromes, since for any stabilizer S_i , toggling any input switch will necessarily toggle either zero or two lights in $\mathcal{T}_i = \{v_i\} \cup p(i(v_i))$, depending on whether or not the input neighbours v_i . Additionally, we note that breaking a light at a node after applying the switch at that node represents ambivalence between applying an X or a Y , but if Alice is interested in

finding the proper recovery map instead of just the map’s size, she should leave all lights unbroken. Then, when she is done toggling switches, she can choose to turn off any lights at vertices whose switches she toggled without having this count as a move in round (2). We conclude that decoding algorithms are QLO strategies. \square

We note that construction of the recovery map is very closely related to the calculation of the distance.

The unified expression of all three algorithms, combined with the many complex techniques to perform optimizations on graphs that have been developed in past decades, suggest that the study of approximating optimal QLO strategies may be a promising pathway for devising coding algorithms.

4.5 Applications of the graph formalism

We proceed to provide constructive evidence in three areas for the utility of a graph representation. First, in Section 4.5.1, we argue that for near-term experimental purposes, the graph formalism provides a simple and flexible prescription for the design of codes with a desired rate R and distance d . Intuitively, this advantage occurs because we can appeal to the geometrical and topological structure of graphs, as well as take inspiration from well-studied graphs, to get close to a distance d . We then describe improved results for random codes and construct an efficient graph decoder for a family of stabilizer codes constructed from graphs.

4.5.1 Flexible code design

Generally, stabilizer tableaus have proven more useful as a description rather than a constructive mechanism. Most well-known stabilizer codes constructed are actually CSS codes [50, 52, 53, 59], and non-CSS stabilizer codes are usually found by some alternate representation. The lack of use of stabilizer tableaus is not unusual, as it is simply not obvious as to what collections of Pauli strings construct codes with high distance, easy decoding, gates, geometric properties etc. The universality of the graph representation of stabilizer codes, combined with a rich history of graphs in error correction [51, 53, 62, 80], suggests that a promising technique to construct certain codes lies in finding sufficiently well-behaved graphs.

Due to its universal expressive power, the graph representation in this chapter has parameters that scale with distance. As we showed previously, the distance is bounded above by degree parameters of the graph, and the canonical stabilizers have weights that also scale with the degree. Therefore, the graph representation is best suited for finding codes with a desired approximate numerical values of code parameters, as opposed to asymptotically good LDPC codes. In other words, graphs provide a flexible technique to generate potentially practical small-scale codes.

As an example of this flexibility, if one wanted to create a code with a particular distance, one can set the degree of the graph in accordance with Corollary 4.4.4. On graphs that do not have large overlaps in sets of neighbours, the distance will be determined by the degree of the input vertices as well as the output-degrees of input neighbours. Achieving a certain rate translates to having a sufficiently high density of inputs, which in turn can influence

the required degree of the input neighbours. Some experimental devices or algorithms may benefit from codes that have at most a particular number of physical qubits or encode a minimum number of logical qubits, both of which are easy to set in the graph formalism. If ensuring that the physical qubits behave similarly in a highly uniform manner, a graph could be chosen to be highly regular and symmetric, such as the 5-, 7-, and 9-qubit codes from Section 4.3. Further still, a graph can be chosen to be planar and local in two dimensions, or perhaps supporting only a fixed number of long-range connections for ease of practical implementation. On the other hand, a graph embedded into a higher-dimensional space, such as a high-dimensional grid graph for example, could be easier to represent or simulate classically. We will give examples of codes with each of these properties below.

The distance calculations of codes in this section were performed by direct computation. The code is freely available for use [81].

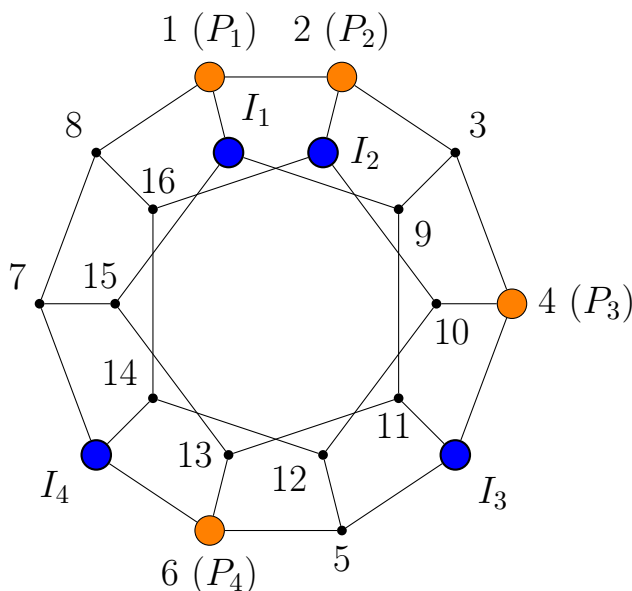


Figure 4.6: The $J_{16,4,3K}$ dodecahedral code. Blue nodes are inputs, black nodes are outputs, and orange nodes are pivots. This code is the optimal packing of input nodes into the dodecahedral graph so that no inputs have a path between them of length less than 3. As the dodecahedron has odd cycles, it is not a bipartite graph and therefore this code is a non-CSS stabilizer code. The rate of the code is higher than that of the 5-qubit code. The labels indicate an ordering of the input and output nodes as well as the pivots (lowest numbered nodes next to each input). There are no extra input-pivot edges but we allow pivot-pivot edges where this does not change our constructions. An ordering can be chosen on the nodes to avoid all pivot-pivot edges, such as by swapping nodes 1 and 15.

4.5.2 The dodecahedral code

We now showcase a few examples of novel small codes that we constructed from the graph formalism. As a first example, we examine the 7-qubit Steane code in Figure 4.3, which takes the shape of a cube. Such a geometric structure motivates the exploration of other

highly regular geometric solids as graph codes, such as the platonic solids. While the graphs of a tetrahedron and octahedron perform rather poorly as codes due to their particular symmetries, the graph of a dodecahedron represents a relatively good code. Figure 4.6 exhibits the dodecahedral code, which has parameters $[[16, 4, 3]]$. Since the degree of every node is 3, the dodecahedral code saturates its distance-degree bound. The rate has also been optimized while not compromising the distance. To maintain a distance equal to the degree, no two inputs may share a neighbour (as otherwise there exists a logical operator of lower weight), so the maximum number of inputs that can be selected is 4. We remark that this graph is not a CSS code, being non-bipartite, but has rate $1/4$. As such, it has the same distance and a higher rate than perhaps the most well-known non-CSS stabilizer code, the $[[5, 1, 3]]$ 5-qubit code from Section 4.3.

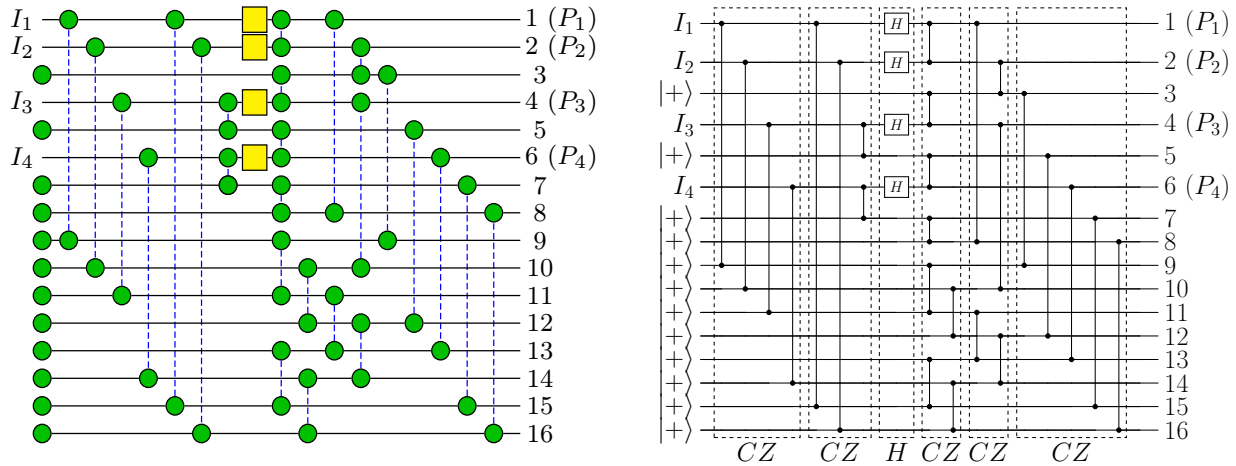


Figure 4.7: Two representations of the encoding circuit of the dodecahedral code, labelled in the same manner as the graph in Figure 4.6. The construction of this circuit is described in Section 4.4.1 and a similar construction is detailed in Appendix H. On the left, the representation is of a ZX diagram. Yellow boxes indicate H gates and blue dashed edges are Hadamarded. On the right, the representation is of a standard quantum circuit. Each dashed block represents a set of transversal (depth-1) operations, so that the circuit depth is the number of blocks, in this case 6. The representation here is partially optimized, by inspection, to improve upon the upper bound given in Theorem 4.4.6. It is possible to move some CZ gates connecting output nodes from one block to the other side of the layer of Hadamard gates to produce a depth-5 (but more visually complicated) circuit, which is provably optimal.

To complete our discussion of the dodecahedral code, we apply Theorem 4.4.6 to give the code a low-depth encoding circuit. Figure 4.7 illustrates two representations of the encoding circuit. On the left, we draw a ZX diagram which appears as an intermediate step in the algorithmic construction in Theorem 4.4.6. On the right, we translate the ZX diagram into standard quantum circuit notation. The translation is an immediate consequence of the ZX-calculus rules discussed in Appendix C: a Z node with a single output is a $|+\rangle$ state and a Hadamarded edge between two Z nodes implements a CZ gate. Corresponding to Theorem 4.4.6, the CZ gates before the layer of Hadamards form the input-output edges; the Hadamards effectively form input-pivot edges; and the CZ gates after the layer of Hadamards

form the edges from non-inputs to non-inputs. We observe also that the application of the ZX-calculus simplification rules to the diagram in Figure 4.7, such as merging Z nodes together, recovers the graph representation of the dodecahedral code itself. In this sense the encoding circuit appears almost immediately from the graph representation.

While our results about the worst-case encoder depth suggest that it may have a depth of up to 9, we have applied some heuristic analysis to reduce the depth to 6. Further compilation of this circuit would allow us to reduce the depth further. This is because output-output edges commute with every gate in the circuit as they are not on the input-pivot wires containing the only non-diagonal gates. In particular, the 5 gates in the last block can be moved to the second, first, fourth, first, and first blocks, respectively, resulting in a circuit of depth 5. This is the minimum possible depth as that is the number of gates acting on some qubits, such as the first input.

4.5.3 Covering spaces and the 5-covered icosahedral code

We next consider a code based on the graph of an icosahedron. Since the vertices of an icosahedron have degree 5, we can hope that a code based on this graph would have distance 5. Unfortunately, we find that the code underperforms the degree bound because a Y gate on two antipodal vertices is equivalent to applying a Z to each vertex. Hence, a logical Y on any input is a logical operation of weight 3, with one Y on the vertex opposite the input and two more on any two antipodal vertices. This observation also implies that if we wish to add more than one input to the icosahedron, our distance will be reduced further, as a logical operation would just consist of Y 's on two vertices opposite the inputs.

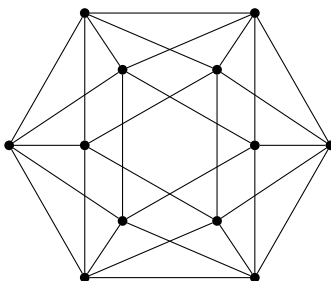


Figure 4.8: The graph of an icosahedron. Although it has degree 5, marking a single node as an input only creates a code of distance 3. We can puncture the icosahedron through the two central faces and take the double cover of the graph with an added index of each vertex matching the winding number of a path around the puncturing axis. If we select one of the 6 outer nodes, nodes that are not vertices of the punctured faces, and mark both copies of the selected nodes as inputs, we create a $J(22, 2, 5)_K$ code. We can improve the rate by covering the icosahedron 5 times and selecting nodes along the perimeter, each rotated 300° (5 steps) around the puncturing axis from the last. Since we mark one node every 300° , we create 6 input nodes, since $6 \cdot 300^\circ = 5 \cdot 360^\circ$. The 5-covered icosahedral code has parameters $J(54, 6, 5)_K$.

To get around this issue, we lift the graph into a finite covering space. Specifically, we can imagine taking a double cover of the icosahedron by puncturing the icosahedron in the center of two opposite faces and attaching a winding number to each vertex, which is computed

modulo 2. In doing so, we find that the double-covered graph with a single input has distance 5. Such a graph can even support two inputs, located at a pair of vertices in the same position in the icosahedron but merely at different indices. This produces a $J22, 2, 5K$ code.

In fact, we can improve the rate slightly by taking an n -cover of the icosahedron. Specifically, when $n = 5$, we can fit 6 input vertices, where the inputs are not vertices of the punctured faces, but rather on the ring between them, and where each input is wound 300° or 5 steps around the punctured axis from the previous input. In Figure 4.8, if we puncture the two central faces, the inputs in the 5 copies of the icosahedron will be on copies of the 6 vertices along the perimeter, each rotated 300° from the last. This construction creates a $J54, 6, 5K$ code.

The ideas used to create the five-covered icosahedron can be extended more generally to extend otherwise finite graphs. In fact, arbitrarily complicated covers can be proposed, leading all the way up to the universal cover of the graph. If regularity and a finite set of vertices are desired, some periodic boundary conditions can be established to keep the graph finite. In general, such covering space graphs may provide a promising path towards code design recipes in this framework. In the case of Cayley graphs, similar ideas have already been used to construct quantum LDPC codes from Cayley graphs of free groups with generators comprised of columns of a classical parity check matrix [82].

4.5.4 Planar and higher-dimensional lattice-type codes

Lattice-type codes enable the construction of families of codes with increasing degree, and thus potentially increasing distance, while also preserving some notions of regularity that are often desirable in code construction. If we wish to remain in two dimensions and also have a Euclidean lattice, we are restricted in the sense that the triangular lattice, which has degree 6, is the highest-degree such lattice. As long as a triangular lattice is taken to be of a certain minimum size, it does yield distance-6 codes. Beyond degree 6, we can either raise the dimension or embed graphs in non-Euclidean spaces. For example, an embedding of triangular surfaces into hyperbolic spaces yields the Poincaré’s disk map. However, since the Poincaré disc packs infinitely many points into a finite space, we would have to construct finite approximations and then study the effect of artificially establishing a finite boundary. Analysis of such effects might lead to discovering interesting code families. In particular, such classes of codes in non-Euclidean spaces may prove useful and might be connected to HaPPY codes [83], which also use graphs in hyperbolic space.

The second approach, increasing the dimension, is more amenable to analysis. A simple, general recipe to construct a code from a lattice is to cut off the lattice in each dimension at a finite number of steps, endow the finite version with periodic boundary conditions in each direction, and embed some inputs and pivots within the vertices such that the choices of pivots are valid and inputs are not connected.

One immediate advantage of this approach is a robustness to deformation that does not hold for CSS codes. In particular, we noted in Theorem 4.2.9 that a graph code is CSS if and only if it is bipartite. For lattices with periodic boundary conditions, the bipartite condition is equivalent to the length of every single dimension of the torus being even. Such a requirement is very non-local and does not change the central architecture of the code. Even for CSS torii, the addition of one vertex far from any inputs such that it forms an odd-length

cycle will make the code no longer CSS but will not meaningfully affect any of the code’s parameters.

When constructing families of codes in the graph formalism, it is important to consider the geometry of the graph as well as the placement of the inputs. To make use of the graph formalism for computing stabilizers and logical operations, the identification of pivot nodes is paramount. While the ZXCF does not allow for pivot-pivot edges, such edges do not affect the expressions of the graph formalism. Thus, for easy pivot selection, it suffices for all of the inputs to be separated by paths of length at least 3 from each other in the graph. Although such a restriction is not necessary for code construction, it does allow for any input’s neighbour to be chosen as its pivot as that node would necessarily not border any other inputs. The downside to such graphs is that their rate is bounded as $R \leq \frac{1}{d}$, where d is the largest degree of the graph. In other words, such graphs have a strong rate-distance trade-off. Nonetheless, these graphs may be interesting at small scales, as we have already seen.

In higher dimensions, perhaps the simplest lattice we can use to build a code is the boolean hypercube in an arbitrary m dimensions. We represent the hypercube by labelling nodes as length- m bitstrings and connecting two nodes if their Hamming distance is exactly 1, i.e. they differ by one bit flip. We observe immediately that the hypercube code is CSS for all m , since the hypercube is bipartite. To select inputs, we observe that if we wish to place inputs such that they are separated by paths of length at least 3, we can leverage classical coding theory to provide this guarantee automatically. Specifically, we consider the *classical* $[2^r - 1, 2^r - r - 1, 3]$ Hamming codes [84]. Letting $m = 2^r - 1$, we can equivalently express the parameters as $[m, m - \log(m + 1), 3]$, where the code is perfect when m is one less than a power of 2. Note that all logarithms in this chapter are taken to be base 2. Since this code has $m - \log(m + 1)$ logical bits, there are a total of $\frac{2^m}{m+1}$ codewords represented as length- m bitstrings. Since the Hamming code’s distance is 3, all such codewords are guaranteed to have a separation in the hypercube by paths of length at least 3. Therefore, by choosing the input nodes in the m -dimensional hypercube to be those whose bitstring is a codeword in the $[m, m - \log(m + 1), 3]$ Hamming code, we obtain a code with $\frac{2^m}{m+1}$ logical qubits, $2^m - \frac{2^m}{m+1} = \frac{m2^m}{m+1}$ physical qubits, and a distance D_m bounded above by the degree m . That is, potentially a $\llbracket \frac{m2^m}{m+1}, \frac{2^m}{m+1}, D_m \rrbracket$ family of codes. Due to the length-3 separation of inputs, any choice of pivots uniquely connected to a corresponding input will do; later, we will show that it is both possible and particularly convenient to choose the pivots such that they are also separated by paths of length at least 3. We will also later prove in Section 4.5.5 that $D_m \gtrsim m/2$, up to an additive error of 2, and give evidence that $D_m = m$. For example, for $m = 7$, the code is $\llbracket 112, 16 \rrbracket$ with distance between 4 and 7. Asymptotically, the code scales as $\llbracket n, \Theta(\frac{n}{\log n}), \Theta(\log n) \rrbracket$.

To improve the rate further without the strong distance-rate trade-off barrier $R \leq \frac{1}{d}$, we will need to use the most general form of graph codes, namely those with inputs separated by paths of length 2. We conclude this section with some remarks on how such codes may be constructed. In a grid lattice on a m -dimensional torus, we wish to pack inputs more closely while being mindful of the fact that our distance will be bounded above by the number of output nodes next to each output node. One such construction is as follows. First, consider a foliation of the m -torus into sequentially numbered “layers” of $(m - 1)$ -dimensional toric

hypersurfaces that together stack into a m -dimensional torus. In each layer, we will consider sets of vertices grouped by their *index*, the sum of their integer coordinates taken mod 3. We can assume that the size of each torus dimension is a multiple of 3 to make sure these sets are well-defined. Note that the index does not consider the m th coordinate, as that is determined by the number of the layer that a node ends up in.

- (1) In layer 1, we set all nodes of index 0 to be inputs, with pivots in layer 2.
- (2) In layer 2, we set all nodes of index 0 or 1 to be pivots.
- (3) In layer 3, we set all nodes of index 1 to be inputs, with pivots in layer 2.
- (4) We repeat this 3-layer structure as many times as desired.

Such a pattern is essentially a 3-layered, high-dimensional analogue of a checkerboard pattern. Again, we see that our distance upper bound is d , as vertices such as those of index 1 in layer 1 have d inputs among their $2d$ neighbours. More sophisticated techniques are necessary to lower-bound the distance. However, the rate of this code is a constant $\frac{2}{7}$, which is achieved at any scale of this code, without the need for extreme numbers of qubits for the asymptotic behaviour of the code parameters to be expressed. Additionally, we note that if an odd number of 3-layer structures are used or if any of the dimensions of each layer is odd, the code graph will have a cycle of odd length, meaning that the resulting code will not be a CSS code.

These examples showcase a wide variety of families and constructions, both small and large, that can be achieved with the graph formalism. While some are sufficiently small to admit brute-force computational distance calculations, others are more difficult to analyze and will require additional distance-bounding tools to understand. We take a first step in this direction in the next section.

4.5.5 Decoding algorithms and analysis

We continue our discussion by constructing a simple greedy decoding algorithm on graphs. We give a sufficient-condition characterization of graphs for which the greedy decoder successfully recovers errors up to half of the theoretical maximum. That is, graphs which satisfy this certain property have a provable distance *lower bound* based on its degree. Finally, we will show that the $\mathbb{J}_{\frac{m2^m}{m+1}, \frac{2^m}{m+1}}\mathbb{K}$ boolean hypercube code, defined in Section 4.5.4, satisfies this characteristic and thus is efficiently decodable.

Denote for simplicity $oip(v) := o(i(p(v)))$, $ip(v) = i(p(v))$, and $oi(v) = o(i(v))$. In Theorem 4.4.15, we showed that decoding amounts to strategies in QLO. There, we presented a more sophisticated approach in which the lights on pivots encoded information about stabilizers that were connected to the pivots' corresponding inputs. In our greedy decoder, it will be simpler for analysis purposes to do away with this notion and decode more directly. That is, X errors on a node v toggle lights in $o(v) \Delta oip(v)$, Z errors on a pivot v toggle lights in $oi(v)$, and Z errors on a non-pivot output v toggle the light at v . (Y errors are treated as both an X and a Z error.) As a consequence, there are no lights at all on pivots (since there are no stabilizers there). Moreover, we apply recoveries by directly performing the same operations, e.g. if we wish to do a X -recovery on a node v , we toggle lights in

$o(v) \Delta oip(v)$ and destroy the light at v . We note that this paradigm is equivalent to the QLO game instance from Theorem 4.4.15. In particular, suppose that after every switch flip on v Alice also flips the switches on $ip(v)$, which immediately toggles the lights on the neighbours, i.e. turning off the lights in $p(v)$ and turning on the lights in $oip(v)$. This rule maps the QLO game in the theorem to the setup we have given here. But the flipping of input switches can be moved post-hoc to round (1) in the game, not changing the number of moves made in round (2), and thus the two paradigms are entirely equivalent.

Algorithm 1: Greedy graph decoder

```

Function GreedyDecoder( $G$ ):
  explored  $\leftarrow$  [], ( $v_0, n_0$ )  $\leftarrow$  (nil, 0)
  while True do // X error recovery loop
    for  $v \in \mathcal{O} \cup \mathcal{P}$  do
      gap  $\leftarrow$  2NumLights( $o(v)$ ) -  $|o(v)|$ 
      // If more than half of lights around  $v$  are on, 'gap' is
      // positive
      if gap >  $n_0$  then
         $v_0 = v, n_0 = \text{gap}$ 
      if  $v_0 \in \text{explored}$  or gap = 0 then
        break
      Recover $_X(v_0)$  // toggle lights at  $o(v_0) \Delta oip(v_0)$ , destroy light at
       $v_0$ 
      Append  $v_0$  to explored
  explored  $\leftarrow$  [], ( $v_0, n_0$ )  $\leftarrow$  (nil, 0) // Reset tracking variables
  while True do // Z error on pivots recovery loop
    for  $v \in \mathcal{P}$  do
      gap  $\leftarrow$  2NumLights( $oi(v)$ ) -  $|oi(v)|$ 
      if gap >  $n_0$  then
         $v_0 = v, n_0 = \text{gap}$ 
      if  $v_0 \in \text{explored}$  or gap = 0 then
        break
      Recover $_Z(v_0)$  // toggle lights at  $oi(v_0)$ 
      Append  $v_0$  to explored
  for  $v \in \mathcal{O}$  do // Z error on outputs recovery loop
    if LightIsOn( $v$ ) then
      Recover $_Z(v)$  // Destroy light at  $v$ 
  return

```

The greedy decoder is a strategy in the decoding instance of QLO. In particular, the operations permitted are Recover $_X$ and Recover $_Z$, which flip switches or destroy lights depending on the node v chosen. We showed earlier in Theorem 4.4.15 how a QLO strategy maps to a physical recovery operation. The construction of the algorithm is based on the following intuition. If $v \in \mathcal{O}$ suffers a X error, the stabilizers at $o(v) \Delta oip(v)$ will measure -1 , so in the QLO game the lights in $o(v) \Delta oip(v)$ will turn on. Perhaps there will be some

Z errors in $o(v) \subseteq \mathcal{O}$, each of which correspond to turning on a single light in $o(v)$. Therefore, assuming it is difficult to turn on more than half of the lights in $o(v)$, a good guess is that if more than half of the lights are on in $o(v)$ then v has suffered an X error, at which point we can apply X on v to reverse the error, via RECOVER_X . Note that we do not consider the status of the lights in $oip(v)$ when deciding whether to toggle v , as all lights in $oip(v)$ can be toggled by applying an X to any neighbour of $p(v)$. The recovery operation may itself turn on more lights in other places, so to avoid issues related to parallelism, we work in sequence and apply X recoveries one at a time, in order of nodes which have the most neighbours with lights on. A similar story holds for Z errors on $v \in \mathcal{P}$. They are detected by stabilizers in $oi(v)$, so we apply the analogous greedy recovery operation there. Finally, for remaining lights on in $v \in \mathcal{O}$, we directly destroy the lights with Z operations.

We note that this decoder echoes the greedy strategy using by Sipser and Spielman [51]. There, variables were similarly toggled to satisfy as many unsatisfied constraints as possible. A key distinguishing feature of our work is the ability of nodes to act both as constraints and as variables. When a graph is bipartite, the nodes can be partitioned into variables and constraints, but this only allows one to work with CSS codes, as discussed in Theorem 4.2.9. Studying more general expander graphs through the graph formalism seems like a promising avenue for future work.

The key property behind the intuition about graphs that enable greedy-type decoding is the idea that it must be difficult to simulate an X error on some v by using a small amount of moves to turn on most of the lights in $o(v)$. We now formalize this property to give a simple performance guarantee of the greedy decoder.

In this definition, we are specifically interested in how many lights an operation at node v can toggle in the set $o(u)$, the set we examine to determine whether to toggle the switch at u .

Definition 4.5.1. Let $G = (V, \{o, i, p\})$ be a graph with input, output, and valid pivot nodes. We say that G is B -sensitive if

- (a) for all $u \in \mathcal{O} \cup \mathcal{P}$, $v \in \mathcal{O} \cup \mathcal{P}$, $u \neq v$, $|o(u) \cap (o(v) \Delta oip(v))| \leq B$ (X error on any output or pivot v),
- (b) for all $u \in \mathcal{O} \cup \mathcal{P}$, $v \in \mathcal{O}$, $u \neq v$, $|o(u) \cap (\{v\} \Delta o(v) \Delta oip(v))| \leq B$ (Y error on non-pivot output v),
- (c) for all $u \in \mathcal{O} \cup \mathcal{P}$, $v \in \mathcal{P}$, $u \neq v$, $|o(u) \cap (oi(v) \Delta o(v) \Delta oip(v))| \leq B$ (Y error on pivot v),
- (d) and for all $u \in \mathcal{I}$, $v \in \mathcal{P}$, if $u \neq i(v)$, i.e. v is not the pivot corresponding to input u , then $|o(u) \cap oi(v)| \leq B$ (Z error on pivot v).

The case $|o(u) \cap \{v\}| \leq B$ (Z error on non-pivot output v) is not included because it is always satisfied, since we always take $B \geq 1$.

These four conditions together form a sufficient condition to place a relatively tight guarantee on the greedy decoder's performance.

Theorem 4.5.2 (Greedy guarantee). *Let G be a B -sensitive graph. Denote $\delta_* := \min_{v \in V} \deg(v)$ the minimum degree of G . Then the greedy graph decoder corrects at least $\lfloor \frac{\delta_*}{2B} \rfloor$ errors. In other words, the less sensitive a graph is, the more effective the greedy decoder. For constant B , the decoder thus corrects $\Theta(\delta_*)$ errors.*

Proof. The decoder will fail if it makes either of the following two errors: (1) it applies $\text{Recover}_P(v)$ when v did *not* suffer a Pauli P error (Y errors are treated separately as both an X and a Z error) or (2) it fails to apply a $\text{Recover}_P(v)$ when v *did* suffer a Pauli P error. By the construction of the greedy decoder, this phenomenon occurs only if enough errors happened to flip at least $\lceil \frac{d}{2} \rceil$ lights in $o(v)$ or in $oi(v)$ if v is a pivot. Indeed, in the former case, enough errors occurred to have turned on the majority of lights in $o(v)$ or $oi(v)$ without the corresponding error having occurred on v , and in the latter case it turned off the majority of lights even when the corresponding error occurred. Conditions (a)-(c) of Definition 4.5.1 guarantee that it takes strictly more than $\lfloor \frac{1}{B} \lfloor \frac{\delta_*}{2} \rfloor \rfloor = \lfloor \frac{\delta_*}{2B} \rfloor$ errors to trick the decoder in either way during the X -recovery part of the algorithm, and condition (d) guarantees the same lower bound for the Z -on-pivots-recovery part of the algorithm. In condition (d), note that we equivalently used $o(u)$ for $u \in \mathcal{I}$ rather than $oi(u)$ for $u \in \mathcal{P}$ (as in the Z -on-pivots-recovery loop in Algorithm 1), and we have disregarded the $u = i(v)$ case which corresponds to an actual Z error on $p(u)$ which would be correctly decoded. Thus, in all cases at least $\lfloor \frac{\delta_*}{2B} \rfloor$ errors are required to cause the decoder to act incorrectly, which completes the proof. \square

Recall that key code properties, the weight of canonical stabilizers, the distance, and the canonical encoding circuit depth, are all bounded above by the degree. Since the number of errors corrected t and the distance are related by $2t + 1 \leq \text{dist}(C) \leq 2t + 2$, our result also implies a two-way bound on the distance of B -sensitive graphs.

