



Measurement-based quantum computation beyond qubits

Robert Ivan Booth

► To cite this version:

Robert Ivan Booth. Measurement-based quantum computation beyond qubits. Quantum Physics [quant-ph]. Sorbonne Université, 2022. English. NNT : 2022SORUS022 . tel-03867179

HAL Id: tel-03867179

<https://theses.hal.science/tel-03867179>

Submitted on 23 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



SORBONNE UNIVERSITÉ - EDITE DE PARIS

*Laboratoire d'informatique de Sorbonne Université (LIP6) /
Quantum Information
Laboratoire lorrain de recherche en informatique et ses applications /
Equipe Mocqua*

Measurement-based quantum computation beyond qubits

with applications to higher-dimensional and
continuous-variable quantum systems

ROBERT IVAN BOOTH

PHD THESIS IN COMPUTER SCIENCE

SUPERVISED BY DAMIAN MARKHAM AND SIMON PERDRIX

Publicly defended in February 2022, with a jury consisting in:

- MARKHAM Damian, Chargé de Recherche au CNRS, Sorbonne Université, *Directeur de thèse*

- PERDRIX Simon, Directeur de Recherche Inria, Loria, *Superviseur de thèse*

This work is licensed under the [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

ABSTRACT

Understanding the fundamental structures at play in quantum computation is a key issue in the development of quantum technologies. Such an understanding provides tools for reasoning about the potential and limits of quantum computers. It is also critical when reasoning about computational architectures for physical implementations, and in minimising the different resources required.

Measurement-based quantum computation (MBQC) is an alternative model for quantum computation, which makes careful use of the properties of the measurement of entangled quantum systems to perform transformations on an input. It differs fundamentally from the standard quantum circuit model in that measurement-based computations are naturally irreversible. This is an unavoidable consequence of the quantum description of measurements, but begets an obvious question: when does an MBQC implement an effectively reversible computation? The measurement calculus is a formal framework for reasoning about MBQC which encodes a computation as a sequence of logical commands and with the remarkable feature that every computation can be related in a canonical way to a graph. This allows one to use graph-theoretical tools to reason about MBQC problems, such as the reversibility question, and the resulting study of MBQC has had a large range of applications.

However, the vast majority of the work on MBQC has focused on architectures using the simplest possible quantum system: the qubit. It remains an open question how much of this work can be lifted to other quantum systems. In this thesis, we begin to tackle this question, by introducing analogues of the measurement calculus for higher- and infinite-dimensional quantum systems. More specifically, we consider the case of qudits when the local dimension is an odd prime, and of continuous-variable systems familiar from the quantum physics of free particles. In each case, a calculus is introduced and given a suitable interpretation in terms of Hilbert space operations. We then relate the resulting models to the standard circuit models, using graph-theoretical tools called “flow” conditions. In the finite-dimensional case, this amounts to the study of outcome determinism—deciding when it is possible to eliminate the probabilistic nature of the measurements by using outcome-dependant corrections on the resulting state. In CV, we must treat the subtler question of convergence, since there MBQCs are only ever an approximation to the desired operation, and it is necessary to ensure one recovers the desired computation in some ideal limit.

DEDICATION AND ACKNOWLEDGEMENTS

I have spent over three years working on the research in this thesis, and to be quite honest I am a bit shocked to have reached the finish line. I am deeply grateful to my doctoral advisors Damian and Simon for the time and passion they have invested in me. They offered me the perfect balance between guidance and the freedom to pursue my own research goals, and, despite all complications, have always made time for me when I needed it. I am also thankful to the member of my jury, Claudia Faggian, Elham Kashefi and Ross Duncan and especially to Robert Raußendorf and Dan Browne who graciously agreed to be rapporteurs.