Corollary 4.5.3 (Distance bound). *Let G be a B -sensitive graph and minimum degree δ_* , and let $C(G)$ be the code that G represents. Then $\lfloor \frac{\delta_*}{B} \rfloor \leq 2 \lfloor \frac{\delta_*}{2B} \rfloor + 1 \leq \text{dist}(C(G)) \leq \delta_*$.*

Similarly, we can give a bound on the encoding circuit based directly on the distance.

Corollary 4.5.4 (Encoding circuit bound). *Let G be a B -sensitive graph and minimum degree δ_* . Let $C(G)$ be the code that G represents, and let \mathcal{C} be its canonical encoding circuit as defined by the algorithm from Theorem 4.4.6. Then $\text{depth}(\mathcal{C}) \leq \delta_* = 2B \lfloor \frac{\delta_*}{2B} \rfloor + B - B \leq B(2 \lfloor \frac{\delta_*}{2B} \rfloor + 1) - B \leq B(\text{dist}(C(G)) - 1)$.*

The proof is an immediate consequence of needing a depth of at least δ_* from Theorem 4.4.6 and of Corollary 4.5.3.

Although they are not necessary for the purposes of establishing Theorem 4.5.2, several end-of-line optimizations to Algorithm 1 can improve its practical performance.

- (1) *Neglecting destroyed lights.* Redefine gap to be the difference between the number of lights on in $o(v)$ and the number of lights that are *off but not destroyed* in $o(v)$. The only difference between this definition and the original is that lights which are destroyed are not counted. This follows because once a light is destroyed, it does not contribute to the QLO game anymore. Equivalently, a node with a destroyed light has already had some Pauli on it, which increased the weight of the total Pauli string by 1. Therefore, adding another Pauli to the same node does not increase the weight.
- (2) *Gap edge case.* In the X loop, if $\text{gap} = 1$ for the chosen node v , then only apply the recovery if the majority of un-destroyed lights in $oip(v)$ are on. This is because it costs

one move in QLO to apply the recovery, and if the majority of lights are off in $oip(v)$ then one might actually turn more lights on than off by recovering, which could slightly increase the total number of moves.

- (3) *Parity redundancy.* In the X recovery loop, consider only $o(v) \setminus oip(v)$ instead of $o(v)$, since lights in $o(v) \cap oip(v)$ cannot be turned on by X on v because X_v toggles each such light twice. Nodes in $o(v) \cap oip(v)$ can be affected by all other nodes which are neighbours of $p(v)$.

For a given graph code, a smaller sensitivity implies an increased effectiveness of the greedy decoder. We now give a family of codes for which the sensitivity is nearly optimal. Previously, we defined the hypercube code in Section 4.5.4 with parameters $\lfloor \frac{m2^m}{m+1}, \frac{2^m}{m+1} \rfloor$. We label the nodes of the hypercube by their length- m binary string representation. Denote by e_i the i th standard basis vector in \mathbb{Z}_2^m , i.e. $(e_i)_i = 1$ and $(e_i)_{j \neq i} = 0$. Moreover, we showed by injection of the classical Hamming code that the input nodes of the hypercube code are separated by paths of length at least 3. Before we prove that the hypercube has sensitivity 2, we give a useful lemma.

Lemma 4.5.5 (Hypercube separation). *It is possible to choose pivots on the hypercube code such that every path between pivots has length at least 3.*

Proof. The minimum path length between inputs is already 3. By homogeneity of the hypercube, it is enough to choose the pivots in a uniformly consistent way for every input. One example which works is to set $p(v) = \{v + e_1\}$ for all $v \in \mathcal{I}$. This assignment will never choose $p(v) \in \mathcal{I}$ since the inputs are separated by paths of length at least 3. Now suppose there exists a path between two pivots p_1 and p_2 with length less than 3. In other words, with at most 2 bit flips, we can go from p_1 to p_2 , so $p_2 = p_1 + e_a + e_b$ for some $a, b \in [m]$. Since $p_1 = i_1 + e_1$ and $p_2 = i_2 + e_1$, where i_j is the input corresponding to p_j , $i_2 = i_1 + e_a + e_b$, which contradicts the fact that inputs are separated by paths of length at least 3. \square

We note that there are several other transformations that can be applied to the hypercube to choose a set of pivots. One such other example is a $\frac{\pi}{2}$ axis-aligned rotation.

Theorem 4.5.6 (Hypercube sensitivity). *Every hypercube code is 2-sensitive.*

Proof. By homogeneity, let $u = 0^m$ without loss of generality, so that $o(u)$ has only weight-1 bitstrings. We expand into each of the four cases in Definition 4.5.1. The general idea is that when we take neighbour-type operations $p(\cdot), o(\cdot), i(\cdot)$ on a bitstring with weight M , the resultant bitstring's weight can only change by 1 due to the connectivity of the hypercube.

- (a) Let $u, v \in \mathcal{O} \cup \mathcal{P}$. If $o(u) \cap (o(v) \Delta oip(v)) \neq \emptyset$, then $|v| \in \{2, 4\}$. These cases are shown in Figure 4.9(1)-(2).
- i. If $|v| = 2$, let $v = e_i + e_j$ for $i \neq j$. So $o(u) \cap o(v) \subseteq \{e_i, e_j\}$. It is possible, as shown in Figure 4.9(1) for $oip(v)$ to contain weight-1 bitstrings as well. We work forwards. By Lemma 4.5.5, $p(v)$ has at most one element. Since inputs correspond bijectively to pivots, $ip(v)$ thus also has at most one element. Suppose $\exists w \in ip(v)$. Then $oip(v)$ intersects $o(u)$ nontrivially only if $|w| \in \{0, 2\}$. However, u is the unique element

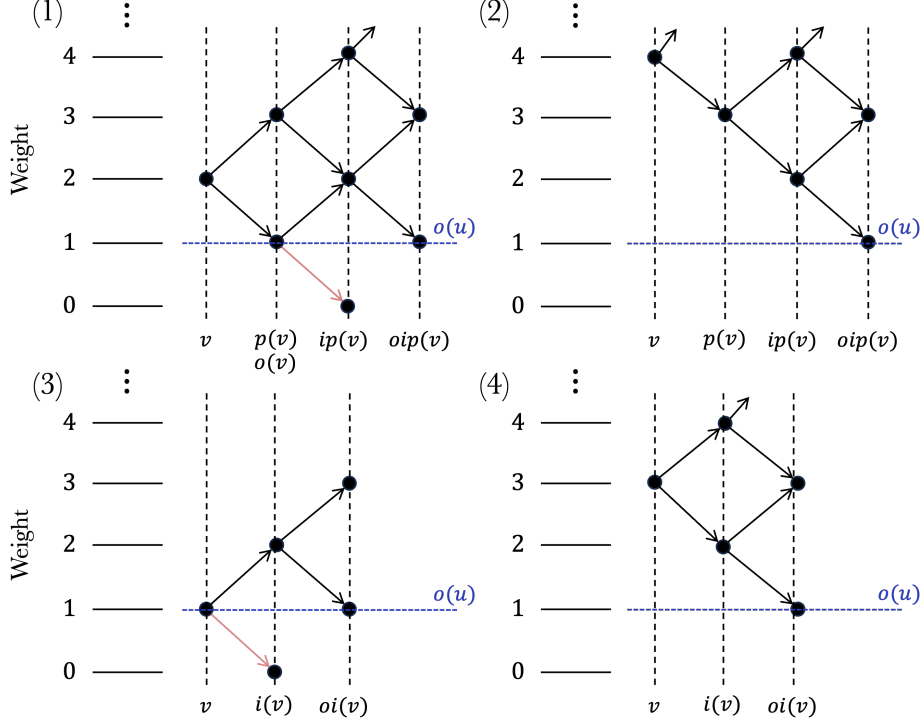


Figure 4.9: Possible weights of nodes in a hypercube code after neighbouring operations (1) $o(v)$ and $oip(v)$ with starting weight $|v|=2$, (2) $oip(v)$ with starting weight $|v|=4$, (3) $oi(v)$ with starting weight $|v|=1$, and (4) $oi(v)$ with starting weight $|v|=3$. $u=0^m$ in all cases, so $|w|=1$ for all $w \in o(u)$. The red arrows correspond to paths that a priori seem possible but do not actually exist.

whose weight is 0, and $u \notin \mathcal{I}$. Thus, since $w \in \mathcal{I}$, $|w| \neq 0$ so $|w|=2$. Let $w = e_k + e_l$ for some $k \neq l$. Since w and v are separated by a path of length 2, $|w - v|=2$. Moreover, $|v|=2$. The only way to transform $e_i + e_j \rightarrow e_k + e_l$ is if at least one of $\{e_i, e_j\}$ equals one of $\{e_k, e_l\}$. Without loss of generality, say $e_i = e_k$. Then $o(u) \cap o(v) \subseteq \{e_i, e_j\}$ and $o(u) \cap oip(v) \subseteq \{e_i, e_l\}$, so $o(u) \cap (o(v) \Delta oip(v)) \subseteq \{e_j, e_l\}$, and hence $|o(u) \cap (o(v) \Delta oip(v))| \leq 2$.

ii. If $|v|=4$, then $o(v)$ has weight at least 3, so the only possible intersection must come from $oip(v)$, as shown in Figure 4.9(2). We argue similarly as before; namely that $ip(v)$ has at most one element, and if such an element w exists it must have weight 2 for $oip(v) \cap o(u) \neq \emptyset$. We write $w = e_i + e_j$ for $i \neq j$. Hence, $oip(v) = o(w)$ has at most two weight-1 elements, e_i and e_j . So $|o(u) \cap (o(v) \Delta oip(v))| \leq 2$.

(b) In case (a) we showed that any nontrivial overlap with $o(v) \Delta oip(v)$ requires $|v| \equiv 0 \pmod{2}$. But $v \in o(u)$ only if $|v|=1$. In the former case, i.e. $|v| \equiv 0 \pmod{2}$, $v \notin o(u)$, so we reduce to bounding $|o(u) \cap (o(v) \Delta oip(v))|$ which we have done already in case (a). In the latter case, $o(u) \cap (o(v) \Delta oip(v)) = \emptyset$ so $|o(u) \cap (\{v\} \Delta o(v) \Delta oip(v))| = |o(u) \cap \{v\}| \leq 1$.

(c) Now $v \in \mathcal{P}$, and $u \in \mathcal{O} \cup \mathcal{P}$ as before. If $o(u) \cap oi(v) \neq \emptyset$, then $|v| \in \{1, 3\}$ as shown in Figure 4.9(3)-(4). As seen earlier $|v| \equiv 0 \pmod{2}$ in order for $o(u) \cap (o(v) \Delta oip(v)) \neq \emptyset$.

For $|v|$ even we have shown before the $B = 2$ bound. For $|v|$ odd it suffices to consider the overlap $o(u) \cap oi(v)$. Since $v \in \mathcal{P}$, $i(v)$ is the unique element w associated to the pivot v .

- i. If $|v|=1$, then $|w| \in \{0, 2\}$ as shown in Figure 4.9(3). Since $w \in \mathcal{I}$ and $u \notin \mathcal{I}$, $w \neq u$ so $|w| \neq 0$. Write $w = e_i + e_j$ for some $i \neq j$. Thus, $o(u) \cap oi(v) \subseteq \{e_i, e_j\}$, so $|o(u) \cap oi(v)| \leq 2$.
 - ii. If $|v|=3$, then unless $|w|=1$, $oi(v) \cap o(u) = \emptyset$ as shown in Figure 4.9(4). Then $w = e_i + e_j$ for $i \neq j$, so $o(u) \cap oi(v) \subseteq \{e_i, e_j\}$ and thus $|o(u) \cap oi(v)| \leq 2$.
- (d) Now, $u \in \mathcal{I}$, $v \in \mathcal{P}$, and $u \neq i(v)$. This case has essentially already been proven by part (c). The only difference is that the input node $w = i(v)$ cannot have weight 0 because $u \neq i(v)$.

□

As a consequence of the optimal sensitivity of the hypercube, we can not only correct its errors well by a greedy approach, but also obtain a good distance lower bound that is at most a factor of 2 from optimal.

Corollary 4.5.7. *The d -dimensional hypercube code has distance between $2 \lceil \frac{d}{4} \rceil + 1 \approx d/2$ and d .*

We believe that a more careful analysis requiring detailed casework can show that our algorithm is correct up to $\frac{d}{2}$ errors, and thus distance d . However, this example already shows that we can use this formalism to construct graphs that give simple and intuitive algorithms for decoding.

Conjecture 4.5.8. *The d -dimensional hypercube code has distance d and a greedy decoding algorithm can decode up to $\lfloor \frac{d-1}{2} \rfloor$ errors.*

4.5.6 Random codes with reduced stabilizer weights

One direct technique for which a graph formalism enables more controlled analysis is random codes. Under the stabilizer tableau representation, the quantum Gilbert-Varshamov-bound gives an asymptotic (large n) relation between code parameters n, k, d that, if satisfied, guarantee the existence of a $[n, k, d]$ code.

Theorem 4.5.9 (Quantum Gilbert-Varshamov). *For parameters $d \leq \frac{n}{2}$ and k which depend implicitly on n , as $n \rightarrow \infty$ there exists a $[n, k, d]$ code if $nH(d/n) + d \log 3 < n - k$, where $H(p) := -p \log p - (1 - p) \log(1 - p)$ is the binary entropy function of $p \in [0, 1]$.*

We give a self-contained proof of Theorem 4.5.9 in Appendix F. The proof proceeds probabilistically, namely by generating a uniformly random stabilizer tableau and arguing that such a tableau has a nonzero probability of having distance d if the bound is satisfied. However, because the expected weight (i.e. number of non-identity elements) of a random Pauli string $P_1 \otimes \cdots \otimes P_n$, where $P_i \in \{I, X, Y, Z\}$, is $O(n)$, the random codes generated in the Gilbert-Varshamov fashion will have linear stabilizer weight. A natural question is whether

the average weight can be decreased by a stochastic algorithm that is more fine-grained than uniform randomness. Such a task has proven difficult in the stabilizer tableau representation due to the challenge of generating Paulis that both commute and are not uniformly distributed. On the other hand, we can easily generate random graphs of a certain structure by defining first the possible edges that may be included, and then randomly choosing edges to include in the graph. This insight enables us to extend the result of the quantum Gilbert-Varshamov bound by way of the following theorem.

Theorem 4.5.10. *Let n be the number of physical qubits and define $R(n) < 1$ and $d(n) \in [\omega(1), \frac{n}{\log n}]$. There exists an efficiently sampleable family of distributions \mathcal{S}_n , parameterized by n , over stabilizer codes that as $n \rightarrow \infty$ satisfy three properties.*

(a) *The stabilizer weights are*

$$|S_i| \leq \min(n, (4 + o(1))Rd^2 \log^2 n), \quad (4.15)$$

where S_i is a stabilizer from a tableau sampled from \mathcal{S}_n ,

(b) *the rate is $R(n)$, and*

(c) *with probability at least $1 - n^{-d}$, a random code from \mathcal{S}_n will have distance $d(n)$.*

We remark that the idea of finding a smaller class of objects which achieve desirable properties is conceptually similar to an idea explored recently by Cleve *et al.* [85], who showed that there is a strict subgroup of the Clifford group that also uniformly mixes non-identity Paulis.

Theorem 4.5.10 is positive in that it provides a nontrivial bound on the stabilizer weight of random codes for many choices of $R(n)$ and $d(n)$, and it gives a strong probabilistic concentration of $1 - n^{-d}$. For any $d \in [\omega(1), O(\frac{n}{\log n})]$, this concentration implies that almost all codes in \mathcal{S}_n have the desired properties. On the other hand, Theorem 4.5.10 complements, as opposed to subsuming, the Gilbert-Varshamov bound because it provides a nontrivial weight reduction at substantially sublinear distances. It also forces the stabilizer weight, at least for the generating set we construct, to be at least as large as the distance, which is an artifact of our proof technique. However, the result nonetheless remains interesting because of the guarantees it is able to provide and the flexibility that it offers. Indeed, practically useful codes are seldom asymptotically good. Since the distance and the rate are both determining factors for the stabilizer weight, we obtain a three-way distance-rate-weight trade-off of random codes that can be leveraged to study sublinear-distance codes in which we care much less about one of the three properties than the others. As with the other claims in this chapter, this result is thus complementary of LDPC constructions that are asymptotically good but have intractably large constants. Instead, we interpret this result as evidence that for moderately large codes, e.g. $n \sim 50$ at a scale where we expect little- o asymptotics to take effect, there is a great deal of flexibility in the graph construction to build codes of certain ranges of R and d which also may have a relatively small stabilizer weight.

We proceed to the proof of Theorem 4.5.10.

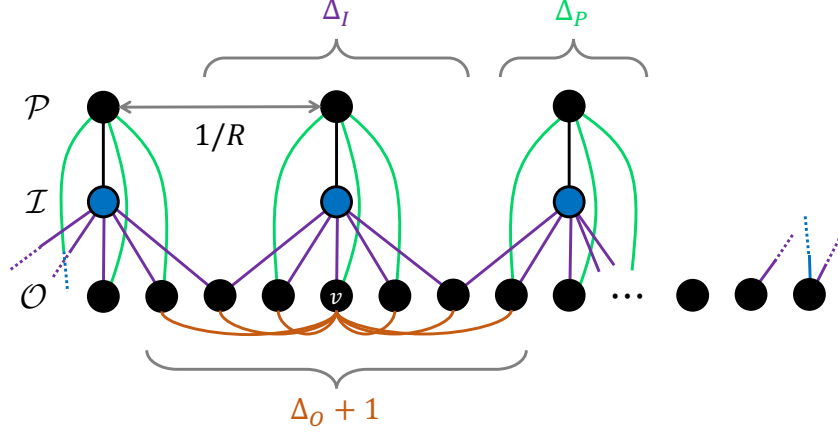


Figure 4.10: General localized random graph construction. Nodes are separated into k input nodes $i \in \mathcal{I}$, (which are spaced apart by $1/R$), k pivot nodes $p \in \mathcal{P}$, and $n - k$ non-pivot output nodes $o \in \mathcal{O}$. Each pivot p (input i) can connect to output nodes within a diameter Δ_P of p (Δ_I of i); here, $\Delta_P = 3$ ($\Delta_I = 5$) and the possible lines are green (purple). Similarly, output nodes o may connect to outputs in a diameter Δ_O of o . For clarity, only the possible connections for a single output v is shown, and here $\Delta_O = 6$.

Proof. We construct elements of \mathcal{S}_n graphically as shown in Figure 4.10 and we denote this graph G . In particular, we begin with an encoder-respecting form, separating the inputs \mathcal{I} , pivots \mathcal{P} , and (non-pivot) outputs \mathcal{O} . Next, we assign each set of nodes a *locality diameter*, respectively $\Delta_I, \Delta_P, \Delta_O + 1$ (the $+1$ since the output node is included in its diameter but does not have a self-edge). The boundary conditions are periodic. Each node may only connect to output nodes within their locality diameter. We sample from \mathcal{S}_n by iterating through each connectable edge and randomly including or excluding it from the graph with probability $1/2$; the resulting stabilizer tableau is the one defined by the collection $S := \{S_v\}_{v \in \mathcal{O}}$ where $S_v := X_v Z_{N_o(v)} X_{p(i(v))} Z_{N_o(p(i(v)))}$ as described in Section 4.4. For notation, we say that S_v contains a Pauli X_i (Z_i) if the i^{th} element of S_v is X_i or Y_i (Z_i or Y_i). Our analysis of this stochastic algorithm adapts the techniques in the analysis of Theorem 4.5.9 to the graph picture. We fix a non-identity Pauli P and consider four cases.

- (1) $P = Z^{\otimes T}$ for $T \subseteq [n]$ and T does not contain any pivots. Pick $i \in T$ and consider $v_i \in G$. Then S_{v_i} must anticommute with P because S_{v_i} contains $X_{v_i} X_{p(i(v_i))}$ which only overlaps P in one position. Hence, P does not commute with S .
- (2) $P = Z^{\otimes T}$ for $T \subseteq [n]$ and T contains at least one pivot $p \in \mathcal{P}$. Let $i \in \mathcal{I}$ be the unique input connected to p . Each of the Δ_I output nodes v within the diameter Δ_I of i have probability $1/2$ of connecting to i . S_v contains X_p if and only if i and v are connected. Since the (anti-)commutativity of P and S_v are determined only by the parity of the number of qubits on which X 's in S_v overlap with Z 's in P , the probability that S_v and P commute is $1/2$ regardless of the other Paulis in S_v and P . Furthermore, consider any other S_w where w is also in the diameter of i . Since w has an edge connecting to i distinct from that of v , the probability of S_w and P commuting is independently $1/2$. This argument is general to all output nodes in the diameter of i , and remaining stabilizer

act on disjoint subspaces. Hence the probability that P commutes with S is $2^{-\Delta_I}$.

- (3) P contains at least one X_p for $p \in \mathcal{P}$. Analogously, $\Pr[P \text{ commutes with } S] = 2^{-\Delta_P}$ by considering the Δ_P nodes in \mathcal{O} which each independently have probability $1/2$ of having a Z_p .
- (4) P contains at least one X_v for $v \in \mathcal{O}$. $\Pr[P \text{ commutes with } S] \leq 2^{-\Delta_O}$ by an analogous argument. We neglect some stabilizers which could anticommute with P by acting through neighbouring pivots, i.e. the $Z_{N_o(p(i(v)))}$ component, since that can only decrease the probability and complicates the expression.

Set $\Delta_O = \Delta_P = \Delta_I := \Delta$. We proceed to bound the probability of the event $A(S)$ that there exists non-identity P with weight $\leq d$ which commutes with S . As shown in Appendix F, there are $2^{nH(d/n)+d \log 3+O(\log n)}$ such Paulis, where $H(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy. By the union bound,

$$\Pr[A(S)] \leq 2^{nH(d/n)+d \log 3+O(\log n)-\Delta} \leq \epsilon, \quad (4.16)$$

where ϵ bounds the fraction of codes which do not have distance at least d . We therefore solve the inequality

$$\Delta \geq \log \frac{1}{\epsilon} + nH\left(\frac{d}{n}\right) + d \log 3 + O(\log n). \quad (4.17)$$

Since $\frac{d}{n} \leq \frac{1}{\log n}$, we can asymptotically expand the binary entropy as $H(d/n) \rightarrow (\frac{1}{\ln 2} - \log \frac{d}{n})\frac{d}{n}$, giving

$$\Delta \geq \log \frac{1}{\epsilon} + d \log n + o(d \log n). \quad (4.18)$$

Here we have used our assumption that $d = \omega(1)$, so that $O(\log n) = o(d \log n)$. Let $\epsilon = n^{-d}$, so that if $\Delta = 2d \log n + o(d \log n) = (2 + o(1))d \log n$ at least $1 - n^{-d}$ of codes asymptotically have distance d . Lastly, we calculate the stabilizer weights. Each stabilizer is of the form $S_v = X_v Z_{N_o(v)} X_{p(i(v))} Z_{N_o(p(i(v)))}$. These terms have at most 1, Δ_O , $\Delta_I R$, and $\Delta_P \Delta_I R$ Paulis, respectively. The worst case occurs when the sets have no overlap and all edges are connected. Hence,

$$|S_v| \leq 1 + \Delta + \Delta R + \Delta^2 R = (4 + o(1))Rd^2 \log^2 n. \quad (4.19)$$

Additionally, $|S_v| \leq n$, which gives the claimed result. \square

An important special case of Theorem 4.5.10 is for graphs in which all inputs are at least 3 nodes away from each other, in which case $R = 1/\Delta$ and thus $|S_v| \leq (2 + o(1))d \log n$.

4.6 Conclusion and outlook

We introduced a graph structure which universally represents all stabilizer codes. Stabilizer tableaux can be efficiently compiled into such graphs, and vice versa. Our primary motivation for such a representation was to gain access to natural graph properties and notions, such

as their degree, geometry, and connectivity, and then to leverage them to improve code construction and analysis. As first steps in this direction, we chose several geometric shapes discretized into graphs and analyzed them as code representations. In doing so, we found a number of constant-size codes with desirable rates and reasonably large numerical distances, as well as a family of hypercube codes that have near-linear rate, logarithmic distance, and good encoding/decoding properties. In similar spirit, we also constructed a class of codes for which, given a desired rate R and distance d , a random code drawn from the class has high probability of having rate R , distance d , and, so long as R and d were not both too large, nontrivially bounded stabilizer weights. This analysis extends the result of the quantum Gilbert-Varshamov bound, which has a distance-rate trade-off but no bound on stabilizer weight due to its coarse-grained analysis.

Chapter 5

Equivalent Quantum Codes

5.1 Introduction

A number of approaches have been created to represent the components of quantum error-correcting codes. The stabilizer formalism is a method that expresses quantum error-correcting codes in terms of stabilizers, operators that, when applied to certain stabilizer states, preserve the state [20]. This approach borrows ideas from group theory to represent the whole class of stabilizers with a finite number of generators. To make the idea of quantum error-correcting codes visual, recent advances have made progress on the topic of representing quantum states through graphs [30]. We as we saw in the last few chapters, graphs can be incredibly powerful in their expressions of quantum states, circuits, codes, and more.

Following the work on graph states, progress has been made on representing Clifford codes using the ZX-calculus [65, 72, 86], a graphical language for expressing and manipulating certain families of tensor networks. The properties of the ZX-calculus allow it to do anything that can be done in the stabilizer formalism, an expression of codes and states as a list of generators of commuting operators. Specifically, these properties include its universality, meaning it can express every quantum operation, its soundness, meaning that we can independently derive equivalence rules for ZX-calculus diagrams, and its completeness, meaning ZX-calculus diagrams can derive equivalences of tableaux [65, 72]. This graphical language has had various applications in quantum information [66–69] and quantum computation problems [70, 71].

Figure 5.1 gives a summary of the work done in graphically presenting quantum Clifford encoders. The set of all quantum Clifford encoders as graphs is split into different categories based on the type of code represented (CSS or general Clifford codes) and four different equivalence operations (output permutations, local operations, local complementation, and unitaries on inputs). Note that equivalence under local operations means equivalence under any local Clifford operations on the outputs. All four of these categories represent different equivalences, which preserve the information the receiver gets while changing the encoder’s ZX diagram in some way. Some of them change the encoder (output permutations, local operations, and unitaries on inputs), and a different set of them change the code (output permutations and local operations).

Expressing quantum Clifford encoders as graphs and finding canonical forms for equivalent graphs has had recent advances in the past few decades. A depiction of this is shown in

All Quantum Clifford Circuits as Graphs

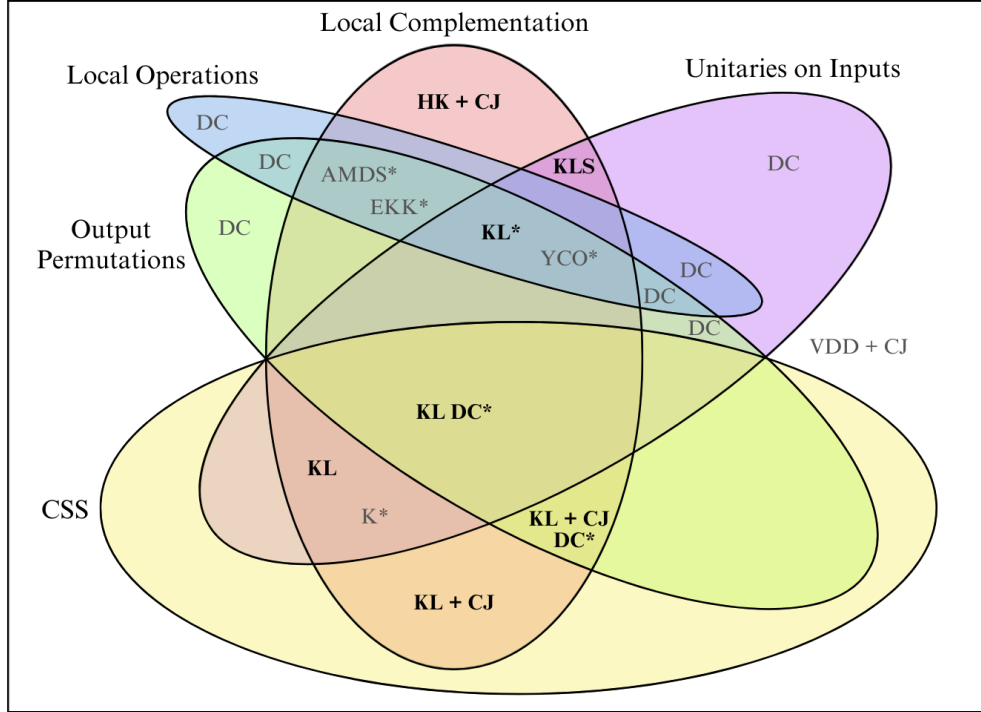


Figure 5.1: A summary of the work done on the equivalence classes of graphs of quantum Clifford encoders. Four of the categories, output permutations, local operations, local complementation, and unitaries on inputs, are different equivalences that preserve the information received. The CSS category is not an equivalence relation and shows results specific to CSS codes. Note that the CSS and local operations categories do not intersect because equivalence by local operations can transform a CSS code into a non-CSS code. The regions of the diagram are labelled with works on studying graphs under the corresponding equivalences. Asterisks denote results that give non-unique forms, and DC denotes results that are direct consequences of previous works. Abbreviations used are explained in the main text.

Figure 5.1. The work of Van den Nest, Dehaene, and De Moor [30] (VDD) provides a conversion between any Clifford state and a graph with local Clifford gates, and the Choi-Jamiołkowski isomorphism [87, 88] (CJ) extends this to a conversion between any Clifford circuit and a graph with local Clifford gates. Starting from the graphs of the Clifford encoders, we find the canonical forms of the direct consequences (DC's) located only within the bubbles for output permutations, local operations, and unitaries on inputs. For output permutations, we remove the numbering on the outputs. For local operations, we remove all local Clifford operations on the outputs. For unitaries on inputs, we remove input-input edges, local Clifford operations on the inputs, and the numbering on the inputs. Any combination of these three become DC in Figure 5.1.

The HK form from Chapter 3 provides a canonical form for quantum Clifford states. In the context of quantum encoders, this is equivalent to having no inputs and only outputs.

Additionally, the KLS form from Chapter 4 built on the HK form, providing a canonical form for Clifford encoders. Chapter 4 shows the process of transforming stabilizer tableaux into the ZX-calculus, then performing operations that preserve equivalence to transform the graph into its canonical form. A similar construction to the one used in Chapter 4 has been studied by Yu, Chen, and Oh [61] (YCO). Adcock *et al.* [89] (AMDS) and Englbrecht, Kraft, and Kraus [90] (EKK) considered equivalence of graph states under local complementations and the effects of relabelling the nodes.

Kissinger [62] (K) found a way to represent the CSS codes using internal measurement nodes. Section 5.3 establishes the KL canonical form of CSS codes and states. In Figure 5.1, direct consequences (DC's) of Section 5.3 follow through a removal of the numbering on output nodes. These fall within the CSS region. In Section 5.6, Section 5.7, and Section 5.8, we consider equivalence classes under all four equivalences for general Clifford encoders.

Informally, our main results in this chapter are specializing the HK and KLS canonical forms to CSS codes. This simpler set of rules for our canonical form allows for the simpler generation of CSS codes. Simply by constructing a bipartite graph and designating nodes in one of the two vertex groups to be inputs, one can design new CSS codes. In this chapter, we also investigate and classify families of small stabilizer codes under the afore-mentioned equivalence relations.

In this chapter, Section 5.2 contains key definitions and background on the ZX-calculus and Clifford encoders. Section 5.3 presents our main result, the KL canonical form for CSS codes, giving a unique, phase-free form for CSS codes that minimizes the number of nodes and clearly shows the Z stabilizers and logical Z operators. These results are also extended to CSS states, which will be defined later. Section 5.4 contains our results on toric codes and specific surface codes, and it shows different forms of these codes, including the canonical form for the toric code based on Section 5.3. These two sections build on the KLS forms for Clifford codes and recent work [62, 91, 92] that introduced the normal form of CSS codes, which can efficiently determine the stabilizers from the ZX normal form. Our representations of CSS codes will also have this property. Furthermore, our representations reduce the number of nodes used in the ZX diagrams so that each node corresponds to either an input or output.

Section 5.5 introduces prime code diagrams, which are code diagrams that are composed of one connected component. Furthermore, we prove the Fundamental Theorem of Clifford Codes, showing a unique prime decomposition of Clifford codes.

Section 5.6 provides another definition of equivalence, permitting outputs to be permuted as a valid operation among equivalent graphs. This definition of equivalence is also considered since changing the order of the outputs does not change any code parameters. Simplifications on the set of non-equivalent Clifford encoders are given to narrow down the search for the canonical form. In Section 5.7 and Section 5.8, we show our results on identifying equivalence classes and finding representative forms. We analyze the equivalence class sizes and the presence of bipartite forms among these classes. Section 5.8 expands on the equivalence classes containing bipartite forms and considers some classes that do not have bipartite forms.

5.2 Background

We begin by defining key terms and background on error-correcting codes and the ZX-calculus.

First, we recall the definition of Pauli matrices, as given in Definition 2.2.1.

The *Pauli matrices* are

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5.1)$$

The Pauli matrices represent quantum gates that can act on qubits and alter their state. All four gates are Hermitian, and the three gates X, Y, Z are pairwise anti-commutative. The *Pauli operators on n qubits* are n -fold tensor products of Pauli matrices, multiplied by a factor of the form i^k where $k \in \{0, 1, 2, 3\}$ and $i = \sqrt{-1}$.

The Pauli operators are all equal to their conjugate transposes, so all Pauli operators are Hermitian and unitary. The Pauli operators form a group, called the *Pauli group*.

Pauli operators can act on states in multi-qubit systems. For example, in a three qubit system, the tensor product $Z \otimes Z \otimes I$ will make Z act on the first qubit, Z act on the second qubit, and I act on the third qubit. The notation for the tensor product can be simplified to $Z_1 Z_2$, with the subscripts showing which qubits the operators are acting on. We may also write these three gates as ZZI , omitting the tensor product symbols. Other Pauli operators on multiple qubits can be written analogously.

Other quantum gates that are commonly used in quantum error-correcting codes are the Hadamard (H), controlled-NOT (CNOT), phase (S), and $\pi/8$ (T) gates, as defined in Definition 2.2.3.

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \quad (5.2)$$

These operations have the property of universality, the ability to approximate any operator to arbitrary accuracy [1].

We define *encoders* of quantum error-correcting codes as families of quantum processes that apply a transformation on some number of input qubits, mapping it to a given range. Specifically, we will only be concerned with the case of *full-rank* or *non-degenerate* encoders where the encoding operation is injective, meaning that the dimension of the range is at least as large as the number of inputs. We write that an encoder takes k inputs, or logical qubits, and gives n outputs, or physical qubits. Note that an encoder can mean any quantum map in the family of such processes defined by the image. Thus, two different circuits that differ only by a unitary operation on the inputs represent the same encoder.

Encoding quantum information into a larger number of qubits provides redundancy, making it possible to correct certain errors. The *stabilizers* of an encoder are a set of commuting operations that can be composed with the output of an encoder without any change to the overall process. In the stabilizer formalism, the stabilizers determine the entire quantum code [93]. A family of encoders are *Clifford codes*, quantum error-correcting codes such that each stabilizer is a Pauli operator on n qubits. All stabilizers of a Clifford code on k inputs form a group isomorphic to \mathbb{Z}_2^{n-k} and can be defined by a set of linearly independent *generators*. For k -to- n codes, or $[[n, k]]$ codes, we have $n - k$ generators. The code maps the input qubits onto elements of the *codespace*, the range of the code, which is the intersection of the $+1$ eigenspaces of the code's stabilizers.

The ZX-calculus is a graphical language used for expressing quantum states, circuits, and codes through tensor networks made of two types of nodes, Z and X nodes. This

chapter makes heavy use of ZX-calculus diagrams and rewrite rules. An introduction to the ZX-calculus with associated definitions and rewrite rules can be found in Appendix C.

We recall the definition of ZX diagrams of codes expressed in their *encoder-respecting form* from Definition 4.2.2. We restate this definition here with a slight modification: we allow X nodes in the diagram. If these X nodes were to be replaced by Z nodes with Hadamard gates on every incident edge, the result would always be a diagram satisfying the definition of Definition 4.2.2, so relaxing this constraint does not meaningfully change the set of encoder-respecting forms.

The *encoder-respecting form* is a ZX representation of a Clifford code that contains Z (green) and X (red) nodes, with each node corresponding to an input or output. Each node has a corresponding free edge, an edge not connected to any other nodes, with input nodes having input edges and output nodes having output edges. The outputs may have local operations on their free edges. Each of the k input nodes may only have connections with the output nodes, while each of the n output nodes may have connections to each other. Additionally, the output edges are numbered from 1 to n .

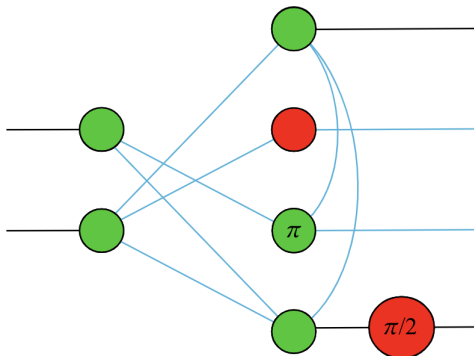


Figure 5.2: Example of an encoder in the ZX-calculus. The incoming edges from the left side are input edges (sending information in) and the outgoing edges on the right side are output edges (sending encoded information out). Note the local operations applied on the output qubits, with blue edges representing edges with Hadamards. This encoder is not in encoder-respecting form.

An example of a Clifford code expressed in encoder-respecting form is shown in Figure 5.2. There are local operations on the output edges, as shown by the blue free edges and X gate (X node with phase $\pi/2$). The X node is not considered an output node since it is isolated as a local operation on its neighbouring Z node. There are internal edges in the graph between the input and output nodes and from the output nodes to other outputs, but not from inputs to inputs. Two qubits of are encoded into four qubits in this example.

We recall from Definition 4.2.3 and Theorem 4.2.5 that encoders with the same sets of stabilizers have the same ZXCF, also known as their KLS canonical form. This form consists of four rules that can be efficiently checked for a given ZX diagram. We restate the main result of Theorem 4.2.5 here.

For any stabilizer code there is a unique equivalent ZX diagram satisfying the following

rules. We say that a ZX diagram satisfying these rules is a KLS diagram and is in KLS form. A KLS diagram must be in encoding-respecting form and all of its nodes must be Z nodes. Such a diagram must also satisfy the following rules.

- (1) *Edge rule:* All internal edges have Hadamards, and there is exactly one Z node per free edge.
- (2) *Hadamard rule:* Output nodes with Hadamard gates on their free edges cannot share an edge with a lower-numbered output node or with an input node.
- (3) *RREF rule:* The adjacency matrix representing the edges between input nodes and output nodes is in reduced row-echelon form (RREF).
- (4) *Clifford rule:* In the RREF matrix, the pivot columns of the input to output adjacency matrix correspond to pivot output nodes. There are no local Clifford operations on the pivot or input nodes, or their free edges. There are also no input-input edges or pivot-pivot edges.

Additionally, we know from Theorem 4.2.5 that a given ZX diagram can be efficiently transformed to its KLS canonical form using a series of ZX rewrite rules. Furthermore, as discussed in Section 4.4.1, KLS canonical forms may be efficiently transformed into quantum circuits. We list a slightly modified version of the transformation procedure, which only differs from the encoder in Section 4.4.1 in where it places the layer of Hadamard gates. The exact ZX-calculus transformation rules that transform a graph code into an encoding circuit described below are shown in Appendix H.

Consider an $\llbracket n, k \rrbracket$ encoder given in its KLS form. Then, it can be efficiently transformed into an equivalent quantum circuit using the following steps.

- (1) Start with k open wires representing the inputs of the circuit.
- (2) Add a $|0\rangle$ state for each of the $n - k$ non-pivot output nodes.
- (3) Apply an H gate to all n wires.
- (4) Apply a CX gate between the wires corresponding to the edges between inputs and non-pivot outputs. The input node is the target qubit, and the output node is the controlled qubit.
- (5) Apply a CZ gate between the wires corresponding to the edges between only outputs.
- (6) Apply the local operations attached to the outputs.

This procedure works by building up the encoder's quantum circuit representation in layers, starting from the input qubits, which correspond to the ZX diagram input nodes, adding auxiliary qubits that encode the information from the input qubits, and connecting the qubits using the appropriate gates.

Lastly, we recall several key definitions regarding graphs.

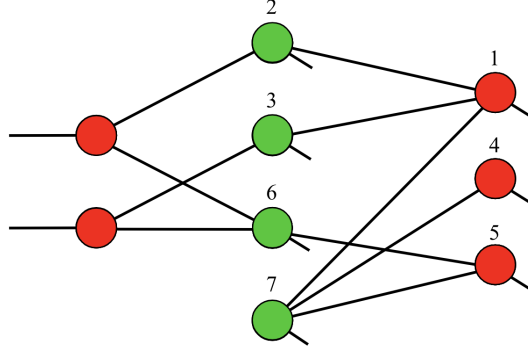


Figure 5.3: Example of a CSS code in KL canonical form. The short diagonal edges are the free output edges of the 7 output nodes.

The *neighbourhood* $N(v)$ of a vertex v in a graph $G = (V, E)$ is the set of all vertices in V adjacent to v , not including v itself. An operation commonly used to apply equivalence transformations to ZX diagrams is local complementation, as defined in Definition 3.2.1.

Let G be a graph $G = (V, E)$, where V and E are the sets of vertices and edges in G , respectively. Consider a vertex $v \in V$. A *local complementation* about vertex v is a transformation of the graph G where all edges connecting two vertices in $N(v)$ are toggled. That is, if the edge existed before the local complementation, it is removed; if it did not exist before, it is added. We denote the effect of this operation as $L_v(G)$.

5.3 Canonical form for CSS codes and states

Calderbank-Shor-Steane (CSS) codes are a commonly studied class of quantum error-correcting codes constructed starting from two classical codes [94–97]. The generators of a CSS code’s stabilizers can be chosen such that each of the generators is either a Pauli operator with only I and Z gates or a Pauli operator with only I and X gates.

We introduce the notion of a CSS state.

Definition 5.3.1. A *CSS state* is a CSS code with 0 inputs.

We now present the KL canonical form of CSS codes and CSS states in the ZX-calculus, and prove that it is canonical in this section. The KL forms for CSS codes are special cases of KLS forms, which are for Clifford codes. However, since CSS codes have nice properties and structure, it is interesting to study the rules and properties governing this subclass of canonical forms, KL forms.

All KL forms are in encoder-respecting form as in Definition 4.2.2, meaning every input and output node has its own free edge, and the output nodes are numbered from 1 to n . However, as stated in Section 5.2, we allow encoder-respecting forms to have both Z and X nodes.

Theorem 5.3.2 (KL canonical form for CSS codes). *For any CSS code, there is a unique equivalent ZX diagram satisfying the following rules.*

- *Bipartite rule:* The nodes can be split into two groups. One group consists of the input nodes (which are all X nodes) as well as the output X nodes. The other group consists of the output Z nodes. The only interior edges allowed are between two nodes from two different groups.
- *Phase-free rule:* All input and output nodes have phase 0 and there are no local operations on any free edges.
- *RREF rule:* The adjacency matrix between the input X nodes and output Z nodes is in reduced row echelon form (RREF). The adjacency matrix between the output X nodes and all output nodes, where the output X nodes are marked as connected to themselves, is also in RREF.

Remark 5.3.3. Note that the first part of the RREF rule is equivalent to the one set in the KLS form, in which the adjacency matrix between the inputs and outputs is in RREF. Additionally, note that the second part of the RREF rule is equivalent to stipulating that no output X node be connected to a lower-numbered Z node. This implies that the second part of the RREF rule is equivalent to the Hadamard rule set in the KLS form, in which outputs without Hadamards cannot connect to lower-numbered output nodes or input nodes.

An example of the KL form is shown in Figure 5.3. The Bipartite rule is made clear by the division of the nodes into columns, with the first and last columns of nodes forming the first group (X nodes) and the middle column forming the second group (Z nodes). The edges satisfy the constraint that the output X nodes only connect to higher-numbered output Z nodes. Lastly, the input X nodes to output Z nodes adjacency matrix is in RREF.

In CSS states, the part in the RREF rule pertaining to input nodes is unnecessary because of the lack of input nodes while the Bipartite and Phase-free rules still apply. As a corollary, we also find the canonical form for CSS states.

Corollary 5.3.4 (Canonical form for CSS states). *For any CSS state, there is a unique equivalent ZX diagram satisfying the following rules.*

- *Bipartite rule:* The nodes can be split into two groups, one with X nodes and the other with Z nodes. The only interior edges allowed are between nodes of different groups.
- *Hadamard rule:* Each X node can only connect to higher-numbered Z nodes.
- *Phase-free rule:* All output nodes have phase 0, and there are no local operations on any free edges.

Now, we build up to the proof of Theorem 5.3.2. To do this, we proceed analogously to Section 4.2.3. Specifically, we show that each KL form corresponds to a distinct CSS code by counting the number of CSS codes and comparing it to the number of KL diagrams, and we later show that any KL form can be converted into the stabilizer representation of the CSS code. These two steps establish the bijection between the KL forms and CSS codes. We start by finding the number of CSS codes.

Lemma 5.3.5. *The number of CSS codes with n physical qubits, p Z stabilizers, and q X stabilizers is*

$$\frac{\prod_{i=1}^p (2^n - 2^{i-1})}{\prod_{i=1}^p (2^p - 2^{i-1})} \cdot \frac{\prod_{i=1}^q (2^{n-p} - 2^{i-1})}{\prod_{i=1}^q (2^q - 2^{i-1})}. \quad (5.3)$$

Proof. Consider choosing the Z stabilizers of the CSS code's stabilizer tableau. Since each stabilizer must be linearly independent from each other, there are $\prod_{i=1}^p (2^n - 2^{i-1})$ ways to choose p independent stabilizers. However, different sets of p generators could represent the same set of stabilizers. For a given set of stabilizers, there are $2^p - 2^{i-1}$ ways to choose the i^{th} generator, so we must divide to find

$$\frac{\prod_{i=1}^p (2^n - 2^{i-1})}{\prod_{i=1}^p (2^p - 2^{i-1})} \quad (5.4)$$

as the number of ways to choose the set of Z stabilizers.

Next, each X stabilizer must commute with all of the Z stabilizers. Since the number of X stabilizers that commute or anti-commute with any single Z stabilizer is equal, there are $2^n/2^p = 2^{n-p}$ X stabilizers to choose from. Using a similar analysis as above, there are

$$\frac{\prod_{i=1}^q (2^{n-p} - 2^{i-1})}{\prod_{i=1}^q (2^q - 2^{i-1})} \quad (5.5)$$

ways to choose the set of X stabilizers.

Multiplying these two counts gives the number of CSS codes with the given parameters, as desired. \square

Now, we find the number of KL diagrams with similar parameters. We will show later that the parameters chosen below make the KL forms correspond exactly to the CSS codes with n outputs, p Z stabilizers, and q X stabilizers.

Consider a KL form of a CSS code. Let there be p output X nodes and $n - p - q = k$ input nodes, so that there are $n - p$ output Z nodes, of which k are pivot nodes in the RREF adjacency matrix between the input nodes and output Z nodes.

First, consider the output nodes. Note that there are n total nodes among the X and Z groups. To count the number of ways to connect edges between the output X and Z nodes in the KL form, note that the Hadamard rule restricts the connections to those from lower-numbered output X nodes to higher-numbered output Z nodes.

Lemma 5.3.6. *In the KL form, the number of ways to connect the $n - p$ output Z nodes and p output X nodes is*

$$\frac{\prod_{i=1}^p (2^n - 2^{i-1})}{\prod_{i=1}^p (2^p - 2^{i-1})}. \quad (5.6)$$

Proof. In the proof of this lemma, we only consider the output nodes of the encoder.

Consider building up the ZX diagram as follows. Each time an output node is added, some number of possible connections could be made between the newly added output node and the nodes that have already been placed. The nodes are added in order, so each node has a higher index than all the nodes that came before it.

Let p' be the number of remaining X nodes that need to be added in the ZX diagram. Let q' be the number of remaining Z nodes that need to be added in the ZX diagram. The function $f(p, p', q')$ counts the number of ways to add nodes and edges starting from some arbitrary state that has p' remaining X nodes and q' remaining Z nodes. The total number of X nodes after placing all nodes will be p . We find a recursive relation for $f(p, p', q')$.

When $p' = 0$ and $q' \neq 0$, all of the remaining Z nodes can be added in and connected arbitrarily to the p pivots in $2^{pq'}$ ways, giving $f(p, 0, q') = 2^{pq'}$.

When $p' \neq 0$ and $q' = 0$, all of the remaining X nodes can be added in, but they cannot connect to anything since they necessarily are higher-numbered than all of the Z nodes. Therefore, $f(p, p', 0) = 1$.

When $p' \neq 0$ and $q' \neq 0$, either a X node is added or a Z node is added (note there are $2^{p-p'}$ ways to connect edges between the new Z node and $p - p'$ current X nodes), giving the recursive equation

$$f(p, p', q') = f(p, p' - 1, q') + 2^{p-p'} f(p, p', q' - 1). \quad (5.7)$$

We can check that the following function $f(p, p', q')$ satisfies this recursive equation and the base cases considered above:

$$f(p, p', q') = \frac{2^{(p-p')q'} \prod_{i=1}^{p'} (2^{q'+i} - 1)}{\prod_{i=1}^{p'} (2^i - 1)}. \quad (5.8)$$

The total number of ways to connect the $n - p$ Z and p X nodes must be $f(p, p, n - p)$. Evaluating the above expression with these parameters gives a count of

$$\frac{\prod_{i=1}^p (2^{n-p+i} - 1)}{\prod_{i=1}^p (2^i - 1)} = \frac{\prod_{i=1}^p (2^n - 2^{i-1})}{\prod_{i=1}^p (2^p - 2^{i-1})}, \quad (5.9)$$

as desired. □

Now, we count the number of ways to form connections between the input nodes and output Z nodes.

Lemma 5.3.7. *In the KL form, the number of ways to connect the k input nodes and $n - p$ output Z nodes is*

$$\frac{\prod_{i=1}^q (2^{n-p} - 2^{i-1})}{\prod_{i=1}^q (2^q - 2^{i-1})}. \quad (5.10)$$

Proof. We have to count the number of ways to connect the input nodes and output Z nodes to form an RREF adjacency matrix between them. Imagine each input node and its corresponding pivot node (in the RREF matrix) as a single *super-node*. Super-nodes may not connect with each other, since pivots may not connect with other inputs, by the RREF rule. Also, the pivot node is the lowest-numbered node among the Z outputs that the input node connects to, so the super-node can only connect with non-pivot nodes that are higher-numbered.

Therefore, we have k super-nodes and $q = n - p - k$ single output Z nodes, and connections are restricted to those between super-nodes and higher-numbered single output Z nodes. This is equivalent to $f(k, k, q)$ from the proof of Lemma 5.3.6, so the number of ways to connect the input nodes and output Z nodes must be

$$\frac{\prod_{i=1}^k (2^{q+i} - 1)}{\prod_{i=1}^k (2^i - 1)} = \frac{\prod_{i=1}^q (2^{n-p} - 2^{i-1})}{\prod_{i=1}^q (2^q - 2^{i-1})}, \quad (5.11)$$

giving the desired result. □

From Lemma 5.3.6 and Lemma 5.3.7, we find the total number of KL forms by multiplying the two expressions found, giving us a total count of

$$\frac{\prod_{i=1}^p (2^n - 2^{i-1})}{\prod_{i=1}^p (2^p - 2^{i-1})} \cdot \frac{\prod_{i=1}^q (2^{n-p} - 2^{i-1})}{\prod_{i=1}^q (2^q - 2^{i-1})}. \quad (5.12)$$

Since this matches with Lemma 5.3.5, the number of KL forms is indeed equal to the number of CSS codes under certain parameters, so each KL form can correspond to a distinct CSS code. Now, we need to show that restricting the CSS codes to n physical qubits, p Z stabilizers, and q X stabilizers is equivalent to restricting the KL forms to n output nodes, $n - p$ output Z nodes, and p output X nodes.

In Equation (4.10), we found the canonical stabilizer generators of codes by examining their KLS form. In this section, we derive analogous results for CSS codes in KL form. Specifically, starting from the KL form of a CSS code, we determine the Z stabilizers, X stabilizers, and logical Z operators of the code.

Lemma 5.3.8. *Each of the output X nodes corresponds to its own linearly independent Z check.*

Proof. Consider an output X node v . We identify a Z stabilizer that includes the operator Z_v by sliding a Z gate through node v . By the π -copy rule from Definition C.1, this Z gate splits into Z gates on all the other incident edges of node v . Each of these Z gates travels down an incident edge and combines with the output Z node at the other end of the edge. Ultimately, this results in a phase of π on all the neighbours of node v .

Since this is equivalent to placing Z 's on all the neighbours of node v , we have made a Z stabilizer, which is the product of Z_v and the Z gates on the neighbouring output Z nodes.

The Z checks of the output X nodes are linearly independent from each other because each Z check contains a Z operator on a distinct output X node. \square

Lemma 5.3.9. *Each of the non-pivot output Z nodes corresponds to its own linearly independent X check.*

Proof. Consider a non-pivot output Z node v . We identify an X stabilizer by sliding an X gate through this node. By the π -copy rule, this X gate splits into X gates on all the other incident edges of node v . This results in a phase of π on all the neighbours of node v . For each of the neighbours that are input nodes, an X node of phase π can be unmerged from the input X node and slid towards the input's corresponding pivot node. The unmerging rule is given in Definition C.1. By the π -copy rule, all other incident edges, including the free output edge, of the pivot node get a X π node. Then, the output X neighbours of the pivot node receive additional phases of π .

Since this is equivalent to placing X 's on all the pivots of input nodes connected to v and placing X 's on all the output X nodes that end up with phase π , we have made an X stabilizer, which is the product of the X gates just described and X_v .

The X checks of the non-pivot output Z nodes are linearly independent from each other because each X check contains an X operator on a distinct non-pivot output Z node. \square

The *logical operator* of a code maps an element of the codespace onto another element of the codespace. We denote the logical Z operators as \bar{Z} and the logical X operators as \bar{X} . The Z and X stabilizers can be used to determine all the logical operators of a CSS code. Analogously, the Z stabilizers and logical Z operators of a CSS code can be used to determine all the X stabilizers.

Lemma 5.3.10. *The adjacencies of the inputs determine the logical Z operators.*

Proof. Consider an input node v . Similar to Lemma 5.3.8, we identify a logical Z operator by sliding a Z gate through node v .

Since all of the input nodes are X nodes, the Z gate will split into Z gates onto all the incident edges of node v . Ultimately, all the neighbours of node v will have a phase of π due to \bar{Z}_v .

Since this is equivalent to placing Z 's on all these neighbouring nodes of node v , we have made a logical Z operator, which is the product of the Z gates on the neighbouring output Z nodes.

Note that, in the adjacency matrix between the input nodes and output Z nodes, each input node has a corresponding pivot. Therefore, the logical Z operators determined by the input nodes will be linearly independent from each other because each has a Z gate on a distinct element (i.e. the pivot node) in the set of output Z nodes. \square

We are now ready to prove our main result.

Proof of Theorem 5.3.2. For a stabilizer code with n physical qubits, the number of stabilizers and logical operators adds up to n . Considering the KL form of a CSS code with p red output nodes and k input nodes, we find, from Lemma 5.3.8, Lemma 5.3.9, and Lemma 5.3.10, that there are p Z stabilizers, q X stabilizers, and $k = n - p - q$ logical Z operators. Since these three numbers add up to n , all stabilizers and logical Z operators are accounted for by these three lemmas. This means that the KL forms with p output X nodes, $n - p$ output Z nodes, and k input nodes correspond exactly to the CSS codes with n physical qubits, p Z stabilizers, and q X stabilizers.

From Lemma 5.3.8 and Lemma 5.3.9, we also see there is a clear way to convert from a KL form into a representation of the CSS code entirely in terms of its Z stabilizers and X stabilizers.

Then, since KL forms can be converted into a stabilizer representation and the number of KL forms is equal to the number of CSS codes of analogous parameters, it follows that there is a bijection between CSS codes with n physical qubits, p Z stabilizers, and q X stabilizers and KL forms with n output nodes, of which p are red output nodes and $n - p$ are green output nodes, finishing the proof of Theorem 5.3.2. \square

This construction allows us to prove several propositions. First, we complete correspondence between the KL form and the stabilizer tableau. Lemma 5.3.8, Lemma 5.3.9, and Lemma 5.3.10 explain how to construct both types of stabilizers and Z logical operators. Although this is enough to determine the X logical operators, we can also use the following.