Of course, many people have helped me out along the way: Mike Ashfold, who gave me a chance when I really didn't deserve it; Thibaut Jacqmin, Nicolas Treppe and Marco Barbieri, who introduced me to the field of quantum information. I must also thank my co-authors, Aleks Kissinger, Clément Meignant, Pierre-Emmanuel Emeriau and Ulysse Chabaud, as well as my mentors, Tom Douce, Shane Mansfield, Vladimir Zamdzhiev and Titouan Carette. I am profoundly grateful to Kae Nemoto for hosting my visit at the National Institute of Informatics in Tokyo.

At LIP6 I discovered a group of people who became both inspiring colleagues and amazing friends, and who made my time here infinitely more fun: Clément and your damn towel, Nate, Ulysse and the mouth exerciser—the Japan crew—Raja, Luka, Pierre-Emmanuel, Alisa—from the “cool” office—Leo, Francesco, Mattieu, Tom, Shane, Anu, Niraj, Andrea, Shraddha, Rhea, Natansh, Vic, Fede, Simon, Dom, Damien, Matteo, Cyril, Yoann, Verena, Laura, Paul, Rawad, Uta, Armando, Vlad, and all the others I'm surely forgetting.

Thanks also to my lifelong friends Dumas, Dave, Harriet, Annie, Chris, Anki, Boaz, Lydvi, Sid, Lee, Baptiste, Arsène for occasionally reminding me that there is, in fact, a world outside of research and quantum.

Finally, thanks to my parents and sister for bearing with my eccentricities and always supporting me in whatever I do.

TABLE OF CONTENTS

Table of Contents	5
Introduction	8
Summary of results	13
Publications	16
1 Mathematical preliminaries	17
1.1 Hilbert spaces	17
1.1.1 Operators on Hilbert spaces	20
1.1.2 Some important classes of operators	21
1.1.3 The spectral theorem and functional calculi	22
1.1.4 Tensor products	23
1.2 Pure state quantum mechanics	25
1.3 Mixed state quantum mechanics	26
1.3.1 Quantum channels	28
2 Models of quantum computation with qudits	31
2.1 The quantum circuit model	32
2.1.1 Reversible quantum circuits	33
2.1.2 State preparation and measurements	35
2.2 The measurement calculus	36
2.2.1 Measurement spaces	36
2.2.2 Measurement patterns	39
2.2.3 Semantics and determinism	42
2.2.4 Causal flow	43
2.3 Graph states	45
3 Robust determinism in MBQC with qudits	46
3.1 $\mathbb{Z}_d$ -flow is sufficient for robust determinism	47
3.1.1 Recovering gflow	49
3.2 $\mathbb{Z}_d$ -flow is necessary for robust determinism	50

3.2.1	A technical lemma	51
3.2.2	Proof of the converse theorem	60
3.3	A polynomial-time algorithm for $\mathbb{Z}_d$ -flow	62
3.3.1	Correctness	63
3.3.2	Depth optimality	65
	Conclusion and outlook	70
4	Circuit extraction for simple $\mathbb{Z}_d$-flows	71
4.1	Preliminaries	72
4.1.1	Composing measurement patterns	72
4.1.2	Graph-circuit hybrid diagrams	74
4.1.3	Extracting gate teleportations	75
4.1.4	A reformulation of simple $\mathbb{Z}_d$ -flow	78
4.2	Star pattern transformation	80
4.3	Triangularising $\mathbb{Z}_d$ -flow	82
4.3.1	From simple $\mathbb{Z}_d$ -flow to causal flow	83
4.3.2	The extraction algorithm	86
4.4	A worked out example	87
	Conclusion and outlook	90
5	Circuit extraction for extended $\mathbb{Z}_d$-flows	91
5.1	Manipulating $\mathbb{Z}_d$ -flows with local Cliffords	93
5.1.1	Local scaling	93
5.1.2	Local complementation	96
5.2	Quantum circuit extraction subprocesses	102
5.2.1	Extracting edges between outputs	103
5.2.2	Removing intermediate measurement spaces	104
5.2.3	Diagonalising extended $\mathbb{Z}_d$ -flow	107
5.2.4	Correctness of the extraction algorithm	109
5.2.5	Discarding subgraphs disconnected from the outputs	112
5.3	The extraction algorithm	113
5.4	Some worked out examples	114
5.4.1	The Z -rotation gadget	114
5.4.2	The total graph	116
	Conclusion and outlook	117
6	Convergence in CV MBQC	119
6.1	Preliminaries	120
6.2	The gate teleportation protocol	122
6.3	CV-MBQC and $\mathbb{R}$ -flow	127
6.4	CV-MBQCs with simple $\mathbb{R}$ -flow converge	131