Proposition 5.3.11. *The adjacencies of the pivots determine the logical X operators.*

Proof. Consider an input node v . We identify a logical X operator by sliding a X gate through node v . Since all input nodes are X nodes and the X gate is an X node with a phase of π , we merge and unmerge it with the input node to move it along the edge connecting the input to its pivot, an output Z node. Then, we use the π -copy rule to turn the X gate into X gates on each other edge connected to the pivot. Note that this means that an X gate will be placed on the pivot's free edge as well as each other internal edge connected to the pivot. Since the pivot node cannot be connected to any inputs other than v and the graph is bipartite, this means that these X gates can be moved towards the output X nodes and then merged and unmerged along each of those outputs' free edges.

Note that, in the adjacency matrix between the input nodes and output Z nodes, each input node has a corresponding pivot. Therefore, the logical X operators determined by the input nodes will be linearly independent from each other because each has an X gate on a distinct element, the pivot node. \square

Remark 5.3.12. The stabilizers of a CSS code need to commute with each other and with each logical operation, while the logical Z and X operations on a single input should anti-commute. From Lemma 5.3.10 and Lemma 5.3.11 we see that logical Z and X operations can only overlap on pivot nodes, and since each only has a local operation on the pivot node corresponding to the input of the logical operator, the only anti-commuting operations will be logical Z and X operations on the same input.

For stabilizer commutation, we see from Lemma 5.3.8 and Lemma 5.3.9 that a Z and X stabilizer can only intersect at an X output node or at its Z output neighbours, as those are

the elements of a Z stabilizer. Each of the Z output nodes present in the Z stabilizer will also place a term on the neighbouring X output node. This will make the parity of total overlapping nodes even, making sure the stabilizers commute.

The same argument as above shows why Z stabilizers commute with logical X operations. Since X stabilizers only have gates on Z output nodes at the corresponding non-pivot node and on several pivot nodes, a logical Z operation will either not intersect it or intersect the stabilizer exactly twice, at a pivot and a non-pivot connected to the input of the logical Z . Either way, this proves that the stabilizers commute with the logical operations and each other.

We may consider CSS codes in terms of only its Z stabilizers and logical Z operators, which is equivalent to the usual representation of the codes in terms of their Z stabilizers and X stabilizers. From Lemma 5.3.8 and Lemma 5.3.10, the Z stabilizers and logical Z operators can be found directly from the KL form by examining the connections to output Z nodes and input nodes, respectively.

The above construction allows us to easily transform a KL diagram into a stabilizer tableau. The reverse is also easy to accomplish by applying the following procedure. If we start with a stabilizer code, we first compute its Z stabilizers and logical Z operations. We then row-reduce the list of Z stabilizers, identifying the pivot columns. We create n output nodes, with an X node for each pivot of the row-reduced Z stabilizers and a Z node for each non-pivot. Note that these are not the same as the pivot and non-pivot nodes in the context of the adjacencies from the input nodes. Each output node is connected to a free edge and the connections between the Z and X output nodes are made in accordance with the operations in the row-reduced list of Z stabilizers. The list of logical Z operations is then transformed by the stabilizer operations until none of the logical operations have any terms on nodes which are pivots of the stabilizers. The remaining logical operations will only have terms on the Z output nodes, at which point they can be row-reduced and connected to input X nodes, using the row-reduced matrix as an adjacency matrix. This completes the construction of a KL form from a stabilizer tableau.

In some cases, it is possible to further reduce the number of nodes in a diagram in its canonical KLS form. Some of these simplifications are also relevant to the KL form.

Definition 5.3.13. The *reduced KLS form* can be found by completing the following steps:

- (1) We first remove any output nodes of phase zero and degree 2 using the identity removal rule.
- (2) If an output node now has more than one free output edge, is only connected to an input node, and the input node is only connected to this output node, the Hadamards on the output node's free edges can be manipulated so that the topmost free edge of the node has no Hadamard.
- (3) Any input nodes of phase zero and degree 2 may be removed.

The second step to the reduced KLS form can be done by using the Hadamard-sliding rule from Definition C.2 on the output node and a connected input node. Unitary operations that appear on the input node are removed. The output node's free edges all get an additional

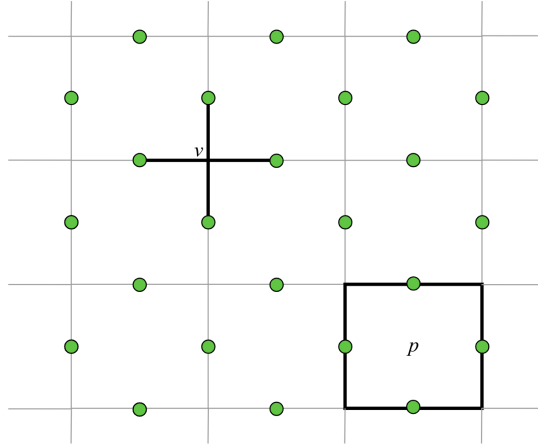


Figure 5.4: A section of the torus. The stabilizers associated with the intersections of the grid such as v have X gates on the nodes immediately surrounding the intersection. The stabilizers associated with the plaquettes such as p have Z gates on the nodes immediately surrounding the plaquette. All nodes are shown in green, but this will change once we add in edges.

Hadamard gate due to the rewrite rule, causing the toggling of Hadamards on all the free edges. Out of the two possible Hadamard configurations, one configuration results in the topmost free edge having no Hadamard gate.

These reduced forms allow for further, albeit limited, reduction of the number of nodes in the KLS form of a Clifford code.

5.4 Toric and surface codes

As an example of the CSS codes explored in the previous section, we now consider toric codes, a specific class of surface codes with periodic boundary conditions, as introduced in [52] and certain surface codes, in the form studied by Kissinger [62]. We first construct a symmetrical form for the toric code starting from Kissinger’s *ZX normal form*, a representation of CSS codes in the ZX-calculus that clearly shows stabilizers using internal nodes representing quantum measurements and shows logical operators using connections from input nodes to output nodes. The ZX normal form generally has fewer edges and long-range connections at the cost of having more nodes. A consequence of Theorem 4.2.5 and its proof in Appendix D is that the KL canonical form can be efficiently derived starting from any equivalent diagram, including the ZX normal form. We also provide the KL forms for some toric and surface codes.

We begin with a definition of toric codes.

Definition 5.4.1. A *toric code* is a quantum error-correcting code that can be represented on a torus \mathcal{T} . For an $m \times n$ toric code, \mathcal{T} is wrapped by m circles along one axis and n circles along another. These circles form an $m \times n$ grid.

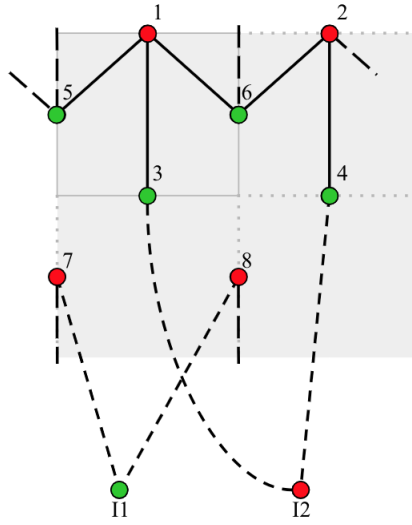


Figure 5.5: A ZX-calculus diagram of the 2×2 toric code. Edges with long dashes represent edges that wrap around the torus. For example, the vertical dashed edge coming from node 5 meets node 7 and the dashed edge from node 2 meets node 5. Edges with short dashes are input-output edges. The free input and output edges are not shown. Note that this diagram is not in KL form, since there is a green input node. It could be transformed into KL form using ZX rewrite rules.

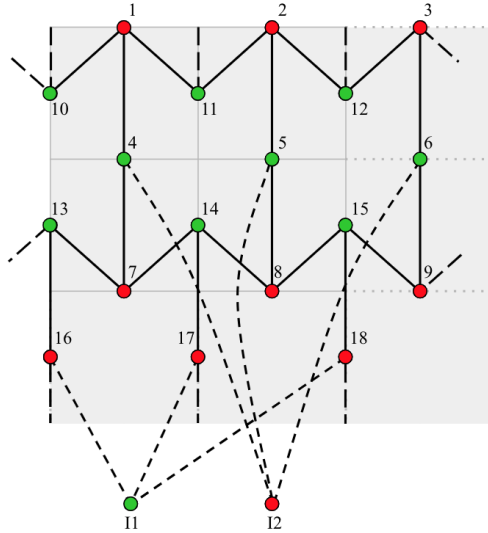


Figure 5.6: A ZX-calculus diagram of the 3×3 toric code. Edges with long dashes represent edges that wrap around the torus. For example, the vertical dashed edge coming from node 10 meets node 16 and the dashed edge from node 3 meets node 10. Edges with short dashes are input-output edges. The free input and output edges are not shown. Note that this diagram is not in KL form, since there is a green input node. It could be transformed into KL form using ZX rewrite rules.

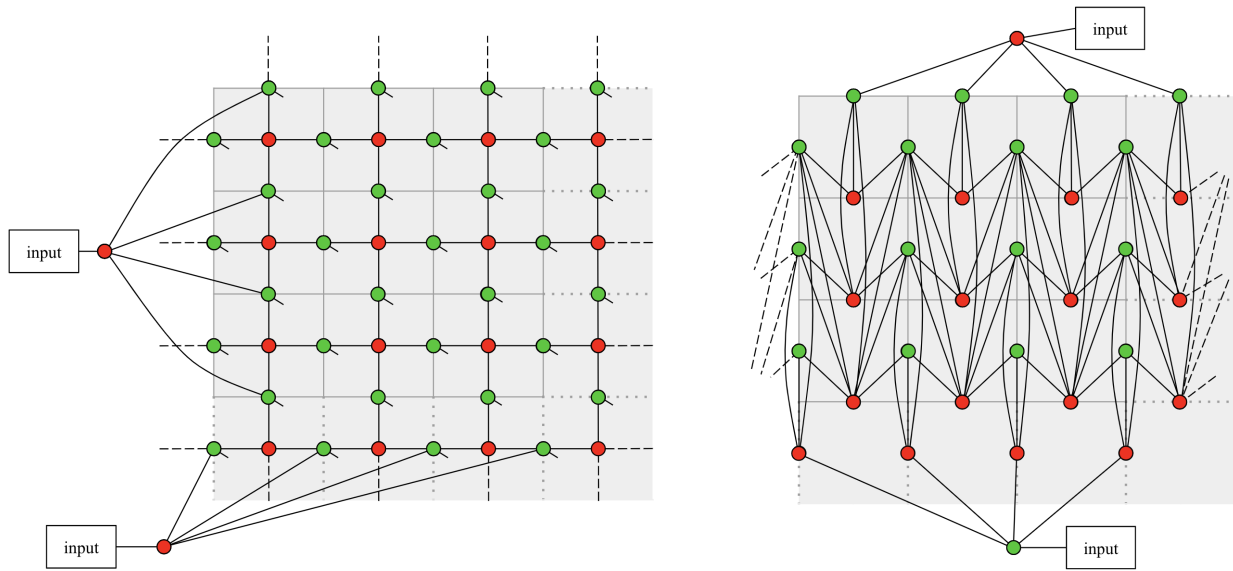


Figure 5.7: The left diagram is the ZX normal form of the 4×4 toric code. The output nodes, which are all the Z nodes, are shown with their free edges. The X nodes in the toric grid are internal nodes. This representation of the code has fewer edges and local connections, at the cost of having internal nodes. The right diagram is a symmetrical form of the 4×4 toric code. There is a symmetry between the X and Z nodes. Though this is not in KL form, it is easily converted into the KL form. This presentation has a minimal set of nodes, one for each input and output free edge, although the edges are not local.

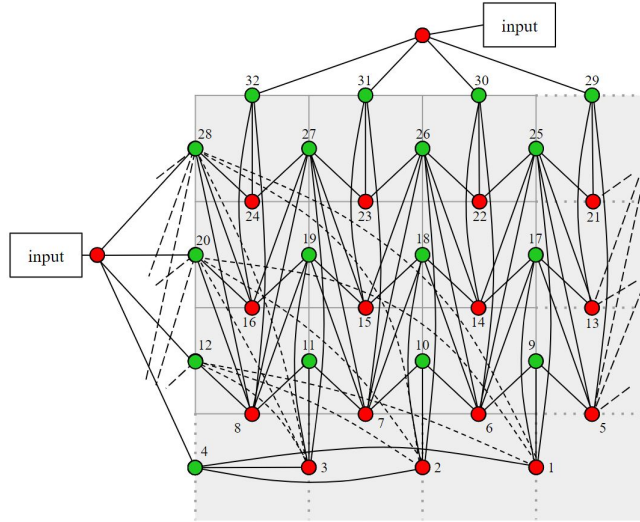


Figure 5.8: The 4×4 toric code in KL form. Long-dashed edges on the left and right edges of the grid wrap around the torus. The curved edges between nodes 1, 2, 3 and nodes 12, 20, 28 are dashed for clarity. The free output edges are not shown.

A node or equivalently, a qubit, is placed at the midpoint of each of the $2mn$ edges on \mathcal{T} . The stabilizers are defined as follows.

The four nodes surrounding each of the mn four-sided faces form a Z check (stabilizer with only Z 's and I 's) consisting of Z 's on these four nodes and I 's on all other nodes.

The four nodes surrounding each of the mn intersections form an X check (stabilizer with only X 's and I 's) consisting of X 's on these four nodes and I 's on all other nodes.

An illustration of these stabilizers are shown in Figure 5.4.

We now determine the structure of the symmetrical forms of the 2×2 and 3×3 toric code's ZX diagram. We do this by using the stabilizers to deduce the output edges with Hadamards and internal edges between output nodes.

We present the ZX-calculus form of the 2×2 toric code in Figure 5.5. This has an arrow-like structure among the output-output edges, as seen by the group of nodes 1, 3, 5, and 6, as well as nodes 2, 4, 5, and 6.

Also, the resulting 3×3 toric code is shown in Figure 5.6, with its full derivation given in Appendix G. Note that by wrapping this pattern around a torus, we see that it is horizontally periodic. The edges among vertices 1, 4, 10, and 11 form an upward-arrow-like structure. Similarly, nodes 2, 5, 11, and 12 form this structure and, on a torus, nodes 3, 6, 10, and 12 do so as well. By the simplicity of this diagram, it is relatively easy to read off the stabilizers by placing gates on the free output edges and seeing how the π -copy rule affects the diagram.

For larger toric codes and the surface codes, we use the ZX-calculus software *Quantomatic* [98] to simplify the known ZX normal form [62] of a code into its canonical form. In our algorithm, the main focus is on performing the bialgebra rule on internal nodes, so that after running the first part of the algorithm all internal nodes will be removed from the diagram, leaving only input and output nodes. Then, the Hadamard sliding rule from

Definition C.2 provides the operation that can repeatedly move Hadamards until the encoder diagram is symmetric.

The procedure we follow may be written as the following algorithm.

- (1) Use basic simplifications, by merging nodes, applying the state-copy rule, applying the Hopf rule, removing scalars, removing loops, or combining two Hadamards into the identity from Definition C.1 and Definition C.2.
- (2) Apply one iteration of the bialgebra rule from Definition C.1 to remove an internal node. If there are no more internal nodes, proceed to step (3). Otherwise, return to step (1).
- (3) Repeatedly apply the Hadamard-sliding rule from Definition C.2 until reaching the desired colours of nodes. It is not the case that any colour configuration can be reached. For example, in the toric code, it turns out that it is impossible for the colours to alternate every row, as one row on either end has the opposite colour from the rows it is connected to.

The reason why we can perform step (2) is due to the fact that after applying the bialgebra rule from Definition C.1 to an internal node, the additional nodes that appear can be merged with other nodes in the graph. If neither of the two nodes the bialgebra rule is applied to is internal, this will not decrease the number of nodes. Thus, while at least one internal node remains in the graph, the number of nodes can be reduced this way.

We now use the above algorithm to derive the general ZX diagram for the $m \times n$ toric code. We begin by presenting our symmetrical form of the 4×4 toric code, which was derived from the ZX normal form. These are both shown in Figure 5.7. As can be seen in the diagrams, the number of output nodes is reduced by a factor of 2, and the diagram in Figure 5.7(b) retains a high degree of symmetry. When moving horizontally, it can be seen that there are periodic patterns of nodes, with one column having 3 Z nodes and 1 X node and the next having 3 X nodes and 1 Z node. Also, the edges between the columns of nodes are local in one direction, as their length does not scale with the horizontal dimension of the toric code.

Using the algorithm on larger dimension $m \times n$ toric codes shows that they have the same general structure as that of Figure 5.7(b). To construct it geometrically, first place an input X node at the top of the diagram and an input Z node at the bottom of the diagram. Then, on the unfolded toric grid, the first and second rows (out of $2n$ rows) of m nodes each are designated as Z nodes. Then, the rows alternate as rows of X and Z nodes until the very bottom two rows of the output nodes, which are rows of X nodes. This is reflected in the 4×4 example.

We now need to identify the diagram's edges. We start by drawing an edge from each of the top row's Z nodes to each of the X nodes within its column. Furthermore, the second row's Z nodes have edges connecting them to each of the X nodes in the neighbouring columns, as well as one edge connecting it to the bottommost X node in the same column. The next row of Z nodes (the fourth row of m nodes from the top) have edges to all the X nodes in the neighbouring columns that are in rows strictly below it, as well as one edge to the bottommost X node in the same column. This pattern follows for the other rows of Z nodes.

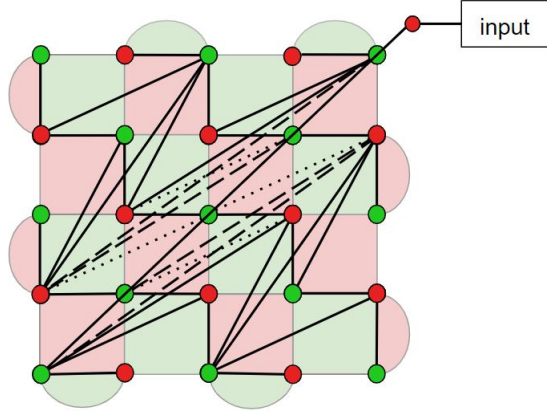


Figure 5.9: A 5×5 surface code in its ZX canonical form. Note its resemblance with the toric code diagram when viewed at a 45° angle. The red input node connects to all 5 Z nodes in the main bottom-left to top-right diagonal. Some edges are dotted or dashed for clarity. The free output edges are not shown.

Since there is a symmetry between the Z and X nodes, we see the same arrow-shaped patterns extending upwards from rows of X nodes.

We convert this symmetrical form of the toric code into its KL form by changing the input Z node into an input X node and keeping the stabilizers the same. This gives Figure 5.8 as the KL form for the toric code, with the numbering reflecting the Hadamard rule.

We also extend our results to the rotated surface codes, shown in Equation (12) from Kissinger [62]. This is a surface code defined such that each face shaded in green represents a Z check while each face shaded in red represents an X check. A Z check consists of Z gates on each of the nodes on the perimeter of the green face, and X checks are similarly defined.

In Figure 5.9, we show the result of simplifying the 5×5 surface code. If it is rotated by 45° counterclockwise, it closely resembles the patterns of edges and colours seen in the general toric code. The neighbouring diagonals (from bottom-left to top-right) of nodes of different colours connect in arrow-shaped patterns, just as in the toric code.

In general, the $(2k + 1) \times (2k + 1)$ surface code can be made to have a similar structure as shown in Figure 5.9.

5.5 Prime codes

When expressed in the ZX-calculus, Clifford codes can have multiple connected components. The tensor product of operations of the connected components is the operation of the entire ZX diagram. For example, any connected component with no free edges is a scalar which scales the tensor of the rest of the diagram. In this section, we consider codes with respect to their connected components.

We note the following statement about ZX diagrams with multiple connected components.

Proposition 5.5.1. *If a ZX diagram has multiple connected components that share no connections between each other, then these components are not entangled. Equivalently, if the*

components are entangled, then they share some connections.

We introduce the notion of *prime* codes, defined as follows.

Definition 5.5.2. A *prime code diagram* is a ZX diagram in KLS form that cannot be expressed as a disconnected graph after a sequence of rewrite rules.

We show the following result about prime codes, which we name the Fundamental Theorem of Clifford Codes (FTCC), analogously to the Fundamental Theorem of Arithmetic.

Theorem 5.5.3 (Fundamental Theorem of Clifford Codes). *Consider a Clifford code with an encoder-respecting form satisfying the constraint that the input-output adjacency matrix is full rank. Then, there exists a unique decomposition of the code into a product of prime codes (up to a permutation of input nodes).*

We prove the FTCC later in this section. To begin, we first prove the following lemma considering the properties of connected components of KLS forms.

Lemma 5.5.4. *The connected components of a KLS form are all prime.*

Proof. Consider a connected component \mathcal{D} in the KLS form of the code \mathcal{C} . Since the adjacency matrix between all inputs and outputs of \mathcal{C} is full-rank and in RREF, the adjacency matrix N between the inputs and outputs of \mathcal{D} has pivot nodes for each of its input nodes. Also, N is full rank, so N must be in RREF. Furthermore, note that any row operations on N preserve the input-pivot connections.

Since the component \mathcal{D} is in RREF, satisfying the RREF rule, and since it is a subgraph of a KLS diagram, it satisfies the Edge, Hadamard, and Clifford rules of Section 4.2.1. Thus, \mathcal{D} must also be in KLS form.

The ZX-calculus is complete for stabilizer quantum mechanics [72] so any two equivalent diagrams can be made equal through a sequence of basic rewrite rules from Definition C.1. The basic rewrite rules of the ZX-calculus that can affect whether two nodes are in the same connected component are the state copy and Hopf rules from Definition C.1. The state copy rule requires an internal node (a node without free edges) connected to exactly one node of the opposite colour. None of the other rules are able to produce such an internal node, so the state copy rule cannot be applied. For example, the bialgebra rule can never cause an internal node to have only one edge. The Hopf rule requires two nodes sharing two edges. Since none of the other basic rewrite rules cause two nodes to share two edges, the Hopf rule cannot be applied either.

We now show that no sequence of row operations on the adjacency matrix N can turn the initial connected graph of \mathcal{D} into disconnected components. For the sake of contradiction, suppose \mathcal{D} is split into multiple connected components due to row operations. Then, row operations can turn each connected component's input-output adjacency matrix into RREF, so the adjacency matrix for \mathcal{D} is disconnected and (after appropriate input permutations) in RREF. Since N was initially connected and in RREF, and the RREF is unique, we reach a contradiction. Thus, no sequence of row operations on N can turn \mathcal{D} into disconnected components.

Therefore, all the nodes in \mathcal{D} are always in the same connected component. Since \mathcal{D} is in KLS form and it cannot become disconnected, \mathcal{D} is prime.

Since \mathcal{D} was chosen arbitrarily, this implies that the connected components of a KLS form are all prime. \square

The encoders considered below will always be in encoder-respecting form. We now go through the process of converting an arbitrary encoder into its KLS form to show that the end result is the same had we converted two disconnected components into KLS, possibly having to rearrange the input nodes. As defined in Appendix D, the *ZX-HK form* is an intermediate form of a code that satisfies the Edge and Hadamard rules for KLS forms, but not necessarily the RREF or Clifford rules.

Lemma 5.5.5. *If \mathcal{X} is an arbitrary Clifford encoder in the ZX-calculus, let $KLS(\mathcal{X})$ denote its KLS form in the ZX-calculus. If an encoder \mathcal{C} can be decomposed into components \mathcal{A} and \mathcal{B} , where there are no edges between the components, then $KLS(\mathcal{C})$ can be decomposed into components $KLS(\mathcal{A})$ and $KLS(\mathcal{B})$, again with no edges between the components.*

Proof. As we saw in Appendix D, the conversion from an arbitrary encoder-respecting form to the KLS form involves only irrelevant unitaries on inputs, local complementation, and row operations on the input-output adjacency matrix.

Transforming a code into its ZX-HK form relies only on local complementations in Equation (3.13), Equation (3.15), and Equation (3.16). Since local complementation only toggles edges of the neighbours of a node, it cannot affect whether two nodes are in the same connected component, since any vertices it might disconnect will always neighbour the node about which the local complementation is applied. Thus, if the ZX-HK form of the encoders are \mathcal{A}' , \mathcal{B}' , and \mathcal{C}' , respectively, we find that \mathcal{C}' can be decomposed into components \mathcal{A}' and \mathcal{B}' , with no edges between the components, since local complementation happens entirely within the components.

The next step is to transform the ZX-HK form's adjacency matrix between the input and output nodes into RREF. When transforming \mathcal{C}' into RREF, note that we can first transform the separate components \mathcal{A}' and \mathcal{B}' into RREF. Each input node of \mathcal{C}' has a corresponding pivot node. Then there exists a permutation of the inputs that will result in \mathcal{C}' being in RREF if we order the inputs to match the order of the pivots. Permuting can be done by row operations. Since the RREF of the adjacency matrix is unique, this is the desired RREF for \mathcal{C}' . Note that the resulting diagram \mathcal{C}'' can still be decomposed into components \mathcal{A}' and \mathcal{B}' , with no edges between the components. This is because the order of the inputs within each component is unchanged.

The next step in converting into KLS form involves local complementing at the inputs of pivot nodes. Then, if there are edges between pivot nodes in the resulting form, we perform local edge complementations on the corresponding input nodes, followed by a permutation of the same input nodes. The former does not affect whether two nodes are in the same connected component. The latter also does not alter this property because local complementation does change graph connectivity and the input-output adjacency matrix is preserved in RREF after the permutation. This completes the transformation into the KLS form.

Thus, we have shown that $KLS(\mathcal{C})$ can be decomposed into components $KLS(\mathcal{A})$ and $KLS(\mathcal{B})$, which share no edges. \square

Note that the output nodes of \mathcal{A} and \mathcal{B} remain the same after transforming them into KLS form. Thus, ordering the inputs of $\text{KLS}(\mathcal{A})$ and $\text{KLS}(\mathcal{B})$ so that they match with the ordering of the pivot output nodes, the resulting diagram is the same as $\text{KLS}(\mathcal{C})$.

Next we show why equivalent Clifford encoders share the same set of prime components.

Theorem 5.5.6. *Given two Clifford encoders with the same codespace, each entirely made up of prime components, they have equivalent ZX diagrams up to a permutation of the inputs.*

Proof. First, we note that two encoders with the same codespace must have the same KLS form. Therefore, the statement is equivalent to showing that, given a Clifford encoder \mathcal{C} entirely made up of prime components, its ZX diagram is equivalent to the KLS form up to a permutation of inputs.

We now induct on the number of prime components in \mathcal{C} . If \mathcal{C} has exactly one prime component, then its entire diagram must be in KLS form. Since the KLS form for \mathcal{C} is unique, this means \mathcal{C} and its KLS form are identical, and thus equivalent up to a permutation of inputs.

Now, suppose all encoders with $i \leq n$ prime components are equivalent to their KLS form up to a permutation of inputs. We want to show that this implies any encoder \mathcal{C} with $n + 1$ prime components is equivalent to its KLS form up to a permutation of inputs.

Denote the connected component of \mathcal{C} that has output node 1 as \mathcal{A} . Then, the remaining part of \mathcal{C} that shares no edges with \mathcal{A} can be denoted as \mathcal{B} . Note that \mathcal{A} is already in KLS form, since \mathcal{A} must be prime. By the inductive hypothesis, we have that \mathcal{B} is equivalent to $\text{KLS}(\mathcal{B})$ up to input permutations, so, after an appropriate sequence of rewrite rules, \mathcal{C} can be decomposed into \mathcal{A} and $\text{KLS}(\mathcal{B})$.

By Lemma 5.5.5, we have that $\text{KLS}(\mathcal{C})$ can be decomposed into $\text{KLS}(\mathcal{A})$, which is just \mathcal{A} , and $\text{KLS}(\mathcal{B})$. This proves that \mathcal{C} is equivalent to $\text{KLS}(\mathcal{C})$ up to input permutations. □

Now, we prove the Fundamental Theorem of Clifford Codes.

Proof of Theorem 5.3 (FTCC). We begin with a Clifford code with an encoder-respecting form satisfying the constraint that the input-output adjacency matrix is full rank. Then, after converting it into its KLS form, Lemma 5.5.4 gives that all its connected components are prime. Therefore, we have constructed a decomposition of the code into primes.

Now, we show why this construction is unique. For the sake of contradiction, suppose there is another different decomposition of the code into primes. Then, by Theorem 5.5.6, these two ZX diagrams are equivalent up to a permutation of inputs. Note that we can rearrange the inputs at will using row operations without changing the structure of any of the primes, so this second decomposition must be the same as the one constructed above.

Thus, the decomposition exists and it is unique. □

5.6 Another definition of equivalence

Previous works have examined the equivalence classes of graphs under local complementation [89, 99, 100]. In Clifford codes, the presence of designated input and output vertices makes the definition of equivalence more exotic.

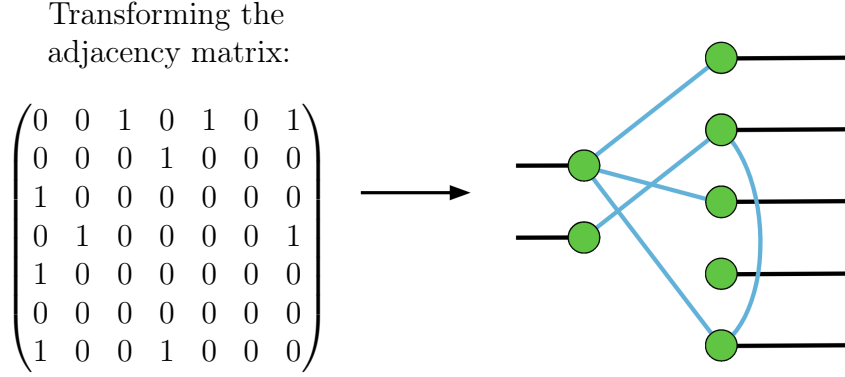


Figure 5.10: In the adjacency matrix, the first row corresponds to the first input, the second row corresponds to the second input, and so on. After the inputs, the following row corresponds to the first output, and the other outputs follow. The same applies for the columns as well as the rows. We see that the matrix is symmetric, as an adjacency matrix should be. In the ZX diagram on the right, we see the ZX encoder for the graph code with the given adjacency matrix.

In the following sections, we consider only the ZX diagrams for Clifford codes that have no local operations on the free output edges. Such codes are exactly represented as graphs as discussed in Chapter 4.

Definition 5.6.1. Two ZX diagrams are *locally equivalent* if and only if one can be converted to the other through a sequence of local complementations and local operations on the free output edges.

We now provide another definition of equivalence that turns the focus to the topological structure of the code, letting us ignore specific orderings of output nodes and the local operations attached on the free output edges.

Definition 5.6.2. We say that two Clifford codes \mathcal{C}_1 and \mathcal{C}_2 are *equivalent* if and only if their ZX diagrams are locally equivalent up to some permutation of the output nodes or applications of any unitary operators on the inputs.

We now list six operations which preserve encoder graph equivalence. We conjecture that this is a list of equivalent operations generates all others.

Conjecture 5.6.3. The ZX diagrams for two Clifford codes \mathcal{C}_1 and \mathcal{C}_2 are *equivalent* if and only if the diagram for one of the codes can be reached from the other after a sequence of operations consisting only of the following:

- (1) Applying a local complementation about any vertex of the graph.
- (2) Permuting the output vertices.
- (3) Permuting the input vertices.

- (4) Performing row operations on the adjacency matrix of input to output edges.
- (5) Removing an input-input edge.
- (6) Applying local operations on the output edges.

All of the operations in Conjecture 5.6.3 are reversible, so, if code \mathcal{C}_1 can be made equivalent to \mathcal{C}_2 , the reverse is also true.

Operation (1), local complementation as in Definition 3.2.1, is included to account for equivalence of encoder graphs based on their entanglement [89]. Additionally, local complementation can be performed on a graph by applying the correct sequence of local operations and applying Equation 3.11.

Two encoder diagrams should also be equivalent if the information they produce can be ordered differently to become the same. In this way, operations (2) and (3) reflect this, since connections among the vertices of the graph remain the same and these operations only change the order in which the information is inputted or outputted.

Operation (4) consists of adding rows of the adjacency matrix between input and output nodes in modulo 2. As discussed in Appendix D, this operation is equivalent to applying a controlled- X gate between two inputs, thus preserving the equivalence of the encoder. Similarly, operation (5) applies a controlled- Z operation to the inputs. Both of these are allowed by Definition 5.6.2. Lastly, operation (6) preserves equivalence since all local operations can be removed by multiplying by their corresponding conjugate, which is allowed by Definition 5.6.1.

We have thus shown one of the directions of Conjecture 5.6.3.

Note that this definition of equivalence does not allow two encoders to be in the same equivalence class if they only differ by an extra output which is not connected to anything else. That is, if the two encoders perform the same encoding, but one appends an additional fixed output state, this definition of equivalence marks them as different.

An example of these extra outputs is shown in Figure 5.10. The fourth output vertex is not connected to any input or output. It does not provide any more encoding of information from the inputs than if it was not present. For this reason, removing extra states is more useful for practical purposes.

There are some simplifications that can be made on the set of encoders we consider by using the above operations. This is so that we consider only encoder graphs that could possibly be non-equivalent.

We can now try to use these operations to find equivalences between prime codes. These operations allow us to impose conditions on selecting representative elements of equivalent codes. Operations (3) and (4) of Conjecture 5.6.3 allow the input-to-output portion of the encoder diagram to be expressed in RREF. All encoder diagrams considered from here on will be expressed already satisfying the RREF rule from Section 4.2.1.

Continuing from the RREF of the encoder graph, operation (2) from Conjecture 5.6.3 can be used to move the pivot nodes to have lower-numbered indices than all the other outputs. In this way, the first output node can be made into the pivot node corresponding to the first input node, the second output node can be made into the pivot node corresponding to the second input node, and so on. Thus, these k pivot nodes are fixed as the first k output nodes. For brevity, the other $n - k$ non-pivot output nodes are called *free* output nodes.

In Conjecture 5.6.3, we could freely manipulate local Clifford gates at nodes. Therefore, for our purposes, we remove all local Clifford gates present at the nodes of the ZX diagram for the encoder, just like in the graph codes studied in Chapter 4.

A further simplification is that graphs with pivot-pivot edges are omitted, since they can always be transformed into a graph without pivot-pivot edges using a sequence of local complementations.

We group these simplifications into the following result.

Claim 5.6.4. *To find the distinct encoders in an equivalence class of the set of Clifford codes, it is sufficient to find the distinct encoders in the equivalence class satisfying the following constraints:*

- *The input-output adjacency matrix is in RREF.*
- *The pivot nodes are the lowest-numbered output nodes, and they are ordered to match the order of the input nodes.*
- *Local Clifford gates on the free output edges are all removed, leaving only output Z nodes with phase 0.*
- *Diagrams with pivot-pivot edges are not included.*

An example of the simplifications on the diagrams as well as how the adjacency matrices transform into encoders is shown in Figure 5.10.

5.7 Tabulations from code

Keeping in mind the new definition of equivalence and the simplifications made on the set of Clifford encoder graphs being considered, we now sort the encoders into their equivalence classes. To do this, we used the disjoint set algorithm to split encoders into equivalence classes based on whether an operation from Conjecture 5.6.3 caused one encoder to change into another.

Each encoder graph is converted into an integer based on the *variable* edges present in the graph, which are the input-free edges, pivot-free edges, and free-free edges. Note that the input-pivot, input-input, and pivot-pivot edges are fixed, so these are not included among the variable edges.

The variable edges' values in the adjacency matrix are made into a single integer a using binary representation. Note that this adjacency matrix includes all vertices, so it is a $(n + k) \times (n + k)$ matrix.

For example, in the $\mathbb{J}_5, 2\mathbb{K}$ codes, the 7×7 adjacency matrix would look like the following:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & a_{14} & a_{13} & a_{12} \\ 0 & 0 & 0 & 1 & a_{11} & a_{10} & a_9 \\ 1 & 0 & 0 & 0 & a_8 & a_7 & a_6 \\ 0 & 1 & 0 & 0 & a_5 & a_4 & a_3 \\ a_{14} & a_{11} & a_8 & a_5 & 0 & a_2 & a_1 \\ a_{13} & a_{10} & a_7 & a_4 & a_2 & 0 & a_0 \\ a_{12} & a_9 & a_6 & a_3 & a_1 & a_0 & 0 \end{pmatrix}$$

$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
1	1	2	6	17

(a) Number of equivalence classes for $J_n, 1K$ codes.

Rep:	
Size:	3

(b) $J_2, 1K$ code equivalence class representatives and sizes.

Rep:		
Size:	3	21

(c) $J_3, 1K$ code equivalence classes showing the size of the class underneath a representative.

Rep:						
Size:	3	30	45	54	84	198

(d) $J_4, 1K$ code equivalence classes showing the size of the class underneath a representative.

Rep:						
Size:	3	39	78	84	84	
	204	297	306	315	360	540
	558	1332	1404	2376	3024	3276

(e) $J_5, 1K$ codes equivalence classes showing the size of the class underneath a representative.


Figure 5.11: (a) shows the number of equivalence classes for $J_n, 1K$ encoder graphs. (b-e) show an element of the equivalence classes to denote the representative of the class and gives the size of the class. We only consider classes in which every graph is prime.

The top-left 4×4 submatrix reflects the fixed input-pivot edges, as well as the lack of input-input edges and pivot-pivot edges. The terms a_i are the binary digits of a . We place a_0 near the bottom-right corner and fill in the rows above from right to left.

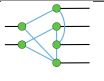
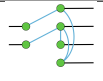
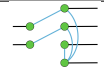
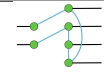
After converting the ZX diagrams into integers, we use the disjoint set algorithm, which is useful for separating the whole set of possible encoder graphs into equivalence classes.

$n = 2$	$n = 3$	$n = 4$	$n = 5$
0	1	4	18

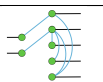
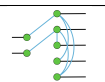
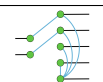
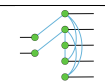
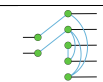
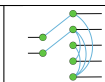
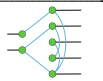
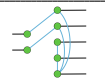
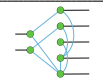
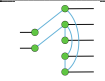
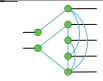
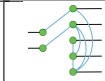
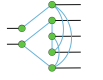
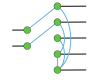
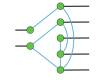
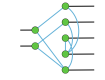
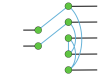
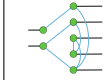
(a) Number of equivalence classes for $J_n, 2K$ codes.

Rep:	
Size:	9

(b) $J_3, 2K$ codes equivalence class reps. and sizes.

Rep:				
Size:	36	45	99	234

(c) $J_4, 2K$ codes equivalence classes showing the size of the class underneath a representative.

					
63	108	144	414	459	486
					
540	972	1080	1080	1152	1188
					
1620	2268	2484	4896	5184	5832

(d) $J_5, 2K$ codes equivalence classes showing the size of the class underneath a representative.

Figure 5.12: (a) shows the number of equivalence classes for $J_n, 2K$ encoder graphs. (b-d) show an element of the equivalence classes to denote the representative of the class and gives the size of the class. We only consider classes in which every graph is prime.

The code takes an integer representation, say a , of an encoder graph, performs one operation from Conjecture 5.6.3 on the encoder graph, then merges the disjoint sets of a and the integer representing the resulting encoder graph. All possible such operations are applied, and the resulting values are merged with a 's disjoint set.

When a local complementation is performed on a free output, it is possible that an input-pivot edge is removed. Furthermore, some input-input edges could be added. To fix this, we first employ operation (5) from Conjecture 5.6.3 to set all input-input edges to 0. Then, operations (3) and (4) are used to turn the submatrix representing the input-to-output adjacency matrix into RREF. Operation (2) is used to put the pivots back into their fixed positions, so they once again correspond to their input vertices.

The results of the code are shown in Figure 5.11 and Figure 5.12. We have only shown

the equivalence classes that have a single connected component, similar to the prime codes discussed in Section 5.5. The equivalence classes with multiple connected components can always be built up from connected components of smaller sizes, and finding these classes reduces to finding ways to partition the graph into groups of nodes within connected components. As shown in Figure 5.11(a) and Figure 5.12(a), the number of equivalence classes increases quickly as the number of output vertices increases.

For the $J_n, 1K$ codes, the number of equivalence classes for $n = 1$ through 4 are $(n - 1)!$. However, this pattern seems to break for larger values of n . Furthermore, for the $J_n, 2K$ codes, the number of equivalence classes for $n = 2$ through 5 are $(n - 2) \cdot (n - 2)!$. It is possible that these patterns for small n arise from the number of ways to permute the non-pivot output nodes.

Furthermore, in Figure 5.11(b-e) and Figure 5.12(b-d), the equivalence classes show a variety of sizes, with many of the sizes having a factor of 3 or 9. The values of the sizes generally have many divisors, suggesting nice combinatorial patterns.

We make the following conjecture regarding the recurring factors of 3 and 9.

Conjecture 5.7.1. For positive integers $n > k$, the equivalence classes of J_n, kK codes with a single connected component have sizes divisible by 3^k .

Note that the factor of 9 is shared across the sizes of the equivalence classes of encoder graphs for the $J_3, 2K$, $J_4, 2K$, and $J_5, 2K$ codes. Similarly, there is a common factor of 3 across the sizes for the $J_2, 1K$, $J_3, 1K$, $J_4, 1K$, and $J_5, 1K$ codes. Also, based on the diagrams in Figure 5.11(b) and Figure 5.12(b), an analogous diagram can be drawn for $J_4, 3K$ codes, with the free output node having an edge to each pivot node. The resulting diagram is in a class of size 27 because each input-pivot pair has three different ways to share edges with the free node. Note that this is also the only class with prime graphs among $J_4, 3K$ codes. Thus, for $J_n, n - 1K$ codes, there is a clear way to see why the analogously constructed graphs have a class size of 3^{n-1} . In general, we speculate that a factor of 3 arises from each input-pivot pair and the effects of different local Clifford gates among $\{I, Z, S, SZ, H, HZ\}$ when applied on the pivot free edge. If this holds, then all equivalence classes for J_n, kK codes for $n > k$ would have sizes divisible by 3^k .

5.8 Equivalence classes with bipartite forms

When an equivalence class for an J_n, kK code contains a bipartite graph, we can choose to narrow our search for a canonical form to bipartite forms. These graphs are simpler, with no edges among output nodes, making them good candidates as canonical forms for these equivalence classes. We now turn to setting criteria for selecting a specific bipartite form in an equivalence class that could serve as a simple representative.

First, consider the case of $J_4, 2K$ codes. An example of the input-output adjacency matrix of a bipartite form, taking into account the RREF and pivot simplifications from Section 5.6, could look like:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

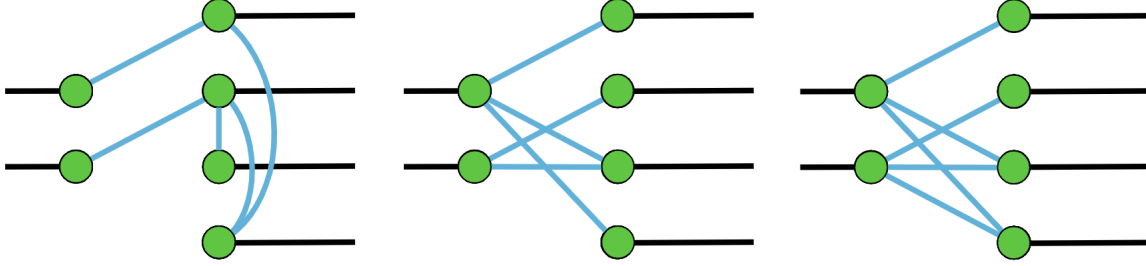


Figure 5.13: Three graphs from the same $J_4, 2K$ code equivalence class. The representative graph is shown on the left. The other two graphs are both bipartite forms.

By considering all possible combinations of 0's and 1's for the values of the bolded entries, there are 16 possible bipartite forms among all $J_4, 2K$ codes.

Per the discussion on prime codes in Section 5.5, we will be considering codes that cannot be disconnected. In this section, codes that cannot be disconnected are called *connected*.

Proposition 5.8.1. *Among all connected $J_4, 2K$ bipartite ZX diagrams, there is only 1 distinct diagram up to equivalence through operations 2 through 4 from Conjecture 5.6.3.*

Proof. There are 16 total possible input-output adjacency matrices for $J_4, 2K$ bipartite codes, since there are 2^2 ways for each input to connect to free outputs. If there are two or fewer input-to-free output edges, then either an output node is alone or the input nodes are in separate connected components.

Then, there are only 5 possible input-output adjacency matrices in this case:

$$\begin{aligned} & \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}. \end{aligned}$$

Consider the first matrix above. Switching the third and fourth output vertices (corresponding to the third and fourth columns of the matrix) results in

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

which is the second matrix. From here, we use operation 4 to replace the first row with the sum of the first and second rows modulo 2:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Permuting the outputs achieves the third and fourth matrices. Lastly, starting from the above matrix, we use operation 4 to replace the second row with the sum of the current first

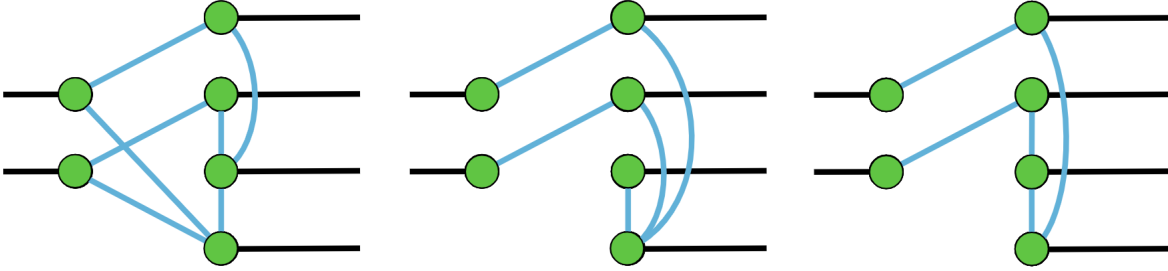


Figure 5.14: The representatives of the three different equivalence classes lacking bipartite forms among the classes for $\mathbb{J}4, 2\mathbb{K}$ ZX diagrams.

and second rows modulo 2 to find

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

This can be permuted to give the fifth matrix. Analogous sequences of operations can bring any of the other matrices to another, so all 5 of the graphs are equivalent, as desired. \square

From Proposition 5.8.1, the representative form for the equivalence class that contains these 5 adjacency matrices is chosen to be

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Note that this graph has the property of having the fewest edges. We can break ties between the four matrices with the fewest edges by selecting the graph with more edges on the first input and first output.

By writing one of these input-to-output adjacency matrices as a full 6×6 matrix, we produce its ZX diagram. In Figure 5.13, the ZX diagram of the above matrix is shown in the center and the representative of the diagram's equivalence class from Figure 5.12 is shown to the left. The rightmost ZX diagram is another bipartite form in the same equivalence class.

Now, we present a general method of simplifying a bipartite $2 \times n$ input-to-output adjacency matrix.

Proposition 5.8.2. *Consider a $\mathbb{J}n, 2\mathbb{K}$ encoder graph equivalent to some bipartite form. It is also equivalent to a bipartite form where the two inputs are both connected to at most $\lfloor \frac{n}{2} - 1 \rfloor$ of the same free outputs.*

Proof. In this proof, we only consider encoders that are equivalent to a bipartite form.

For the sake of contradiction, suppose all bipartite forms of this equivalence class have at least $\lfloor \frac{n}{2} \rfloor$ shared free outputs. In an input-to-output adjacency matrix, this would look like

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The first two columns are fixed to be input-pivot edges, as usual. If there are at least $\lfloor \frac{n}{2} \rfloor$ shared free outputs, the other $n - 2$ columns must have a majority of columns containing two 1's. In this example, 3 out of 5 columns contain two 1's.

However, using operation 4 from Conjecture 5.6.3, the top row can be replaced with the sum of the top and bottom row modulo 2.

Note that this means all the free outputs that were shared by both inputs have their edges with the first input disconnected, so at least $\lfloor \frac{n}{2} \rfloor$ columns do not have two 1's.

Furthermore, after the operation, the first column cannot possibly have two 1's, so one additional column does not have two 1's. The example matrix above turns into

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

We can rearrange output vertices to bring back the pivots. The matrix is thus equivalent to

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

We can rearrange output vertices to bring back the pivots. The matrix is thus equivalent to

Thus, the maximum number of columns with two 1's is now $n - 1 - \lfloor \frac{n}{2} \rfloor$. However,

$$n - 1 - \lfloor \frac{n}{2} \rfloor < \lfloor \frac{n}{2} \rfloor,$$

so we reach a contradiction, since there are now fewer than $\lfloor \frac{n}{2} \rfloor$ shared free outputs in an equivalent bipartite form.

Therefore, the claim holds. □

Proposition 5.8.2 demonstrates that we can choose a bipartite form that has a relatively small number of shared free outputs. In fact, if the top row is the horizontal vector \mathbf{a} and the bottom row is the horizontal vector \mathbf{b} , by linear operations, there are only 3 possibilities of unordered combinations of two vectors in the rows. They are (\mathbf{a}, \mathbf{b}) , $(\mathbf{a} + \mathbf{b}, \mathbf{b})$, and $(\mathbf{a} + \mathbf{b}, \mathbf{a})$. Lastly, we choose which of these bipartite forms has the fewest shared free outputs and thus minimizes this number.

In an attempt to show the uniqueness of the bipartite forms in an equivalence class, we conjecture the following, which would allow for an efficient way to check whether two bipartite forms are equivalent.

Conjecture 5.8.3. In an equivalence class that contains bipartite forms, all bipartite forms in the class can be transformed from one to another using only output permutations, input permutations, and row operations on the input-output adjacency matrix.

One straightforward approach starts by assuming for the sake of contradiction that two bipartite graphs, G_1 and G_2 , are equivalent even though they cannot be transformed from one to another using only the three operations in Conjecture 5.8.3. A contradiction could be reached if we are able to show that the entanglement between two of the nodes is different in the diagrams. Quantifying the entanglement could be possible using the partial trace.

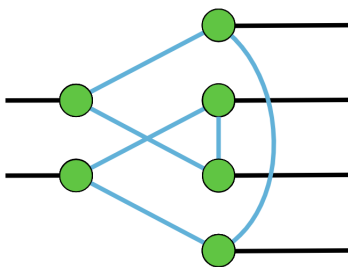


Figure 5.15: A ZX diagram with the minimum number of output-output edges in its equivalence class. The equivalence class has no bipartite forms and does not contain any ZX diagrams with 0 output-output edges or 1 output-output edge.

Besides equivalence classes with bipartite forms, there are also some classes that do not have bipartite forms. Among the equivalence classes of $J_4, 2K$ codes from Figure 5.12, five of the classes have zero bipartite forms. Three of these classes have connected graphs, and they are shown in Figure 5.14. Finding a clean, representative form for these classes is less intuitive, but analyzing a few other graphs in these equivalence classes could give a clue as to what to choose. For example, Figure 5.15 shown above could be a better representative for the equivalence class containing the leftmost diagram in Figure 5.14. Figure 5.15 is symmetric, and it has the fewest output-output edges.

5.9 Conclusion

This chapter presented our work on producing the KL canonical forms for CSS codes, extending the work done in Chapter 4. Furthermore, we showed the resulting KL canonical forms of the toric code and certain surface codes. Additionally, we introduced the notion of prime codes and proved the Fundamental Theorem of Clifford Codes. We tabulated results found when considering codes with much looser equivalence conditions, and we analyzed possible representative forms, such as bipartite forms, for the equivalence classes found.

Chapter 6

Conclusion

In this thesis we improved the results of García, Markov, and Cross [45] by deriving a simpler graph merging formula and by completely characterizing linearly dependent triplets of stabilizer states. Both our characterization in terms of extended graph states and in terms of inner products reveal much structure in the additive properties of stabilizer states that can possibly be generalized. Future work can continue characterizing linearly dependent n -tuples of stabilizer states for $n \geq 4$ as well as stabilizer decompositions of magic states [29, 32, 36, 37], using the graph formalism.

Our results on stabilizer states, general Clifford codes, and CSS codes find an elegant, minimal form in the ZX-calculus for these quantum operations. From Kissinger [62], it was known that phase-free ZX diagrams are CSS codes, but now we have shown an optimal and unique representation, reducing the number of nodes to have one per input and output. In code search, it is sufficient to consider just one representative from each equivalence class, meaning a sufficiently good classification of canonical forms can massively improve our ability to discover new codes.

Additionally, we showed that graph properties are intimately tied to code properties. Key code properties such as weight, distance, encoding and logical operator circuit depths are all controlled by small linear functions of graph degrees. Furthermore, key coding algorithms such as distance approximation, weight reduction, decoding are all strategies on various instances of quantum lights out (QLO) games. The former observation allowed us to leverage graph algorithms to efficiently construct encoding circuits with controlled depth upper bounds as well as build logical operation circuits whose depths, in the case of diagonal or certain Clifford gates, are conceptually distinct and quantitatively better than simply unencoding, applying, and re-encoding. The latter result led us to design an efficient greedy QLO strategy for decoding, and prove that it succeeds up to a small constant factor on at least a certain class of graphs which include the hypercube code. We believe that further study in graph-based decoding algorithms will reveal efficient decoders for many other families of graphs. Altogether, the universal graph representation enables insights and improvements that are general across all or large classes of stabilizer codes by providing avenues of construction and analysis that are substantially less obvious via conventional representations of additive quantum codes.

There are several directions in which to explore from this point. The first is general. Classically, graph representations have shown a strong correspondence between graph properties

and code properties beyond simple objects like the degree. Notably, spectral expander graphs have led to good classical codes. A characterization effort connecting graph properties such as spectrum, expansion, cycle sizes, density, geometry, and topology to distance, decoding, stabilizer weight, etc. could significantly extend our insights into stabilizer codes. It is also worthwhile to more deeply study the quantum lights out game, as insights onto their strategies have equivalent interpretations on coding algorithm performance. First steps towards the worst- and average-case analysis of coding algorithms based on the hardness of certain computational problems have appeared recently [101], and their connection to QLO is an interesting question.

A second direction is directly constructive. Given particular architectures or algorithms of experimental interest, is it possible to systematically design graphs whose codes are particularly suitable for such devices or algorithms in terms of locality of connectivity, geometry, rate, and distance?

The third direction involves refining the approaches used in this thesis. It would be useful to investigate if there exists a collection of graphs that, in exchange for representing a restricted subset of stabilizer codes, have low-weight stabilizers. Such an approach may open new paths forward for practical code constructions and corresponding algorithms and would lie in an optimal middle ground between the approach of surface-type code constructions and the universal graph representation. Additionally, the behaviour of graphs, and more importantly, graph codes, under logical and physical non-Clifford operations could be studied more closely. In particular, there likely exist elegant formulas for manipulating linear combinations of graphs to apply non-Clifford gates, allowing for the study of universal fault-tolerant quantum computation.

Appendix A

Stabilizer rank of magic states

Here we discuss a first attempt at finding upper bounds on the stabilizer rank of n -qubit magic states by using the graph formalism. Magic states are special non-Clifford states which allow one to implement non-Clifford gates in a fault tolerant manner [27].

Definition A.1. An n -qubit magic state $|T_n\rangle$ is the state $|T\rangle^{\otimes n}$, where $T := \frac{|0\rangle + e^{\frac{\pi i}{4}}|1\rangle}{\sqrt{2}}$.

We recall from Definition 2.3.3 that the *stabilizer rank* $\chi(|\psi\rangle)$ of a state $|\psi\rangle$ is the smallest integer χ such that there exists a set of χ stabilizer states S such that $|\psi\rangle \in \text{span}(S)$.

The stabilizer rank of a magic state is deeply tied to the runtimes of classical simulations of quantum circuits and has been explored extensively [29, 32, 37]. In order to tighten the upper bounds on $\chi(|T_n\rangle)$, a Metropolis-Hastings numerical search algorithm that applies random transformations to stabilizer states to maximize the projection of the magic state onto their span was developed [32]. An attempt at experimenting with different variations of this method did not yield any stabilizer decompositions for larger numbers of qubits, due to the extremely large search space. Another method, introduced in [36], uses *cat states* and *contractions*. The method produced the improved upper bounds on $\chi(|T_n\rangle)$ by finding a rank 3 decomposition of the 6-qubit cat state to be found by inspection. Since two cat states can be combined into a magic state, this allowed for a 6-qubit decomposition of $\chi(|T_6\rangle)$. Additionally, by combining rank 3 decompositions of cat states and tracing out a qubit to join, this gave an asymptotic upper bound equivalent to finding a rank 3 decomposition of $\chi(|T_4\rangle)$.

We showcase these decompositions in the graph formalism, which we used to represent the n -qubit magic state, $(T|+)\rangle^{\otimes n}$. It is written as a linear combination of extended graph states written in the canonical form from Definition 3.3.2. By comparing pairs of extended graph states, we can examine whether they can be merged together into a single state by using Theorem 3.5.3. While we were able to express the n -qubit magic state as a sum of $2^{\frac{n}{2}}$ stabilizer states, it then proved impossible to simplify further simply by combining two stabilizer states into one. Future work could try to develop more general merging criteria and formulas involving more than three extended graph states. Then, a computer might be able to follow a heuristic with simulated annealing or any other optimization algorithm. In order to find such a heuristic, it would be useful to study properties of sums of extended graph states that provide more insights into the structure of low-rank stabilizer decompositions.

To find patters in known optimal stabilizer decompositions, we convert the stabilizer decompositions found in [29, 36] into canonical form.