TABLE OF CONTENTS

6.4.1	Star pattern transformation	132
6.4.2	Simple $\mathbb{R}$ -flow triangularisation	134
6.5	A worked-out example	141
	Conclusion and outlook	143
	Conclusion, outlook and unresolved problems	145
	Bibliography	149

INTRODUCTION

The advent of quantum mechanics at the start of the last century marked a turning point in our understanding of the behaviour of matter. The old physical theories [Max61; Boh13] were either swept aside or needed to be considered anew within the models [Sch26; Hei25; DF26] being developed to fit previously unexplained experimental phenomena [Pla01; Ein05; DG28]. The subsequent developments have led to a much deeper understanding of many domains, from chemistry, through nuclear physics, to electronics and many others. Such was its impact that it has been retroactively called “the quantum revolution” [Pea08]. It is also not unfair to say that whole areas of mathematical research, such as the theories of Hilbert spaces [von30] and operator algebras [MN36], would not exist, or certainly not in their modern form, were it not for their connection with the burgeoning quantum theory.

The realisation that the properties of quantum systems could be used to encode and manipulate information as one would with a computer, and that it might actually be possible to extract some kind of advantage from such a procedure, came later. It is often tracked back to an early 1970s manuscript of Stephen Wiesner, “Conjugate Coding”, or more prosaically to Richard Feynman’s famous 1981 lecture at MIT. He suggested that simulation of quantum systems would require building simulators of a quantum nature, and the field was set for the “second quantum revolution”, of quantum information and quantum technology.

Early on, Benioff [Ben80; Ben82], followed by Deutsch [Deu85], realised that the computing machines of Turing [Tur36] could be given a grounding in the systems described by classical physics. Turing machines are an abstract model for a computer which forms the foundation of much of classical computability and complexity theory. By reinterpreting what it means for a system to compute a function, Deutsch introduced quantum Turing machines (QTM) which were the first formal model for quantum computation. In formulating such a machine, he used a quantum generalisation of the bits familiar from classical computation theory, later dubbed the “qubit”, or quantum bit [Sch95]. Soon enough followed the first quantum algorithms which demonstrated an advantage over any known classical alternative [DJ92; Sho94; Gro96; Sho97], as well as the first theoretical results

separating classes of computational problems solvable using classical computers from those involving quantum computers [BB94; BV93].

The year 1993 saw two seemingly unrelated results which are of particular importance to this thesis. Building off of the work of Deutsch, Bernstein and Vazirani, Chi-Chih Yao [Chi93] introduced a circuit model for quantum computers, analogous to the Boolean circuit model for classical computation, and showed that (under some natural assumptions) it was equivalent to the QTM model. This model has stood the test of time, and today the majority of results in quantum computation are formulated in terms of quantum circuits.

The same year, Bennett et al. [Ben+93] published the *quantum state teleportation* protocol, which makes use of a key property of quantum systems, *entanglement*. It is well-established that measuring a quantum system in some sense destroys it. They showed that, using an entangled pair of quantum systems a and b at respective physical locations A and B , the state of a could, after being destroyed through measurement, be recovered at the system b , without the state being known either at A or B , nor being transported along any physical path from A to B . This protocol was realised experimentally in 1997 by Bouwmeester et al. [Bou+97].