We provide examples of stabilizer decompositions for two special cases, $n = 3$ and $n = 6$. Let $S_{n,v}$ be the star graph on n vertices with central vertex v , where the only edges are those of the form (u, v) for all vertices $u \neq v$. Let K_n be the complete graph on n vertices and let I_n be the empty graph on n vertices.

$$|T_3\rangle = \frac{i - e^{\frac{i\pi}{4}}}{2} Z_1 Z_2 Z_3 |I_3\rangle + \frac{1 + e^{\frac{i\pi}{4}}}{2} H_1 H_2 S_3 |S_{3,3}\rangle - \frac{i + e^{\frac{i\pi}{4}}}{2} Z_1 Z_2 Z_3 |K_3\rangle \quad (\text{A.1})$$

$$\begin{aligned} |T_6\rangle = & -\frac{i}{2} H_1 Z_1 S_2 S_3 S_4 S_5 S_6 |S_{6,1}\rangle + \frac{e^{\frac{3i\pi}{4}}}{2} H_1 |S_{6,1}\rangle \\ & + \frac{e^{\frac{i\pi}{4}}}{2\sqrt{2}} H_1 Z_1 H_2 H_3 H_4 H_5 Z_6 |S_{6,6}\rangle + \frac{1}{2\sqrt{2}} H_1 H_2 H_3 H_4 H_5 S_6 Z_6 |S_{6,6}\rangle \\ & - \frac{1}{2} H_1 S_2 Z_2 S_3 Z_3 S_4 Z_4 S_5 Z_5 S_6 Z_6 |K_6\rangle - \frac{e^{\frac{i\pi}{4}}}{2} H_1 Z_2 Z_3 Z_4 Z_5 Z_6 |K_6\rangle \end{aligned} \quad (\text{A.2})$$

Even for the 3-qubit case, there are multiple ways to decompose the magic state into 3 stabilizer states, yet in all of the ways, there seems to be an empty graph, a complete graph, and a star graph. In fact, the star graph can be transformed into a complete graph through local complementation. The same is true for star graphs in the expression for $|T_6\rangle$. This means that a search for magic state decompositions could just involve applying various local Clifford operators to complete and empty graphs.

For completeness, we give the representations of the 3-qubit and 6-qubit magic states using only empty and complete graphs. Note that these are not in canonical form.

$$\begin{aligned} |T_3\rangle = & \frac{i - e^{\frac{i\pi}{4}}}{2} Z^{\otimes 3} |I_3\rangle + \frac{i + e^{\frac{i\pi}{4}}}{2} (HSZ)^{\otimes 3} |K_3\rangle \\ & - \frac{i + e^{\frac{i\pi}{4}}}{2} Z^{\otimes 3} |K_3\rangle \end{aligned} \quad (\text{A.3})$$

$$\begin{aligned} |T_6\rangle = & -\frac{1}{2} S_1 H_1 (Z)^{\otimes 6} |K_6\rangle + \frac{e^{\frac{3i\pi}{4}}}{2} S_1 H_1 S_1 (SZ)^{\otimes 6} |K_6\rangle \\ & - \frac{i}{2\sqrt{2}} S_1 X_1 (HS)^{\otimes 6} |K_6\rangle + \frac{e^{-\frac{i\pi}{4}}}{2\sqrt{2}} (HS)^{\otimes 6} |K_6\rangle \\ & - \frac{1}{2} H_1 S_1 (SZ)^{\otimes 6} |K_6\rangle - \frac{e^{\frac{i\pi}{4}}}{2} H_1 Z_1 (Z)^{\otimes 6} |K_6\rangle \end{aligned} \quad (\text{A.4})$$

Appendix B

Proofs of transformation rules

Here we prove the expressions for $|\psi_{PQ}\rangle$ in Table 3.1. Recall that we have $|\psi_{PQ}\rangle = \frac{1}{2}((I + P_u)I_v + (I - P_u)Q_v)|G\rangle$ from Equation (3.17). We also have the shorthand for sets of neighbours, $N_w = N(w)$ and $M_w = N_w \cup \{w\}$. Let $\mathbb{1}_{u,v}$ be an indicator function equal to 1 if u is connected to v in G and 0 otherwise. In these proofs we also make use of graph stabilizers and the operator Δ for the symmetric difference. When applying Theorem 2.5.2 and Theorem 3.5.1, we show the sets A and B used.

The case of $|\psi_{ZZ}\rangle$ is just the toggling of an edge. The cases of $|\psi_{ZX}\rangle$ and $|\psi_{XX}\rangle$ are derived in [42], but we include the proofs of these cases for completeness.

Lemma B.1 (Elliott, Eastin, and Caves [42]).

$$|\psi_{ZX}\rangle = \left(\prod_{w \in N_v} CZ_{u,w} \right) |G\rangle. \quad (\text{B.1})$$

Proof. Let G' be the graph formed from G where all the edges incident to u are removed.

$$|\psi_{ZX}\rangle = \frac{1}{2} \left(\underbrace{(I + Z)_u |G\rangle}_{A=M_u, B=\{u\}} + X_v \underbrace{(I - Z)_u |G\rangle}_{A=M_u, B=\{u\}} \right) \quad (\text{B.2})$$

$$= \frac{1}{\sqrt{2}} H_u |G'\rangle + X_v \frac{1}{\sqrt{2}} H_u \left(\prod_{w \in M_u} Z_w \right) |G'\rangle \quad (\text{B.3})$$

$$= \frac{1}{\sqrt{2}} H_u \underbrace{\left(I + (-1)^{\mathbb{1}_{u,v}} \left(\prod_{w \in M_u} Z_w \right) \left(Z_u^{\mathbb{1}_{u,v}} \prod_{w \in N_v} Z_w \right) \right)}_{A=\{u\}, B=M_u \Delta N_v \Delta \{u\}^{\mathbb{1}_{u,v}}} |G'\rangle \quad (\text{B.4})$$

$$= Z_u^{1+2\mathbb{1}_{u,v}} \left(\prod_{w \in M_u \Delta N_v} CZ_{u,w} \right) |G'\rangle = \left(\prod_{w \in N_v} CZ_{u,w} \right) |G\rangle \quad (\text{B.5})$$

Here, $\{u\}^{\mathbb{1}_{u,v}}$ denotes that the set is empty if u and v are not connected in G and is equal to $\{u\}$ otherwise. \square

Lemma B.2.

$$|\psi_{YZ}\rangle = S_v Z_v \left(\prod_{w \in M_u} CZ_{v,w} \right) |G\rangle. \quad (\text{B.6})$$

Proof. Let G' refer to the graph resulting from toggling all the edges between vertices in the set M_u in G .

$$|\psi_{YZ}\rangle = \frac{1}{2} ((I + Y)_u + Z_v(I - Y)_u) |G\rangle \quad (\text{B.7})$$

$$= \frac{1}{2} ((I - iZX)_u |G\rangle + Z_v(I + iZX) |G\rangle) \quad (\text{B.8})$$

$$= \frac{1}{2} \left(\underbrace{\left(I - i \left(\prod_{w \in M_u} Z_u \right) \right)}_{A=M_u} |G\rangle + Z_v \underbrace{\left(I + i \left(\prod_{w \in M_u} Z_u \right) \right)}_{A=M_u} |G\rangle \right) \quad (\text{B.9})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) |G'\rangle + \frac{1+i}{2} Z_v \left(\prod_{w \in M_u} S_w^3 \right) |G'\rangle \quad (\text{B.10})$$

$$= \frac{1+i}{2} Z_v \left(\prod_{w \in M_u} S_w^3 \right) \underbrace{\left(I - i Z_v \prod_{w \in M_u} Z_w \right)}_{A=M_u \Delta \{v\}} |G'\rangle \quad (\text{B.11})$$

$$= Z_v \left(\prod_{w \in M_u} S_w^3 \right) \left(\prod_{w \in M_u \Delta \{v\}} S_w \right) \left(Z_v^{1,u,v} \prod_{w \in M_u} CZ_{v,w} \right) |G\rangle \quad (\text{B.12})$$

$$= S_v Z_v \prod_{w \in M_u} CZ_{v,w} |G\rangle \quad (\text{B.13})$$

□

Lemma B.3 (Elliott, Eastin, and Caves [42]). *If the edge (u, v) is in the graph G ,*

$$|\psi_{XX}\rangle = H_u H_v CZ_{u,v} \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) |G\rangle. \quad (\text{B.14})$$

Otherwise,

$$|\psi_{XX}\rangle = \left(\prod_{p \in N_u, q \in N_v} CZ_{p,q} \right) |G\rangle. \quad (\text{B.15})$$

Proof. If the edge (u, v) is in the graph G , we apply Theorem 3.3.11.

$$|\psi_{XX}\rangle = \frac{1}{2}((I + X)_u + (I - X)_u X_v) |G\rangle \quad (\text{B.16})$$

$$= \frac{1}{2} H_u H_v ((I + Z)_u + (I - Z)_u Z_v) H_u H_v |G\rangle \quad (\text{B.17})$$

$$= \frac{1}{2} H_u H_v ((I + Z)_u + (I - Z)_u Z_v) Z_u Z_v \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) |G\rangle \quad (\text{B.18})$$

$$= H_u H_v Z_u Z_v \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) |\psi_{ZZ}\rangle \quad (\text{B.19})$$

$$= H_u H_v CZ_{u,v} \left(\prod_{p \in M_u, q \in M_v} CZ_{p,q} \right) |G\rangle \quad (\text{B.20})$$

If the edge (u, v) is not in graph G , we consider the inner product of $|\psi_{XX}\rangle$ with a computational basis state $|s\rangle$ corresponding to an arbitrary bit string s . Let s_i be the i^{th} bit of s . For any set R , let s_R be the sum of values of s_i for indices $i \in R$.

$$\langle s | \psi_{XX} \rangle = \frac{1}{2} \langle s | (I + X)_u + (I - X)_u X_v | G \rangle \quad (\text{B.21})$$

$$= \frac{1}{2} \left\langle s \left| \left(I + \prod_{w \in N_u} Z_w \right) + \left(I - \prod_{w \in N_u} Z_w \right) \left(\prod_{w \in N_v} Z_w \right) \right| G \right\rangle \quad (\text{B.22})$$

$$= \frac{1}{2} ((1 + (-1)^{s_{N_u}}) + (1 - (-1)^{s_{N_u}})) (-1)^{s_{N_v}} \langle s | G \rangle \quad (\text{B.23})$$

$$= \frac{1}{2} (1 + (-1)^{s_{N_u}} + (-1)^{s_{N_v}} - (-1)^{s_{N_u} + s_{N_v}}) \langle s | G \rangle \quad (\text{B.24})$$

This expression is equal to $\langle s | G \rangle$ if either s_{N_u} or s_{N_v} is even, otherwise this expression is equal to $-\langle s | G \rangle$. Similarly, we have that $\left\langle s \left| \prod_{p \in N_u, q \in N_v} CZ_{p,q} \right| G \right\rangle = (-1)^{s_{N_u} s_{N_v}} \langle s | G \rangle$, which is equal to the expression above. This concludes the proof. \square

Lemma B.4. *If the edge (u, v) is in the graph G ,*

$$|\psi_{YX}\rangle = \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_u \Delta M_v} CZ_{u,w} \right) |L_u(G)\rangle. \quad (\text{B.25})$$

Otherwise,

$$|\psi_{YX}\rangle = \left(\prod_{w \in M_u \Delta N_v} Z_w \right) \left(\prod_{p, q \in M_u \Delta N_v} CS_{p,q} \right) \left(\prod_{p, q \in M_u} CS_{p,q} \right) |G\rangle. \quad (\text{B.26})$$

Proof. Let G' refer to the graph resulting from toggling all the edges between vertices in the

set M_u in G . If the edge (u, v) is in the graph G , we have the following.

$$|\psi_{YX}\rangle = \frac{1}{2} ((I + Y)_u + (I - Y)_u X_v) |G\rangle \quad (\text{B.27})$$

$$= \frac{1}{2} ((I - iZ_u X_u) |G\rangle + X_v (I + iZ_u X_u) |G\rangle) \quad (\text{B.28})$$

$$= \frac{1}{2} \left(\underbrace{\left(I - i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} + X_v \underbrace{\left(I + i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} \right) \quad (\text{B.29})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) |G'\rangle + \frac{1+i}{2} X_v \left(\prod_{w \in M_u} S_w^3 \right) |G'\rangle \quad (\text{B.30})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \left(I + \left(\prod_{w \in M_u} Z_w \right) Z_v X_v \right) |G'\rangle \quad (\text{B.31})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \underbrace{\left(I + \prod_{w \in N_v} Z_w \right) |G'\rangle}_{A=\{u\}, B=N_v} \quad (\text{B.32})$$

$$= \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u Z_u \left(\prod_{w \in N_v} C Z_{u,w} \right) |G'\rangle \quad (\text{B.33})$$

$$= \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_u \Delta N_v} C Z_{u,w} \right) |L_u(G)\rangle \quad (\text{B.34})$$

If the edge (u, v) is not in the graph G , we have the following.

$$|\psi_{YX}\rangle = \frac{1}{2} ((I + Y)_u + (I - Y)_u X_v) |G\rangle \quad (\text{B.35})$$

$$= \frac{1}{2} ((I - iZ_u X_u) |G\rangle + X_v (I + iZ_u X_u) |G\rangle) \quad (\text{B.36})$$

$$= \frac{1}{2} \left(\underbrace{\left(I - i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} + X_v \underbrace{\left(I + i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} \right) \quad (\text{B.37})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) |G'\rangle + \frac{1+i}{2} X_v \left(\prod_{w \in M_u} S_w^3 \right) |G'\rangle \quad (\text{B.38})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \underbrace{\left(I + i \left(\prod_{w \in M_u \Delta N_v} Z_w \right) \right)}_{A=M_u \Delta N_v} |G'\rangle \quad (\text{B.39})$$

$$= \left(\prod_{w \in M_u} S_w \right) \left(\prod_{w \in M_u \Delta N_v} Z_w \right) \left(\prod_{p,q \in M_u \Delta N_v} CS_{p,q} \right) |G'\rangle \quad (\text{B.40})$$

$$= \left(\prod_{w \in M_u \Delta N_v} Z_w \right) \left(\prod_{p,q \in M_u \Delta N_v} CS_{p,q} \right) \left(\prod_{p,q \in M_u} CS_{p,q} \right) |G\rangle \quad (\text{B.41})$$

□

Lemma B.5. *If the edge (u, v) is in the graph G ,*

$$|\psi_{YY}\rangle = -i \left(\prod_{p,q \in M_u} CS_{p,q} \right) \left(\prod_{p,q \in M_v} CS_{p,q} \right) |G\rangle. \quad (\text{B.42})$$

Otherwise,

$$|\psi_{YY}\rangle = \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_v} CZ_{u,w} \right) |L_u(G)\rangle. \quad (\text{B.43})$$

Proof. Let G' refer to the graph resulting from toggling all the edges between vertices in the

set M_u in G . If the edge (u, v) is in the graph G , we have the following.

$$|\psi_{YY}\rangle = \frac{1}{2} ((I + Y)_u + (I - Y)_u Y_v) |G\rangle \quad (\text{B.44})$$

$$= \frac{1}{2} ((I - iZ_u X_u) |G\rangle + Y_v (I + iZ_u X_u) |G\rangle) \quad (\text{B.45})$$

$$= \frac{1}{2} \left(\underbrace{\left(I - i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} + Y_v \underbrace{\left(I + i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} \right) \quad (\text{B.46})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) |G'\rangle + \frac{1+i}{2} Y_v \left(\prod_{w \in M_u} S_w^3 \right) |G'\rangle \quad (\text{B.47})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \left(I - i \left(\prod_{w \in M_u} Z_w \right) X_v \right) |G'\rangle \quad (\text{B.48})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \underbrace{\left(I - i \prod_{w \in M_v} Z_w \right) |G'\rangle}_{A=M_v} \quad (\text{B.49})$$

$$= -i \left(\prod_{w \in M_u} S_w \right) \left(\prod_{p,q \in M_v} CS_{p,q} \right) |G'\rangle \quad (\text{B.50})$$

$$= -i \left(\prod_{p,q \in M_u} CS_{p,q} \right) \left(\prod_{p,q \in M_v} CS_{p,q} \right) |G\rangle \quad (\text{B.51})$$

If the edge (u, v) is not in the graph G , we have the following.

$$|\psi_{YY}\rangle = \frac{1}{2} ((I + Y)_u + (I - Y)_u Y_v) |G\rangle \quad (\text{B.52})$$

$$= \frac{1}{2} ((I - iZ_u X_u) |G\rangle + Y_v (I + iZ_u X_u) |G\rangle) \quad (\text{B.53})$$

$$= \frac{1}{2} \left(\underbrace{\left(I - i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} + Y_v \underbrace{\left(I + i \prod_{w \in M_u} Z_w \right) |G\rangle}_{A=M_u} \right) \quad (\text{B.54})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) |G'\rangle + \frac{1+i}{2} Y_v \left(\prod_{w \in M_u} S_w^3 \right) |G'\rangle \quad (\text{B.55})$$

$$= \frac{1-i}{2} \left(\prod_{w \in M_u} S_w \right) \underbrace{\left(I + \left(\prod_{w \in M_u \Delta M_v} Z_w \right) \right)}_{A=\{u\}, B=M_u \Delta M_v} |G'\rangle \quad (\text{B.56})$$

$$= \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u Z_u \left(\prod_{w \in M_u \Delta M_v} CZ_{u,w} \right) |G'\rangle \quad (\text{B.57})$$

$$= \frac{1-i}{\sqrt{2}} \left(\prod_{w \in M_u} S_w \right) H_u \left(\prod_{w \in M_v} CZ_{u,w} \right) |L_u(G)\rangle \quad (\text{B.58})$$

□

This completes the proofs of all of the expressions in Table 3.1.

Appendix C

Basics of the ZX-calculus

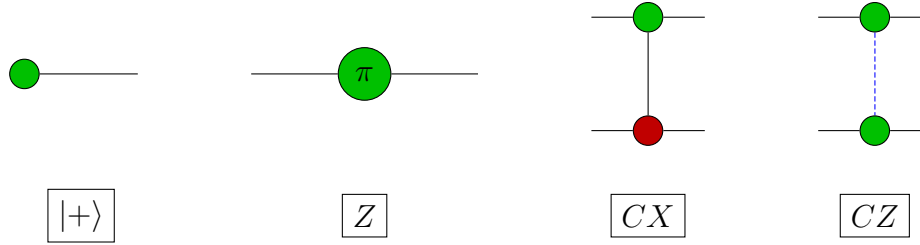
The ZX-calculus is a graphical language used for expressing quantum processes. Specifically, the ZX-calculus consists of *ZX diagrams*, tensor networks made of nodes and edges, with each node representing a specific tensor and each edge acting as an inner product.

Although the ZX-calculus can represent all tensors, we will use it for the representation of Clifford gates. This appendix contains a basic introduction to the ZX-calculus. We cover the basics of which nodes can be used in ZX diagrams as well as several *rewrite rules*, diagrammatic transformations which allow us to manipulate and simplify ZX diagrams. For our diagrams, we use the conventions as described in [72].

The Z (or green) nodes and X (or red) nodes represent tensors that can be used to represent quantum operations such as qubits, gates, or measurements. Each node has a phase, with empty nodes representing a phase of 0. A Z node with n inputs, m outputs, and phase α is equivalent to the tensor $|0\rangle^{\otimes m} \langle 0|^{\otimes n} + e^{i\alpha} |1\rangle^{\otimes m} \langle 1|^{\otimes n}$. An X node with n inputs, m outputs, and phase β is equivalent to the tensor $|+\rangle^{\otimes m} \langle +|^{\otimes n} + e^{i\beta} |-\rangle^{\otimes m} \langle -|^{\otimes n}$. Generally, ZX diagrams ignore normalization and scalar factors.

A ZX diagram represents a tensor network where connections between nodes are inner products on the indices of the corresponding tensors. It is possible to convert efficiently between quantum circuits and ZX diagrams, with examples given in Section 4.4.1, Section 4.5.2, Appendix D, and in Appendix H. Hadamard gates, represented by yellow boxes \blacksquare , can be placed on edges between nodes or on free edges. Another convention for Hadamard gates placed on edges is to colour the edge in blue rather than the default black. For our purposes, edges with Hadamards will usually be represented by blue edges while edges without Hadamards will be represented by black edges.

The fundamentals of the ZX-calculus allow us to express various commonly seen quantum operations. For instance below, we see the initialization of a $|+\rangle$ state, a Z gate, a CX gate, and a CZ gate. In the CX gate, the wire with the Z node is the control and the wire with the X node is the target. Note that the dashed edge in the CZ gate is blue, meaning it is Hadamarded. If the colours of the Z nodes in the $|+\rangle$ state and the Z gate were changed to red, these would be X nodes depicting the $|0\rangle$ state and the X gate.



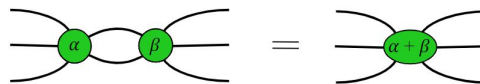
Note that projection operations and measurements can result in a disconnected diagram. For example, the Pauli projector $|+\rangle\langle+| = \frac{I+X}{2}$ would be depicted as follows.



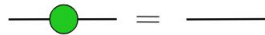
The ZX-calculus also has a set of basic rewrite rules that allow for diagrams to be converted into equivalent forms. Since the ZX-calculus is complete with respect to Clifford codes and states [72], these basic rewrite rules can be used to derive all other rewrite rules.

Definition C.1 (Basic rewrite rules [74]). For each basic rewrite rule below, an analogous rule holds when the colours are interchanged, meaning all Z and X nodes are changed into X and Z nodes, respectively. Note that all other rewrite rules are derived from these eight, but the ones shown are not a minimal set of rewrite rules [102].

- (1) Merging/unmerging rule: Two Z (or X) nodes with phases α and β that are connected by edges with no Hadamards may be combined into a single Z (or X) node with phase $\alpha + \beta$. The resulting node has all the external edges of the two original nodes. A node may also be unmerged into two nodes, with the partition of the external edges connected to each node done arbitrarily.



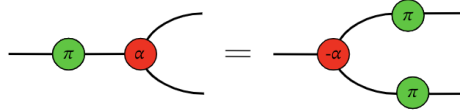
- (2) Identity removal rule: Z (or X) nodes with phase 0 and exactly two edges can be removed. Note that the two edges could both be input or output edges.



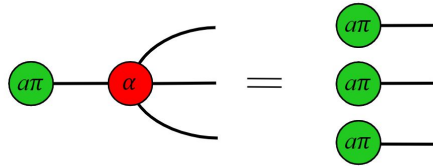
- (3) Hadamard cancellation rule: Two Hadamard gates on one edge can be cancelled since $HH = I$.



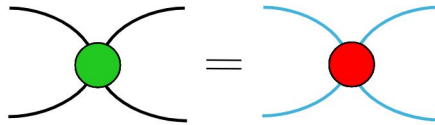
- (4) π -copy rule: A Z (or X) node of phase π slides through and copies onto all the other edges of an adjacent X (or Z) node. The X (or Z) node has its phase negated. Shown below is an example with a Z node of phase π , which implements a Z gate.



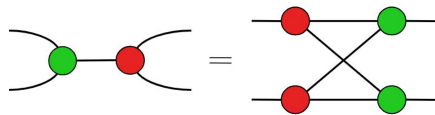
- (5) State-copy rule: A Z (or X node) with a phase of $a\pi$ with $a \in \{0, 1\}$ can be copied through onto all of the other adjacent edges of an X (or Z node) with any phase α .



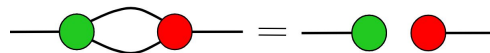
- (6) Colour change rule: A Z (or X) node can be exchanged for an X (or Z) node if all edges adjacent to the node have Hadamards added to them.



- (7) Bialgebra rule: By acting on an edge between a Z and an X node, each external edge gets one node, and a complete bipartite graph is formed between these new nodes. An example is shown below. There may be one or more (rather than two) edges coming in from the left side of the graph, and there may be one or more edges exiting on the right side of the graph.



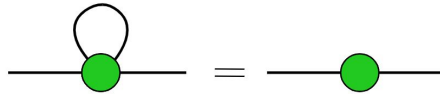
- (8) Hopf rule: If a Z node and X node share multiple edges that have no Hadamards, two of these shared edges may be removed together.



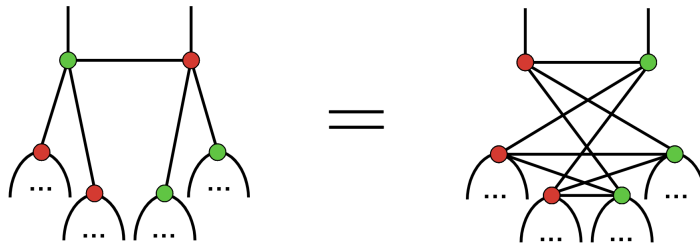
Additional rules that will be used later are given below.

Definition C.2 (Derived rewrite rules). Below are two rules that can be derived from the set of basic rewrite rules above.

- (1) Loop rule: Self-loops on a node can be removed. If the self-loop has a Hadamard, then removing the loop adds a phase of π to the node.



- (2) Hadamard-sliding rule: This rule allows the colours of two adjacent vertices to be swapped while switching their sets of neighbours and toggling the edges between those two sets.



We note that the Hadamard-sliding rule is a special case of Equation 3.12. The case is special since the neighbouring sets of the two top vertices do not intersect.

Appendix D

Tableau to graph proofs

In Chapter 4 we briefly sketched the algorithm that maps encoders to ZXCFs. Here, we give a detailed explanation of this algorithm. The first part of our algorithm maps the encoder into any equivalent ZX diagram. We can then transform the diagram via a sequence of ZX equivalence rules into a ZXCF. To accomplish a transformation into ZX diagrams, we first recall Theorem 3.3.4 from Chapter 3. The theorem proves the existence of a canonical form called HK form for stabilizer states.

Although we did not use ZX calculus to construct the HK form for states, our construction for codes uses graph states with local Clifford operators, which can be mapped directly to ZX calculus.

An HK diagram is constructed by starting with a graph state. As per Definition 2.4.2, a graph state is a Clifford state corresponding to an undirected graph wherein the nodes become $|+\rangle$ qubits and the edges become controlled- Z gates. Each node is then endowed with a single *free edge*, which does not connect to any other node. Local Clifford operations in $\langle H, S, Z \rangle$ are then applied to the qubits of the graph state to create an HK diagram.

Such a construction has the capacity to express any stabilizer state. A direct mapping enables the presentation of a HK diagram into the ZX calculus.

- (1) HK vertices become Z nodes, as a vertex in a graph state begins in the state $|+\rangle$, which is a Z node with a single output.
- (2) HK (non-free) edges become (non-free) edges with Hadamard gates, as both of these correspond to CZ gates.
- (3) HK local operations of S , Z , or SZ become phases on the corresponding node of $\frac{\pi}{2}$, π , and $\frac{3\pi}{2}$, respectively. The local operation H becomes a Hadamard gate on the node's free edge.

Thus, we will effectively consider HK forms to be in the ZX calculus representation and denote them *ZX-HK forms*. We remark that transformations of similar decorated graph state families into ZX calculus presentations have been considered in other contexts, such as by Backens [72].

Our constructions in Chapter 3 are limited to stabilizer states. However, by vector space duality we can equivalently transform operators into states and vice versa. The formal

statement of this duality in quantum information theory is given by the Choi-Jamiołkowski isomorphism. The composition of such a transformation with the result above gives the following lemma.

Lemma D.1. *There exists an efficient transformation of any Clifford ZX encoder diagram with $n - k$ input edges and n output edges into a corresponding ZX presentation of a stabilizer state in ZX-HK form, with $n + (n - k) = 2n - k$ free edges.*

Proof. We proceed by turning the encoder diagram into a Clifford circuit and then mapping the output of that circuit to HK form. Any X (red) nodes in the ZX encoder diagram can be transformed into Z (green) nodes with the same phase surrounded by Hadamard gates. Now, we can interpret the ZX encoder diagram as a state by treating the input edges as additional output edges. This means all free edges of the diagram are output edges so the diagram encodes a Clifford state. This is the ZX version of the Choi-Jamiołkowski isomorphism.

As shown by Backens [72], any Clifford ZX diagram can be decomposed entirely in terms of the following operations.

First, we could have a Z node with only one output or only one input. In a circuit, this is a $|+\rangle$ qubit or a post-selected $\langle +|$ measurement, respectively. We can also have a Hadamarded edge or a node with $\frac{\pi}{2}$ phase, which are represented as H or S gates in circuits, respectively. Lastly, we can have a Z node of degree 3, with either 2 inputs and 1 output or 1 input and 2 outputs that acts as a merge or a split. This is equivalent to applying a CX operation between two qubits where the second qubit is either initialized to $|0\rangle$ before the CX gate or post-selected by the measurement $\langle 0|$ after the CX gate, respectively.

If we need to compute the action of a post-selected measurement, that means we have an internal node, since the measuring node would not have any free edges. To remove an internal node, we first try merging it with a neighbouring node if they share a non-Hadamarded edge. If this is impossible, we consider the neighbours of the internal node, if those can be merged with other nodes, we do so until the internal node has a neighbour that cannot be merged further. We then apply the bialgebra rule from Definition C.1 between the internal node and an unmergeable neighbour. Specifically, we apply the version of the bialgebra rule where all X nodes have been replaced with Z nodes and Hadamard gates. This bialgebra operation creates several new nodes, but since the bialgebra rule changes the colours of the nodes connected to each free edge of the rule, this allows us to merge all new nodes that are not connected to a free edge of the diagram. This means that we can use the bialgebra rule to remove any internal nodes, simplifying out the action of post-selection measurements in our circuit.

As we apply each of these operations we keep track of the current HK form for our state. One concern we might have is that one of these operations will require us to implement a two-qubit gate across two-qubits that are spatially separated in the ZX diagram, and thus temporally separated in our circuit. Since we can always express any diagram using the above operations, we only need to be able to apply the above operations to the current state expressed by the diagram. Thus, repeatedly updating the HK form for the current state encoded by the circuit is all we have to do. All the above operations get applied to the free edges of this state. All the manipulations necessary to keep a state updated in HK form are detailed in Chapter 3. In addition, these steps can all be done efficiently by Theorem 3.3.13,

so this gives us an efficient procedure for turning a ZX diagram into a corresponding stabilizer state in HK form. \square

The application of Lemma D.1 results in a ZX-HK form. That is, there is one Z node per vertex of the graph in HK form, and any internal edge has a Hadamard gate on it. If it would be possible to merge two nodes so that a node has multiple free edges, we add two Hadamard gates to one of the free edges and a phase-free Z node in between the Hadamard gates. These operations do not change the state and they can return a diagram to ZX-HK form. An example of this is seen in Figure 4.2(b)-(c).

Free edges can only have Hadamard gates on them if they satisfy both the condition that their phase is a multiple of π , corresponding to the local Clifford gates H and HZ in HK form, and the condition that the associated node is not connected to any lower-numbered nodes, as indexed by the output edges. Nodes whose free edges have no Hadamard gate are free to have any multiple of $\frac{\pi}{2}$ as a phase, corresponding to local Clifford operations I , S , Z , or SZ , respectively.

We are now equipped with a ZX-HK diagram that represents a state. This diagram has only output edges. To return it into an encoder diagram, we partition the $2n - k$ free edges into $n - k$ input edges and n output edges. In the circuit representation, this is equivalent to turning bra's into ket's and vice versa to map between an operator and a state. For example, $|00\rangle\langle 1| - |11\rangle\langle 0| \leftrightarrow |001\rangle - |110\rangle$. Now, if there are any edges between input nodes (those in \mathcal{I}), we can simply remove them. They correspond to controlled- Z operations, and we can take off any unitary operation on the input by the encoder definition. The same goes for local Cliffords on \mathcal{I} .

At this stage, the obtained ZX-HK form is in encoder-respecting form. It also satisfies the Edge and Hadamard rules—there are no input edges in ZX-HK form so the analogous rule is enforced only on lower-numbered nodes, but if we number the nodes from the beginning such that the input nodes are lower-numbered than all output nodes, then the transformed ZX-HK form will satisfy our ZXCF Hadamard rule. So, all that remains is to simplify the diagram to obey the RREF and Clifford rules.

Lemma D.2. *An encoder diagram in ZX-HK form can be efficiently transformed to satisfy the RREF rule, while continuing to satisfy the Edge and Hadamard rules.*

Proof. This proof relies on two basic properties of ZX calculus. The first is that a CX gate can be expressed on a pair of qubits by adding a pair of phase-free nodes connected by an edge, with a Z node on the control and an X node on the target. The second fact is the bialgebra rewrite rule from Definition C.1, which allows us to rewrite a Z node connected to an X node by the following sequence of steps. First, remove the two nodes and the edge between them. Next, add an X node on each edge previously leading into the Z node; do the same for the X node by adding Z nodes. Lastly, connect each new X node to each new Z node.

Applying a CX gate to a pair of inputs is a unitary operation and does not change our code. As discussed in Appendix C, a CX consists of adding a pair of connected nodes to existing qubit wires, a Z node to the control wire and an X to the target wire. After applying a CX gate this way, we perform the following sequence of steps. The control Z node of the CX gate fuses with the first input. The target X node is used to perform the bialgebra

rule with the second input. This results in two Z nodes where the CX target used to be, one of these is on the free input edge and the other is on the edge connecting the target node to the first input. The latter of these Z nodes is merged with the first input while the Z node on the free edge becomes the new input node for the second input. Meanwhile, the X nodes on each input-output edge previously connected to the second input now find themselves connected to both the first and second input. Additionally, we can turn them into Z nodes after commuting them through the Hadamard gate on their input-output edge, merging them with the outputs on the other side. Any doubled edges are removed by the Hopf rule from Definition C.1. The result is that we added the row of $M_{\mathcal{D}}$ corresponding to the first input too the row of the second. This allows to do arbitrary row operations since $M_{\mathcal{D}}$ is an adjacency matrix and is evaluated mod 2. This concludes the proof of the fact that $M_{\mathcal{D}}$ can be turned into RREF without affecting the Edge and Hadamard rules. \square

The only remaining task is to enforce the Clifford rule. For any pivot node $p \in \mathcal{P}$ with a non-zero phase, let $v \in \mathcal{I}$ be its associated input node. We apply the effect of Equation (3.14) v , which we can do freely since we are just applying $\sqrt{X} = HSH$, a unitary operation, to v , an input node. Notably, this does not change the entries of $M_{\mathcal{D}}$. Importantly, this operation increases the phases of each neighbours of v_{in} by $\frac{\pi}{2}$ (due to multiplication by S). We repeat process until the phase of p vanishes.

The last step of the Clifford rule that we need to satisfy is to remove edges between pivots. If there are any edges between pivots p_1 and p_2 , we can remove them by applying the following procedure. First, we apply the input unitary operation $H_{p_1}H_{p_2}CZ_{p_1,p_2}$. This connects the input nodes and applies H vertices to the inputs. Next, we can now perform the transformation given by Equation (3.12). In particular, one effect of this transformation is toggling the edge (p_1, p_2) since each pivot is connected to its own input. This operation will apply the input unitary $Z_{p_1}Z_{p_2}$, which can be removed as it does not change the encoder. Additionally, this operations swaps the neighbours of p_1 and p_2 , which is also an input unitary that we can correct with a SWAP gate. We repeat until no pivot-pivot edges remain.

With that step, the transformation from Clifford encoder to ZXCF is complete. Although this process may seem lengthy, all of these steps can be done systematically in an efficient manner, without having to go back to fix earlier rules. Specifically, this algorithm takes worst-case $O(n^3)$ time. Creating the HK diagram for the encoder requires us to apply at most $O(n)$ Pauli projections, each of which can be applied in at most $O(n^2)$ time. After the HK form is created, operations such as row-reducing a matrix can be done in $O(n^3)$ time. We suspect that the worst-case time complexity cannot be improved, but that there is a lot of room for heuristic runtime improvements and optimizations.

Appendix E

Derivation of ZXCF counting recursion

In this appendix we provide the derivation of the recursive counting formula of ZXCF diagrams, given in Equation (4.3). To derive f , we provide the following visualization. We start with no assigned nodes and we must sequentially assign the n output nodes to be pivots (case A) or non-pivots (case B), where pivots must be matched with input nodes. The current number of assigned pivots is tracked by p and the number of non-pivot outputs is tracked by o . The number of remaining output nodes to be assigned is tracked by n . The number of remaining input nodes to be matched with a pivot is k , which is $n - m$, since $m = n - k$. Thus, m tracks the number of unassigned output nodes that will need to be assigned as non-pivots.

We first describe $A_{n,m,p,o}$. Suppose we want the next output node to be a pivot (in \mathcal{P}). Since there is a bijection between pivots and inputs, we can only assign additional pivots only if we have more remaining nodes n than the the number that need to become non-pivots m . Otherwise, we have $n = m$ and we cannot assign a node as a pivot, so in that case we have $A_{n,m,p,o} = 0$. The matching between pivots and input nodes is fully constrained by the RREF rule, which sorts the inputs and pivots together. The Clifford rule says that no pivot nodes may have local Clifford operations, so we just need to choose the edges connecting the new pivot to nodes we have already assigned. Since there are no pivot-pivot edges and the pivot connects to only one input, we have exactly 2^o possibilities, where o is the number of previously assigned non-pivot outputs. These o nodes are the only nodes to which we can connect our pivot. Having made an assignment, p increases by 1, and n decreases by 1. Thus, when $n > m$, we have $A_{n,m,p,o} = 2^o f(n - 1, m, p + 1, o)$.

We now describe $B_{n,m,p,o}$. Suppose instead we want the next output node to be a non-pivot (in \mathcal{O}). If $m = 0$, we must assign all of our remaining nodes to be pivots and we cannot assign a node to be an input, so in this case, $B_{n,m,p,o} = 0$. Otherwise, we have to choose the local Clifford operation as well as the node's edges to previously assigned vertices. If we choose to connect the node to none of the p assigned inputs, p assigned pivots, or o assigned vertices, then we are allowed to place any of the 6 local Cliffords on the node. If any of those edges are present, we cannot apply a Hadamard to the output edge due to the Hadamard rule. Hence, 4 choices remain for the local Clifford operation. This works out to a total of $4(2^{2p+o} - 1) + 6 = 2^{2p+o+2} + 2$ possibilities. To finish, we decrement the number of output qubits without changing the number of inputs. This increases o by 1 while decreasing both n and m by 1. Hence, when $m > 0$, we have $B_{n,m,p,o} = (2^{2p+o+2} + 2)f(n - 1, m - 1, p, o + 1)$.

Appendix F

Quantum Gilbert-Varshamov bound

The quantum Gilbert-Varshamov bound, Theorem 4.5.9, is a well known result, discussed in texts such as Nielsen and Chuang [1]. For completeness, we provide a self-contained proof of this theorem.

Proof. We proceed via a probabilistic method. That is, we compute the probability that a random stabilizer code has parameters (n, k, d) where n is large. To construct a random stabilizer code, we begin with Z_1, \dots, Z_{n-k} as stabilizers, and then choose a random Clifford operator U on n qubits. The random stabilizer code is given by stabilizers S_1, \dots, S_{n-k} , defined as $S_1 := UZ_1U^\dagger, \dots, S_{n-k} := UZ_{n-k}U^\dagger$. Such a code is a uniformly random stabilizer code because (a) all of its generators commute and (b) a random Clifford takes distinct non-identity Paulis to uniformly random non-identity Paulis.

We fix a n -qubit non-identity Pauli matrix P and note that $P' := UPU^\dagger$ is a fixed uniformly random non-identity Pauli matrix. Let $p = \Pr[P, S_1] = 0, \dots, [P, S_{n-k}] = 0$ be the probability that P commutes with the entire stabilizer tableau. We note that $p = \Pr[[P', Z_1] = 0, \dots, [P', Z_{n-k}] = 0]$. If P' commutes with Z_v , then the Pauli on the v^{th} qubit must be either I or Z . There are $2(2^{n-k}4^k - 1)$ non-identity Paulis which have I or Z on the first $n - k$ qubits, and $2(4^n - 1)$ total non-identity Paulis. For large enough n we have the following.

$$p = \frac{2(2^{n-k}4^k - 1)}{2(4^n - 1)} \approx \frac{2^{n+k}}{4^n} = \frac{1}{2^{n-k}}. \quad (\text{F.1})$$

On the other hand, the total number of non-identity Paulis with weight at most d is

$$N = \sum_{m=1}^d 3^m \binom{n}{m} \leq 3^d d \binom{n}{d}, \quad (\text{F.2})$$

using the assumption that $d \leq \frac{n}{2}$ so that the last term is the greatest. By Stirling's approximation, as n increases, we have,

$$N \longrightarrow 2^{nH(d/n)+d \log 3+O(\log n)}. \quad (\text{F.3})$$

To complete the proof, we apply the union bound. Let $A(S, P)$ be the event that P commutes with S_1, \dots, S_{n-k} , and let $A(S) = \bigcup_{P \neq I} A(S, P)$. Then

$$\begin{aligned} \Pr[A(S)] &\leq \sum_{P \neq I} \Pr[A(S, P)] \\ &\leq 2^{nH(d/n) + d \log 3 + O(\log n)} 2^{k-n}. \end{aligned} \tag{F.4}$$

A $[n, k, d]$ code exists if and only if $\Pr[A(S)] < 1$. By setting the right-hand side of this inequality to be at most 1, we obtain the quantum Gilbert-Varshamov bound. \square

Appendix G

Constructing the 3-by-3 toric code

In Section 5.4, we provided the 2×2 and 3×3 toric codes in ZX calculus. Here, we provide a more detailed description of the methodology used to determine the structure of the 3×3 toric code.

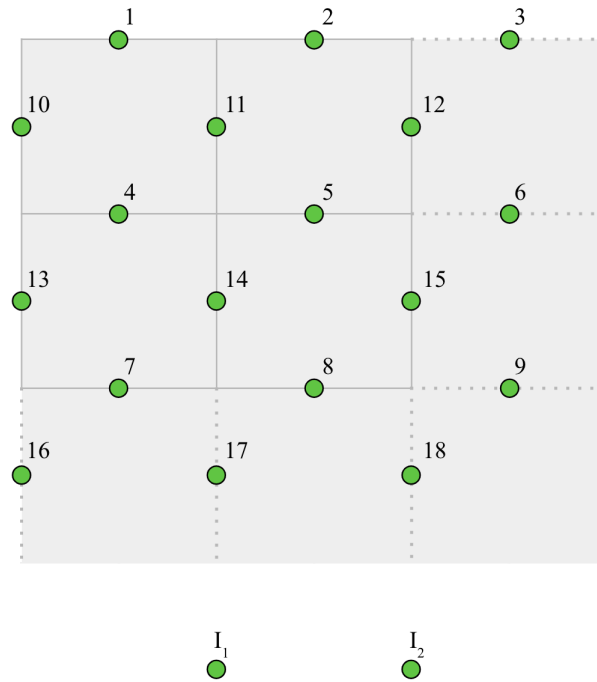


Figure G.1: The input and output nodes in the 3×3 toric code. The boundary conditions are periodic, and all nodes are initially set to Z nodes.

Among the 18 outputs in Figure G.1, we expect some of the free output edges to contain Hadamard gates. For now, we keep the nodes as Z nodes. Suppose the output edge onto vertex 1 has a Hadamard gate. This implies that applying the stabilizer $Z_1 Z_4 Z_{10} Z_{11}$ would result in sliding a Z gate from the end of the output edge, through the Hadamard gate, converting the Z gate to an X gate, then through vertex 1 itself. By the π -copy rule from Definition C.1, the X gate, which is an X node with phase π , copies itself onto all internal

edges connected to vertex 1.

Continuing the assumption that output node 1 has a Hadamard gate, if we instead apply the stabilizer $X_1X_3X_{10}X_{16}$, we slide an X gate from the end of the output edge, through the Hadamard gate, converting the X gate to a Z gate, then onto vertex 1. By the merging rule from Definition C.1, the Z gate, which has phase π , merges with vertex 1, a phase 0 Z node. This results in vertex 1 gaining a phase of π .

By the above, the behaviour of the Z and X gates on an output node with a Hadamard gate is understood. Analogous behaviour occurs on an output node without a Hadamard by switching all the X nodes to Z nodes used in the processes above and vice versa.

To determine all of the edges in the 3×3 toric code in Figure G.1, we consider the process of applying the stabilizers onto the output nodes. Note that all of the internal edges among nodes in the diagram must be edges with Hadamard gate so that the merging rule cannot be applied to merge multiple nodes into one. To simplify our work, we set the output nodes with Hadamards to be 1, 2, 3, 7, 8, 9, 16, 17, and 18. Then, by stabilizer $Z_1Z_4Z_{10}Z_{11}$, the nodes 4, 10, and 11 gain a phase of π from their Z gates while node 1 will cause a π -copy rule to move X gates onto the internal edges connected to node 1. Since all internal edges have Hadamard gates, moving the X gates through the Hadamards will result in Z gates. If these Z gates went to any nodes other than nodes 4, 10, and 11, the stabilizer would not have kept the configuration the same. Therefore, the Z gates must arrive at only nodes 4, 10, and 11. This works because the π 's from these Z gates cancel with the π s already at the nodes. Thus, the only internal edges to node 1 are from nodes 4, 10, and 11.

Using similar reasoning, we can deduce the rest of the internal edges among the output nodes by establishing which nodes must be connected to others by looking at previously established connections. Lastly, we need to determine the logical operators to determine the connections of the input nodes. We look for sets of nodes such that when any stabilizer is applied the input node remains at phase 0. The resulting diagram is shown in Figure 5.6.

Appendix H

Converting ZXCF's into quantum circuits

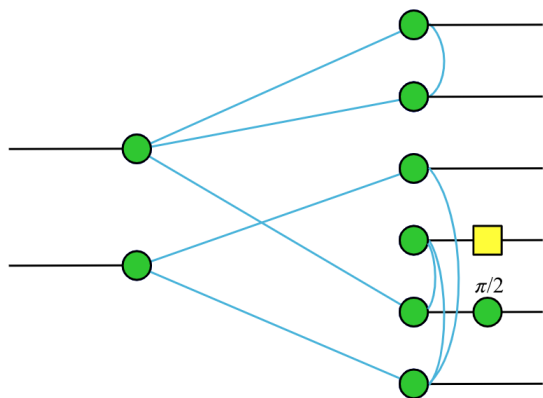
In Section 4.4.1 and Section 5.2, we described a procedure for converting a ZXCF into a quantum circuit, which is repeated here in a slightly modified form. In this appendix, we present a step-by-step example of applying this procedure to a graph code with k logical qubits and n physical qubits.

- (1) Start with k open wires representing the inputs of the circuit.
- (2) Add a $|0\rangle$ state for each of the $n - k$ non-pivot output nodes.
- (3) Apply an H gate to all n wires.
- (4) Apply a CX gate between the pairs wires corresponding to the edges between inputs and non-pivot outputs. The wire of the input node is the target qubit, and the wire of the output node is the control qubit.
- (5) Apply a CZ gate between pairs of wires corresponding to the output-output edges.
- (6) Apply the local operations attached to the outputs to the corresponding wires.

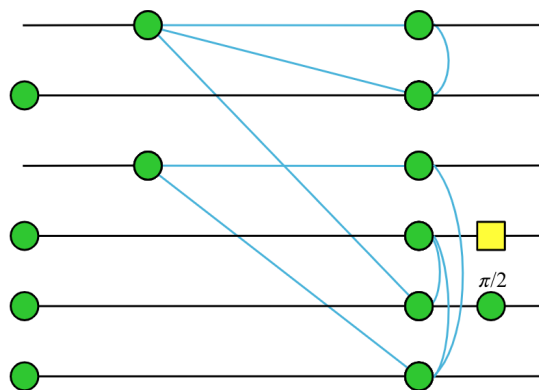
We now show why this works. Consider the example given in Figure H.1a. We will convert this graph code in ZXCF into a circuit. We can first move the input nodes to be along the same horizontal wire as their pivot nodes. Then, we split the non-pivot nodes by unmerging two zero-phase Z nodes. The resulting diagram is shown in Figure H.1b. From here, the edges from inputs to non-pivot outputs can be separated by unmerging nodes and expressing each edge separately, as shown in Figure H.1c. In Figure H.1d, the Hadamards between the inputs and pivots are shown explicitly as yellow boxes. In Figure H.1e, we do a similar unmerging of nodes to separately express the edges between nodes.

The steps used in these diagrams hold in general. We can unmerge each node until all the edges are expressed separately (and the non-pivot nodes have an initial state), and, to keep things organized, we can keep the input-output edges on the left side and the output-output edges on the right side.

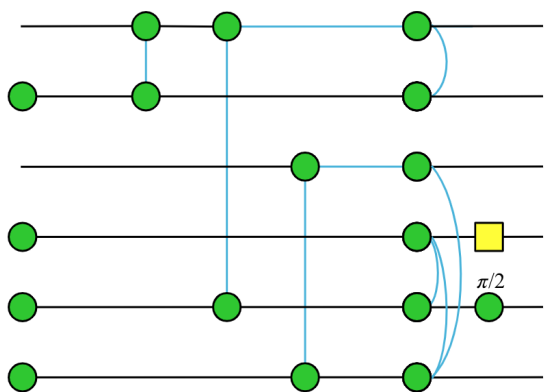
From Figure H.1e, note that the edges with Hadamards between the nodes of a ZX diagram are equivalent to the CZ gates between the corresponding wires in a quantum circuit. Additionally, the Z nodes at the start are equivalent to $|+\rangle$. Note that all of these operations



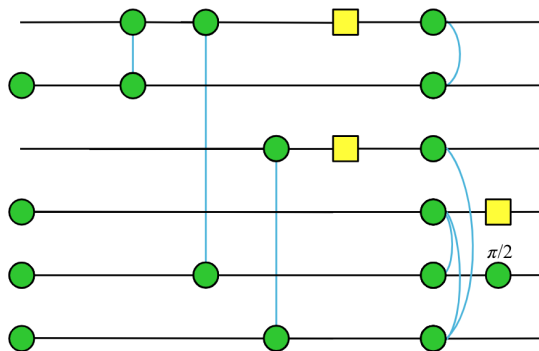
(a) The ZXCF of a graph code. Blue edges represent edges with Hadamards. Note that two of the output edges have local operations. One of the local operations is a Hadamard gate while the other is an S gate.



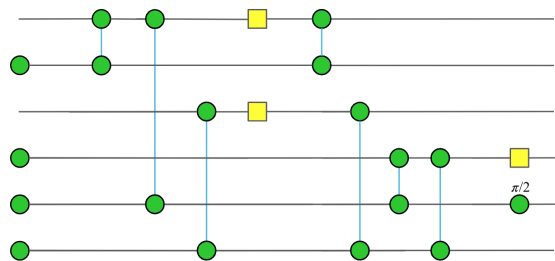
(b) The non-pivot output nodes are unmerged into two Z nodes each, and one of each pair is placed to the left.



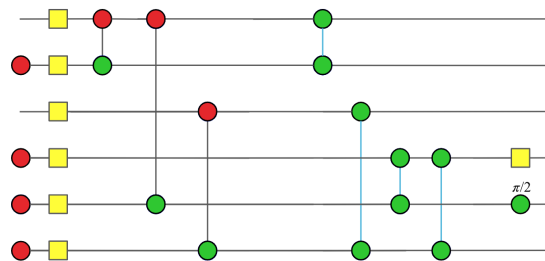
(c) By unmerging the input nodes, the edges between the inputs and non-pivot outputs can be shown separately as CZ gates.



(d) The blue input-pivot edges are displayed with a yellow Hadamard gate on them.



(e) Similar to H.1c, the nodes in each output-output edge are unmerged. Note that the local operations are still at the very right-hand side of the diagram.



(f) The Hadamards in the middle of H.1e are pushed to the left, and the green $|+\rangle$ states transformed into the form $H|0\rangle$, which is a Hadamard on a red $|0\rangle$ state.

Figure H.1: Conversion of a graph code in ZX canonical form into an equivalent quantum circuit diagram.

can be implemented in a standard quantum circuit. We have thus reconstructed the algorithm described in Section 4.4.1.

As a potential additional step, consider sliding the k Hadamards on the input wires towards the start of the circuit, through the Z nodes on the input wires. Since $ZH = HX$, this means each of the CZ 's that the H 's pass through turns into a CX with the target qubit on the input's wire. Also, we may exchange the Z nodes at the start for a X node and an H , since $H|0\rangle = |+\rangle$. The result of this operation is shown in Figure H.1f. From here, we can see why the above procedure produces a quantum encoder from any graph code.

References

- [1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: [10.1017/CBO9780511976667](https://doi.org/10.1017/CBO9780511976667). URL: <https://doi.org/10.1017/CBO9780511976667>.
- [2] L. K. Grover. “A fast quantum mechanical algorithm for database search”. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 212–219. DOI: [10.1145/237814.237866](https://doi.org/10.1145/237814.237866). URL: <https://doi.org/10.1145/237814.237866>.
- [3] P. W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM review* 41.2 (1999), pp. 303–332. DOI: [10.1137/S0097539795293172](https://doi.org/10.1137/S0097539795293172). URL: <https://doi.org/10.1137/S0097539795293172>.
- [4] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick. “A cryptographic test of quantumness and certifiable randomness from a single quantum device”. In: *Journal of the ACM (JACM)* 68.5 (2021), pp. 1–47. DOI: [10.1109/FOCS.2018.00038](https://doi.org/10.1109/FOCS.2018.00038). URL: <https://doi.org/10.1109/FOCS.2018.00038>.
- [5] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. “Quantum money from knots”. In: *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. 2012, pp. 276–289. DOI: [10.48550/arXiv.1004.5127](https://doi.org/10.48550/arXiv.1004.5127). URL: <https://doi.org/10.48550/arXiv.1004.5127>.
- [6] I. M. Georgescu, S. Ashhab, and F. Nori. “Quantum simulation”. In: *Reviews of Modern Physics* 86.1 (2014), p. 153. DOI: [10.1103/RevModPhys.86.153](https://doi.org/10.1103/RevModPhys.86.153). URL: <https://doi.org/10.1103/RevModPhys.86.153>.
- [7] H.-Y. Huang, R. Kueng, and J. Preskill. “Predicting many properties of a quantum system from very few measurements”. In: *Nature Physics* 16.10 (2020), pp. 1050–1057. DOI: [10.1038/s41567-020-0932-7](https://doi.org/10.1038/s41567-020-0932-7). URL: <https://doi.org/10.1038/s41567-020-0932-7>.
- [8] A. Harrow, P. Hayden, and D. Leung. “Superdense coding of quantum states”. In: *Physical review letters* 92.18 (2004), p. 187901. DOI: [10.1103/PhysRevLett.92.187901](https://doi.org/10.1103/PhysRevLett.92.187901). URL: <https://doi.org/10.1103/PhysRevLett.92.187901>.
- [9] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. Van Den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, *et al.* “Evidence for the utility of quantum computing before fault tolerance”. In: *Nature* 618.7965 (2023), pp. 500–505. DOI: [10.1038/s41586-023-06096-3](https://doi.org/10.1038/s41586-023-06096-3). URL: <http://dx.doi.org/10.1038/s41586-023-06096-3>.

- [10] A. Kandala, K. Temme, A. D. Córcoles, A. Mezzacapo, J. M. Chow, and J. M. Gambetta. “Error mitigation extends the computational reach of a noisy quantum processor”. In: *Nature* 567.7749 (2019), pp. 491–495. DOI: [10.1038/s41586-019-1040-7](https://doi.org/10.1038/s41586-019-1040-7). URL: <https://doi.org/10.1038/s41586-019-1040-7>.
- [11] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen. “Deterministic generation of a two-dimensional cluster state”. In: *Science* 366.6463 (2019), pp. 369–372. DOI: [10.1126/science.aay4354](https://doi.org/10.1126/science.aay4354). URL: <https://doi.org/10.1126/science.aay4354>.
- [12] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.* “Quantum supremacy using a programmable superconducting processor”. In: *Nature* 574.7779 (2019), pp. 505–510. DOI: [10.1038/s41586-019-1666-5](https://doi.org/10.1038/s41586-019-1666-5). URL: <https://doi.org/10.1038/s41586-019-1666-5>.
- [13] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, *et al.* “Boson sampling with 20 input photons and a 60-mode interferometer in a 1 0 14-dimensional hilbert space”. In: *Physical review letters* 123.25 (2019), p. 250503. DOI: [10.1103/PhysRevLett.123.250503](https://doi.org/10.1103/PhysRevLett.123.250503). URL: <https://doi.org/10.1103/PhysRevLett.123.250503>.
- [14] C. K. Andersen, A. Remm, S. Lazar, S. Krinner, N. Lacroix, G. J. Norris, M. Gabureac, C. Eichler, and A. Wallraff. “Repeated quantum error detection in a surface code”. In: *Nature Physics* 16.8 (2020), pp. 875–880. DOI: [10.1038/s41567-020-0920-y](https://doi.org/10.1038/s41567-020-0920-y). URL: <https://doi.org/10.1038/s41567-020-0920-y>.
- [15] A. Y. Kitaev. “Quantum error correction with imperfect gates”. In: *Quantum communication, computing, and measurement*. Springer, 1997, pp. 181–188. DOI: [10.1007/978-1-4615-5923-8_19](https://doi.org/10.1007/978-1-4615-5923-8_19). URL: https://doi.org/10.1007/978-1-4615-5923-8_19.
- [16] S. B. Bravyi and A. Y. Kitaev. “Quantum codes on a lattice with boundary”. In: *arXiv preprint quant-ph/9811052* (1998). DOI: [10.48550/arXiv.quant-ph/9811052](https://doi.org/10.48550/arXiv.quant-ph/9811052). URL: <https://doi.org/10.48550/arXiv.quant-ph/9811052>.
- [17] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. “Surface codes: Towards practical large-scale quantum computation”. In: *Physical Review A* 86.3 (2012), p. 032324. DOI: [10.1103/PhysRevA.86.032324](https://doi.org/10.1103/PhysRevA.86.032324). URL: <https://doi.org/10.1103/PhysRevA.86.032324>.
- [18] P. W. Shor. “Scheme for reducing decoherence in quantum computer memory”. In: *Physical review A* 52.4 (1995), R2493. DOI: [10.1103/PhysRevA.52.R2493](https://doi.org/10.1103/PhysRevA.52.R2493). URL: <https://doi.org/10.1103/PhysRevA.52.R2493>.
- [19] D. Gottesman. “An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation”. In: *arXiv preprint arXiv:0904.2557* (2009). DOI: [10.48550/arXiv.0904.2557](https://doi.org/10.48550/arXiv.0904.2557). URL: <https://doi.org/10.48550/arXiv.0904.2557>.
- [20] D. Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997. DOI: [10.48550/arXiv.quant-ph/9705052](https://doi.org/10.48550/arXiv.quant-ph/9705052). URL: <https://doi.org/10.48550/arXiv.quant-ph/9705052>.

- [21] A. Khesin and K. Ren. “Extending the graph formalism to higher-order gates”. In: *Quantum Information and Computation* 23.13–14 (Nov. 2023), pp. 1128–1141. ISSN: 1533-7146. DOI: [10.26421/qic23.13-14-5](https://doi.org/10.26421/qic23.13-14-5). URL: <http://dx.doi.org/10.26421/qic23.13-14-5>.
- [22] D. Aharonov. “A Simple Proof that Toffoli and Hadamard are Quantum Universal”. In: (2003). arXiv: [quant-ph/0301040](https://arxiv.org/abs/quant-ph/0301040) [quant-ph]. URL: <https://arxiv.org/abs/quant-ph/0301040>.
- [23] A. T. Hu and A. B. Khesin. “Improved graph formalism for quantum circuit simulation”. In: *Physical Review A* 105.2 (2022), p. 022432. DOI: [PhysRevA.105.022432](https://doi.org/10.1103/PhysRevA.105.022432). URL: <https://doi.org/10.1103/PhysRevA.105.022432>.
- [24] A. B. Khesin, J. Z. Lu, and P. W. Shor. “Graphical quantum Clifford-encoder compilers from the ZX calculus”. In: (2024). DOI: [10.48550/arXiv.2301.02356](https://doi.org/10.48550/arXiv.2301.02356). arXiv: [2301.02356](https://arxiv.org/abs/2301.02356) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2301.02356>.
- [25] A. B. Khesin, J. Z. Lu, and P. W. Shor. “Universal graph representation of stabilizer codes”. In: (2024). DOI: [10.48550/arXiv.2411.14448](https://doi.org/10.48550/arXiv.2411.14448). arXiv: [2411.14448](https://arxiv.org/abs/2411.14448) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2411.14448>.
- [26] A. B. Khesin and A. Li. “Equivalence Classes of Quantum Error-Correcting Codes”. In: (2024). DOI: [10.48550/arXiv.2406.12083](https://doi.org/10.48550/arXiv.2406.12083). arXiv: [2406.12083](https://arxiv.org/abs/2406.12083) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2406.12083>.
- [27] S. Bravyi and A. Kitaev. “Universal quantum computation with ideal Clifford gates and noisy ancillas”. In: *Phys. Rev. A* 71 (2 2005), p. 022316. DOI: [10.1103/PhysRevA.71.022316](https://doi.org/10.1103/PhysRevA.71.022316). URL: <https://link.aps.org/doi/10.1103/PhysRevA.71.022316>.
- [28] D. Gottesman. “Theory of fault-tolerant quantum computation”. In: *Phys. Rev. A* 57 (1 1998), pp. 127–137. DOI: [10.1103/PhysRevA.57.127](https://doi.org/10.1103/PhysRevA.57.127). URL: <https://link.aps.org/doi/10.1103/PhysRevA.57.127>.
- [29] S. Bravyi, G. Smith, and J. A. Smolin. “Trading Classical and Quantum Computational Resources”. In: *Phys. Rev. X* 6 (2 2016), p. 021043. DOI: [10.1103/PhysRevX.6.021043](https://doi.org/10.1103/PhysRevX.6.021043). URL: <https://link.aps.org/doi/10.1103/PhysRevX.6.021043>.
- [30] M. Van den Nest, J. Dehaene, and B. De Moor. “Graphical description of the action of local Clifford transformations on graph states”. In: *Phys. Rev. A* 69 (2 2004), p. 022316. DOI: [10.1103/PhysRevA.69.022316](https://doi.org/10.1103/PhysRevA.69.022316). URL: <https://link.aps.org/doi/10.1103/PhysRevA.69.022316>.
- [31] M. Hein, J. Eisert, and H. J. Briegel. “Multipartite entanglement in graph states”. In: *Phys. Rev. A* 69 (6 2004), p. 062311. DOI: [10.1103/PhysRevA.69.062311](https://doi.org/10.1103/PhysRevA.69.062311). URL: <https://link.aps.org/doi/10.1103/PhysRevA.69.062311>.
- [32] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard. “Simulation of quantum circuits by low-rank stabilizer decompositions”. In: *Quantum* 3 (Sept. 2019), p. 181. ISSN: 2521-327X. DOI: [10.22331/q-2019-09-02-181](https://doi.org/10.22331/q-2019-09-02-181). URL: <https://doi.org/10.22331/q-2019-09-02-181>.
- [33] A. Kerzner. “Clifford simulation: Techniques and applications”. MA thesis. University of Waterloo, 2021. URL: <http://hdl.handle.net/10012/17038>.

- [34] S. Aaronson and D. Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A* 70.5 (2004), p. 052328. DOI: [10.1103/PhysRevA.70.052328](https://doi.org/10.1103/PhysRevA.70.052328). URL: <https://doi.org/10.1103/PhysRevA.70.052328>.
- [35] C. Gidney. “Stim: a fast stabilizer circuit simulator”. In: *Quantum* 5 (July 2021), p. 497. ISSN: 2521-327X. DOI: [10.22331/q-2021-07-06-497](https://doi.org/10.22331/q-2021-07-06-497). URL: <https://doi.org/10.22331/q-2021-07-06-497>.
- [36] H. Qassim, H. Pashayan, and D. Gosset. “Improved upper bounds on the stabilizer rank of magic states”. In: *Quantum* 5 (Dec. 2021), p. 606. ISSN: 2521-327X. DOI: [10.22331/q-2021-12-20-606](https://doi.org/10.22331/q-2021-12-20-606). URL: <https://doi.org/10.22331/q-2021-12-20-606>.
- [37] S. Peleg, A. Shpilka, and B. L. Volk. “Lower Bounds on Stabilizer Rank”. In: *Quantum* 6 (Feb. 2022), p. 652. ISSN: 2521-327X. DOI: [10.22331/q-2022-02-15-652](https://doi.org/10.22331/q-2022-02-15-652). URL: <https://doi.org/10.22331/q-2022-02-15-652>.
- [38] R. Raussendorf, D. E. Browne, and H. J. Briegel. “Measurement-based quantum computation on cluster states”. In: *Physical review A* 68.2 (2003), p. 022312. DOI: [10.1142/s0219749909005699](http://dx.doi.org/10.1142/s0219749909005699). URL: <http://dx.doi.org/10.1142/s0219749909005699>.
- [39] M. B. Elliott. *Stabilizer states and local realism*. 2008. DOI: [10.48550/arXiv.0807.2876](https://doi.org/10.48550/arXiv.0807.2876). arXiv: [0807.2876 \[quant-ph\]](https://arxiv.org/abs/quant-ph/0807.2876). URL: <https://doi.org/10.48550/arXiv.0807.2876>.
- [40] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. “Entanglement in graph states and its applications”. In: *Quantum computers, algorithms and chaos*. IOS Press, 2006, pp. 115–218. URL: <https://arxiv.org/abs/quant-ph/0602096>.
- [41] M. B. Elliott, B. Eastin, and C. M. Caves. “Graphical description of the action of Clifford operators on stabilizer states”. In: *Phys. Rev. A* 77 (4 2008), p. 042307. DOI: [10.1103/PhysRevA.77.042307](https://link.aps.org/doi/10.1103/PhysRevA.77.042307). URL: <https://link.aps.org/doi/10.1103/PhysRevA.77.042307>.
- [42] M. B. Elliott, B. Eastin, and C. M. Caves. “Graphical description of Pauli measurements on stabilizer states”. In: *Journal of Physics A: Mathematical and Theoretical* 43.2 (2009), p. 025301. DOI: [10.1088/1751-8113/43/2/025301](http://dx.doi.org/10.1088/1751-8113/43/2/025301). URL: <http://dx.doi.org/10.1088/1751-8113/43/2/025301>.
- [43] S. Anders and H. J. Briegel. “Fast simulation of stabilizer circuits using a graph-state representation”. In: *Phys. Rev. A* 73 (2 2006), p. 022334. DOI: [10.1103/PhysRevA.73.022334](https://link.aps.org/doi/10.1103/PhysRevA.73.022334). URL: <https://link.aps.org/doi/10.1103/PhysRevA.73.022334>.
- [44] H. J. García, I. L. Markov, and A. W. Cross. “Efficient Inner-product Algorithm for Stabilizer States”. In: (2013). DOI: [10.48550/arXiv.1210.6646](https://doi.org/10.48550/arXiv.1210.6646). arXiv: [1210.6646 \[CS, ET\]](https://arxiv.org/abs/1210.6646). URL: <https://doi.org/10.48550/arXiv.1210.6646>.
- [45] H. J. García, I. L. Markov, and A. W. Cross. “On the geometry of stabilizer states”. In: *arXiv preprint arXiv:1711.07848* (2017). DOI: [10.26421/qic14.7-8-9](https://doi.org/10.26421/qic14.7-8-9). URL: <http://dx.doi.org/10.26421/qic14.7-8-9>.

- [46] A. Steane. “Multiple-particle interference & quantum error correction”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 452.1954 (1996), pp. 2551–2577. DOI: [10.1098/rspa.1996.0136](https://doi.org/10.1098/rspa.1996.0136). URL: <https://doi.org/10.1098/rspa.1996.0136>.
- [47] A. R. Calderbank and P. W. Shor. “Good quantum error-correcting codes exist”. In: *Phys. Rev. A* 54 (2 1996), pp. 1098–1105. DOI: [10.1103/PhysRevA.54.1098](https://link.aps.org/doi/10.1103/PhysRevA.54.1098). URL: <https://link.aps.org/doi/10.1103/PhysRevA.54.1098>.
- [48] J.-P. Tillich and G. Zémor. “Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength”. In: *IEEE Transactions on Information Theory* 60.2 (2013), pp. 1193–1202. DOI: [10.1109/tit.2013.2292061](https://doi.org/10.1109/tit.2013.2292061). URL: <http://dx.doi.org/10.1109/tit.2013.2292061>.
- [49] N. P. Breuckmann and J. N. Eberhardt. “Balanced Product Quantum Codes”. In: *IEEE Trans. Inf. Theor.* 67.10 (Oct. 2021), pp. 6653–6674. ISSN: 0018-9448. DOI: [10.1109/TIT.2021.3097347](https://doi.org/10.1109/TIT.2021.3097347). URL: <https://doi.org/10.1109/TIT.2021.3097347>.
- [50] P. Panteleev and G. Kalachev. “Degenerate Quantum LDPC Codes With Good Finite Length Performance”. In: *Quantum* 5 (Nov. 2021), p. 585. ISSN: 2521-327X. DOI: [10.22331/q-2021-11-22-585](https://doi.org/10.22331/q-2021-11-22-585). URL: <https://doi.org/10.22331/q-2021-11-22-585>.
- [51] M. Sipser and D. A. Spielman. “Expander codes”. In: *IEEE transactions on Information Theory* 42.6 (1996), pp. 1710–1722. DOI: [10.1109/sfcs.1994.365734](https://doi.org/10.1109/sfcs.1994.365734). URL: <http://dx.doi.org/10.1109/sfcs.1994.365734>.
- [52] A. Y. Kitaev. “Fault-tolerant quantum computation by anyons”. In: *Annals of physics* 303.1 (2003), pp. 2–30. DOI: [10.1016/s0003-4916\(02\)00018-0](https://doi.org/10.1016/s0003-4916(02)00018-0). URL: [http://dx.doi.org/10.1016/s0003-4916\(02\)00018-0](http://dx.doi.org/10.1016/s0003-4916(02)00018-0).
- [53] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder. “High-threshold and low-overhead fault-tolerant quantum memory”. In: *Nature* 627.8005 (Mar. 2024), pp. 778–782. ISSN: 1476-4687. DOI: [10.1038/s41586-024-07107-7](https://doi.org/10.1038/s41586-024-07107-7). URL: <http://dx.doi.org/10.1038/s41586-024-07107-7>.
- [54] J. Edmonds. “Maximum matching and a polyhedron with 0, 1-vertices”. In: *Journal of research of the National Bureau of Standards B* 69.125-130 (1965), pp. 55–56. DOI: [10.6028/jres.069b.013](https://doi.org/10.6028/jres.069b.013). URL: <http://dx.doi.org/10.6028/jres.069b.013>.
- [55] J. Edmonds. “Paths, trees, and flowers”. In: *Canadian Journal of mathematics* 17 (1965), pp. 449–467. DOI: [10.4153/cjm-1965-045-4](https://doi.org/10.4153/cjm-1965-045-4). URL: <http://dx.doi.org/10.4153/cjm-1965-045-4>.
- [56] T. Bergamaschi, L. Golowich, and S. Gunn. “Approaching the Quantum Singleton Bound with Approximate Error Correction”. In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. STOC 2024. Vancouver, BC, Canada: Association for Computing Machinery, 2024, pp. 1507–1516. ISBN: 9798400703836. DOI: [10.1145/3618260.3649680](https://doi.org/10.1145/3618260.3649680). URL: <https://doi.org/10.1145/3618260.3649680>.
- [57] T. Rakovszky and V. Khemani. “The Physics of (good) LDPC Codes II. Product constructions”. In: (2024). DOI: [10.48550/arXiv.2402.16831](https://doi.org/10.48550/arXiv.2402.16831). arXiv: [2402.16831](https://arxiv.org/abs/2402.16831) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2402.16831>.

- [58] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman. “Asymptotically good quantum codes”. In: *Phys. Rev. A* 63 (3 2001), p. 032311. DOI: [10.1103/PhysRevA.63.032311](https://doi.org/10.1103/PhysRevA.63.032311). URL: <https://link.aps.org/doi/10.1103/PhysRevA.63.032311>.
- [59] P. Panteleev and G. Kalachev. “Asymptotically good quantum and locally testable classical LDPC codes”. In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 2022, pp. 375–388. DOI: [10.1145/3519935.3520017](https://doi.org/10.1145/3519935.3520017). URL: <http://dx.doi.org/10.1145/3519935.3520017>.
- [60] T. McElvanney and M. Backens. “Complete Flow-Preserving Rewrite Rules for MBQC Patterns with Pauli Measurements”. In: *Electronic Proceedings in Theoretical Computer Science* 394 (Nov. 2023), pp. 66–82. ISSN: 2075-2180. DOI: [10.4204/eptcs.394.5](https://doi.org/10.4204/eptcs.394.5). URL: <http://dx.doi.org/10.4204/EPTCS.394.5>.
- [61] S. Yu, Q. Chen, and C. H. Oh. “Graphical Quantum Error-Correcting Codes”. In: (2007). DOI: [10.48550/arXiv.0709.1780](https://doi.org/10.48550/arXiv.0709.1780). arXiv: [0709.1780](https://arxiv.org/abs/0709.1780) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.0709.1780>.
- [62] A. Kissinger. “Phase-free ZX diagrams are CSS codes (...or how to graphically grok the surface code)”. In: (2022). DOI: [10.48550/arXiv.2204.14038](https://doi.org/10.48550/arXiv.2204.14038). arXiv: [2204.14038](https://arxiv.org/abs/2204.14038) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2204.14038>.
- [63] Z. Wu, S. Cheng, and B. Zeng. “A ZX-Calculus Approach for the Construction of Graph Codes”. In: (2024). DOI: [10.48550/arXiv.2304.08363](https://doi.org/10.48550/arXiv.2304.08363). arXiv: [2304.08363](https://arxiv.org/abs/2304.08363) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2304.08363>.
- [64] N. Chancellor, A. Kissinger, S. Zohren, J. Roffe, and D. Horsman. “Graphical structures for design and verification of quantum error correction”. In: *Quantum Science and Technology* (2016). DOI: [10.1088/2058-9565/acf157](https://doi.org/10.1088/2058-9565/acf157). URL: <https://doi.org/10.1088/2058-9565/acf157>.
- [65] B. Coecke and R. Duncan. “Interacting quantum observables”. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2008, pp. 298–310. DOI: [10.1007/978-3-540-70583-3_25](https://doi.org/10.1007/978-3-540-70583-3_25). URL: https://doi.org/10.1007/978-3-540-70583-3_25.
- [66] T. Peham, L. Burgholzer, and R. Wille. “Equivalence Checking of Quantum Circuits With the ZX-Calculus”. In: *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 12.3 (2022), pp. 662–675. DOI: [10.1109/JETCAS.2022.3202204](https://doi.org/10.1109/JETCAS.2022.3202204). URL: <https://doi.org/10.1109/JETCAS.2022.3202204>.
- [67] A. Cowtan and S. Majid. “Quantum double aspects of surface code models”. In: *Journal of Mathematical Physics* 63.4 (2022), p. 042202. DOI: [10.1063/5.0063768](https://doi.org/10.1063/5.0063768). URL: <https://doi.org/10.1063/5.0063768>.
- [68] J. van de Wetering. “Constructing quantum circuits with global gates”. In: *New Journal of Physics* 23.4 (2021), p. 043015. DOI: [10.1088/1367-2630/abf1b3](https://doi.org/10.1088/1367-2630/abf1b3). URL: <https://doi.org/10.1088/1367-2630/abf1b3>.
- [69] R. D. East, J. van de Wetering, N. Chancellor, and A. G. Grushin. “AKLT-states as ZX-diagrams: diagrammatic reasoning for quantum states”. In: *PRX Quantum* 3.1 (2022), p. 010302. DOI: [10.1103/PRXQuantum.3.010302](https://doi.org/10.1103/PRXQuantum.3.010302). URL: <https://doi.org/10.1103/PRXQuantum.3.010302>.

- [70] N. de Beaudrap and D. Horsman. “The ZX calculus is a language for surface code lattice surgery”. In: *Quantum* 4 (2020), p. 218. DOI: [10.22331/q-2020-01-09-218](https://doi.org/10.22331/q-2020-01-09-218). URL: <https://doi.org/10.22331/q-2020-01-09-218>.
- [71] A. Kissinger and J. van de Wetering. “Reducing the number of non-Clifford gates in quantum circuits”. In: *Physical Review A* 102.2 (2020), p. 022406. DOI: [10.1103/PhysRevA.102.022406](https://doi.org/10.1103/PhysRevA.102.022406). URL: <https://doi.org/10.1103/PhysRevA.102.022406>.
- [72] M. Backens. “The ZX-calculus is complete for stabilizer quantum mechanics”. In: *New Journal of Physics* 16.9 (2014), p. 093021. DOI: [10.1088/1367-2630/16/9/093021](https://doi.org/10.1088/1367-2630/16/9/093021). URL: <https://doi.org/10.1088/1367-2630/16/9/093021>.
- [73] R. Duncan, A. Kissinger, S. Perdrix, and J. Van De Wetering. “Graph-theoretic Simplification of Quantum Circuits with the ZX-calculus”. In: *Quantum* 4 (2020), p. 279. DOI: [10.22331/q-2020-06-04-279](https://doi.org/10.22331/q-2020-06-04-279). URL: <https://doi.org/10.22331/q-2020-06-04-279>.
- [74] J. van de Wetering. “ZX-calculus for the working quantum computer scientist”. In: (2020). DOI: [10.48550/arXiv.2012.13966](https://doi.org/10.48550/arXiv.2012.13966). arXiv: [2012.13966](https://arxiv.org/abs/2012.13966) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2012.13966>.
- [75] R. Duncan and M. Lucas. “Verifying the Steane code with Quantomatic”. In: *arXiv preprint arXiv:1306.4532* (2013). DOI: [10.48550/arXiv.1306.4532](https://doi.org/10.48550/arXiv.1306.4532). URL: <https://doi.org/10.48550/arXiv.1306.4532>.
- [76] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne. “Benchmarking quantum computers: The five-qubit error correcting code”. In: *Physical Review Letters* 86.25 (2001), p. 5811. DOI: [10.1103/PhysRevLett.86.5811](https://doi.org/10.1103/PhysRevLett.86.5811). URL: <https://doi.org/10.1103/PhysRevLett.86.5811>.
- [77] V. G. Vizing. “On an estimate of the chromatic class of a p-graph”. In: *Diskret. Analiz.* 3 (1964), pp. 25–30. DOI: [10.1007/bf01885700](https://doi.org/10.1007/bf01885700). URL: <http://dx.doi.org/10.1007/bf01885700>.
- [78] J. Misra and D. Gries. “A constructive proof of Vizing’s theorem”. In: *Information Processing Letters* 41.3 (1992), pp. 131–133. DOI: [10.1016/0020-0190\(92\)90041-s](https://doi.org/10.1016/0020-0190(92)90041-s). URL: [http://dx.doi.org/10.1016/0020-0190\(92\)90041-s](http://dx.doi.org/10.1016/0020-0190(92)90041-s).
- [79] U. Kapshikar and S. Kundu. “On the hardness of the minimum distance problem of quantum codes”. In: *IEEE Transactions on Information Theory* 69.10 (2023), pp. 6293–6302. DOI: [10.1109/tit.2023.3286870](https://doi.org/10.1109/tit.2023.3286870). URL: <http://dx.doi.org/10.1109/tit.2023.3286870>.
- [80] R. Tanner. “A recursive approach to low complexity codes”. In: *IEEE Transactions on information theory* 27.5 (1981), pp. 533–547. DOI: [10.1109/tit.1981.1056404](https://doi.org/10.1109/tit.1981.1056404). URL: <http://dx.doi.org/10.1109/tit.1981.1056404>.
- [81] A. B. Khesin and J. Z. Lu. *graphcodes (GitHub Repository)*. URL: <https://github.com/jz-lu/graphcodes>.
- [82] A. Couvreur, N. Delfosse, and G. Zémor. “A construction of quantum LDPC codes from Cayley graphs”. In: *IEEE transactions on information theory* 59.9 (2013), pp. 6087–6098. DOI: [10.1109/isit.2011.6034209](https://doi.org/10.1109/isit.2011.6034209). URL: <http://dx.doi.org/10.1109/isit.2011.6034209>.

- [83] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill. “Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence”. In: *Journal of High Energy Physics* 2015.6 (2015), pp. 1–55. DOI: [10.1007/jhep06\(2015\)149](https://doi.org/10.1007/jhep06(2015)149). URL: [http://dx.doi.org/10.1007/jhep06\(2015\)149](http://dx.doi.org/10.1007/jhep06(2015)149).
- [84] R. W. Hamming. “Error detecting and error correcting codes”. In: *The Bell system technical journal* 29.2 (1950), pp. 147–160. DOI: [10.1002/j.1538-7305.1950.tb00463.x](https://doi.org/10.1002/j.1538-7305.1950.tb00463.x). URL: <http://dx.doi.org/10.1002/j.1538-7305.1950.tb00463.x>.
- [85] R. Cleve, D. Leung, L. Liu, and C. Wang. “Near-linear constructions of exact unitary 2-designs”. In: *arXiv preprint arXiv:1501.04592* (2015). DOI: [10.26421/qic16.9-10-1](https://doi.org/10.26421/qic16.9-10-1). URL: <http://dx.doi.org/10.26421/qic16.9-10-1>.
- [86] B. Coecke and R. Duncan. “Interacting quantum observables: categorical algebra and diagrammatics”. In: *New Journal of Physics* 13(4) (2011), p. 043016. DOI: [10.1088/1367-2630/13/4/043016](https://doi.org/10.1088/1367-2630/13/4/043016). URL: <http://dx.doi.org/10.1088/1367-2630/13/4/043016>.
- [87] M.-D. Choi. “Completely positive linear maps on complex matrices”. In: *Linear algebra and its applications* 10.3 (1975), pp. 285–290. DOI: [10.1016/0024-3795\(75\)90075-0](https://doi.org/10.1016/0024-3795(75)90075-0). URL: [http://dx.doi.org/10.1016/0024-3795\(75\)90075-0](http://dx.doi.org/10.1016/0024-3795(75)90075-0).
- [88] A. Jamiołkowski. “Linear transformations which preserve trace and positive semidefiniteness of operators”. In: *Reports on Mathematical Physics* 3.4 (1972), pp. 275–278. DOI: [10.1016/0034-4877\(72\)90011-0](https://doi.org/10.1016/0034-4877(72)90011-0). URL: [http://dx.doi.org/10.1016/0034-4877\(72\)90011-0](http://dx.doi.org/10.1016/0034-4877(72)90011-0).
- [89] J. C. Adcock, S. Morley-Short, A. Dahlberg, and J. W. Silverstone. “Mapping graph state orbits under local complementation”. In: *Quantum* 4 (Aug. 2020), p. 305. ISSN: 2521-327X. DOI: [10.22331/q-2020-08-07-305](https://doi.org/10.22331/q-2020-08-07-305). URL: <https://doi.org/10.22331/q-2020-08-07-305>.
- [90] M. Englbrecht, T. Kraft, and B. Kraus. “Transformations of Stabilizer States in Quantum Networks”. In: *Quantum* 6 (Oct. 2022), p. 846. ISSN: 2521-327X. DOI: [10.22331/q-2022-10-25-846](https://doi.org/10.22331/q-2022-10-25-846). URL: <https://doi.org/10.22331/q-2022-10-25-846>.
- [91] J. Huang, S. M. Li, L. Yeh, A. Kissinger, M. Mosca, and M. Vasmer. “Graphical CSS Code Transformation Using ZX Calculus”. In: *arXiv preprint arXiv:2307.02437* (2023). DOI: [10.4204/eptcs.384.1](https://doi.org/10.4204/eptcs.384.1). URL: <http://dx.doi.org/10.4204/eptcs.384.1>.
- [92] S. M. Li. “Graphical CSS Code Transformation Using ZX Calculus”. MA thesis. University of Waterloo, 2023. URL: <http://hdl.handle.net/10012/20193>.
- [93] D. Gottesman. “Class of quantum error-correcting codes saturating the quantum Hamming bound”. In: *Phys. Rev. A* 54 (3 1996), pp. 1862–1868. DOI: [10.1103/PhysRevA.54.1862](https://doi.org/10.1103/PhysRevA.54.1862). URL: <https://link.aps.org/doi/10.1103/PhysRevA.54.1862>.
- [94] M. H. Zarei. “Strong-weak coupling duality between two perturbed quantum many-body systems: Calderbank-Shor-Steane codes and Ising-like systems”. In: *Phys. Rev. B* 96 (16 2017), p. 165146. DOI: [10.1103/PhysRevB.96.165146](https://doi.org/10.1103/PhysRevB.96.165146). URL: <https://link.aps.org/doi/10.1103/PhysRevB.96.165146>.

- [95] A. M. Steane. “Enlargement of Calderbank-Shor-Steane quantum codes”. In: *IEEE Transactions on Information Theory* 45.7 (1999), pp. 2492–2495. DOI: [10.1109/18.796388](https://doi.org/10.1109/18.796388). URL: <http://dx.doi.org/10.1109/18.796388>.
- [96] P. K. Sarvepalli and A. Klappenecker. “Sharing classical secrets with Calderbank-Shor-Steane codes”. In: *Phys. Rev. A* 80 (2 2009), p. 022321. DOI: [10.1103/PhysRevA.80.022321](https://doi.org/10.1103/PhysRevA.80.022321). URL: <https://link.aps.org/doi/10.1103/PhysRevA.80.022321>.
- [97] R. J. Harris, N. A. McMahon, G. K. Brennen, and T. M. Stace. “Calderbank-Shor-Steane holographic quantum error-correcting codes”. In: *Phys. Rev. A* 98 (5 2018), p. 052301. DOI: [10.1103/PhysRevA.98.052301](https://doi.org/10.1103/PhysRevA.98.052301). URL: <https://link.aps.org/doi/10.1103/PhysRevA.98.052301>.
- [98] *Quantomatic*. <https://quantomatic.github.io/>. Accessed: August 5, 2023.
- [99] M. Bahramgiri and S. Beigi. “Enumerating the Classes of Local Equivalency in Graphs”. In: (2007). arXiv: [math/0702267](https://arxiv.org/abs/math/0702267) [math.CO]. URL: <https://arxiv.org/abs/math/0702267>.
- [100] A. Bouchet. “Recognizing locally equivalent graphs”. In: *Discrete Mathematics* 114.1–3 (Apr. 1993), pp. 75–86. ISSN: 0012-365X. DOI: [10.1016/0012-365x\(93\)90357-y](https://doi.org/10.1016/0012-365x(93)90357-y). URL: [http://dx.doi.org/10.1016/0012-365x\(93\)90357-y](http://dx.doi.org/10.1016/0012-365x(93)90357-y).
- [101] A. Poremba, Y. Quek, and P. Shor. “The Learning Stabilizers with Noise problem”. In: (2024). DOI: [10.48550/arXiv.2410.18953](https://doi.org/10.48550/arXiv.2410.18953). arXiv: [2410.18953](https://arxiv.org/abs/2410.18953) [quant-ph]. URL: <https://doi.org/10.48550/arXiv.2410.18953>.
- [102] B. Coecke and A. Kissinger. “Picturing quantum processes: A first course on quantum theory and diagrammatic reasoning”. In: *Diagrammatic Representation and Inference: 10th International Conference, Diagrams 2018, Edinburgh, UK, June 18-22, 2018, Proceedings 10*. Springer. 2018, pp. 28–31. DOI: [10.1007/978-3-319-91376-6_6](https://doi.org/10.1007/978-3-319-91376-6_6). URL: https://doi.org/10.1007/978-3-319-91376-6_6.