Variations on this idea, such as the *quantum gate teleportation* protocol [ZLC00], allow one to teleport a quantum state while also applying a programmable transformation on that state [GC99]. This of course makes it possible to consider architectures where computations are carried out using destructive measurements to implement such programmable operations on an input state. These measurement-based models of computation stand in contrast to the QTM and quantum circuits in one major way. Where any computation in those models is *reversible*, in that running the computation backwards recuperates the initial input state, measurement-based models are *irreversible*, since measurements remove systems from the computation.

Such models are placed under the umbrella term *measurement-based quantum computation* (MBQC), and further can mostly be placed into two (non-exclusive) categories: MBQC by consumption of entanglement [RB01; RBB02; RB02; RBB03; Nie06; Bri+09; BB16]; and MBQC by projective measurements [Nie03; Leu02; Leu04; Per05]. These models are essentially equivalent in terms of the computations that they can implement [AL04; JP05], although they have different operational interpretations. In MBQC by consumption of entanglement, one typically operates by constructing a highly entangled state involving multiple quantum systems (a reversible process), before performing a series of subsequent measurements to enact the desired computation. On the other hand, in MBQC by measurements only, one uses *entangling measurements*, and it is therefore not necessary in principle to have access to any reversible entangling operations.

MBQC offers a distinct set of advantages and disadvantages in terms of implementation difficulties when compared to reversible models. For example, in

quantum computation, it is necessary to be able to perform entangling operations to obtain any kind of quantum advantage over classical computers, and they are one of the harder types of operations to implement. MBQC permits one to generate all necessary entanglement at the start of the computation, rather than needing access to entangling operations throughout a computation. On the other hand, this makes it important to maintain that entanglement, with at most minor losses, until the computation completes. MBQC is also a promising architecture for fault-tolerant quantum computation [RHG06; Men14]. Beyond offering an alternative computational model for implementations of quantum computers, the ideas behind MBQC have been applied to a surprising variety of problems. For example, they have been used in quantum foundations, as a discrete toy model for general-relativistic space-time [Rau+11], to study the fundamental quantum behaviors which give rise to computational advantages [Rau13; LDR15; Ber+17; FRB18], and related to closed time-like curves in quantum computation [dGK11].

The *measurement calculus* [DKP07] is a formal model for reasoning about MBQC and whose primitives closely relate to those of MBQC by consumption of entanglement. It encodes a computation as an abstract sequence of commands, called a *measurement pattern*, which is interpreted in terms of manipulations (including measurements) carried out on a register of qubits. The overall computation carried out by the MBQC, called its *semantics*, is in general not reversible, and this leads to the questions: when does a measurement pattern implement a reversible computation, and how does the measurement calculus relate to the other reversible models? The problem is essentially that measurements in quantum mechanics are probabilistic, and in general the semantics of the pattern is reversible only if this randomness can be eliminated. One remarkable feature is that every measurement pattern can be related in a canonical way to a graph, and this allows one to use graph-theoretic techniques to reason about MBQC. *Causal flow* [DK06] and *g-flow* [Bro+07] are graph-theoretical conditions introduced to treat the problem of reversibility. The problem can be re-framed in terms of *outcome determinism*, which eliminates this measurement randomness. They introduced a strong form of determinism, *robust determinism*, and it has been shown that a measurement pattern is robustly deterministic if and only if the underlying graph has g-flow [PSM]. These results have been extended to show how to obtain a quantum circuit equivalent to any robustly deterministic measurement pattern [BK09; MHM15; Dun+20; Bac+21; Sim21].

Flow conditions were essential in formulating blind quantum computation protocols [dGK11; Man+17], as well as estimating the depth advantages of MBQC over quantum circuits [BK09; BKP09; MHM15] and have also been used to study the classical simulatability of quantum computations [MK14]. More recently, there has been an interest in using flow conditions in the context of the ZX-calculus. The

ZX-calculus is a diagrammatic language for reasoning about quantum operations [CD11; CK17; van20]. It differentiates itself from quantum circuits by having a particularly nice set of identities (or rewrite rules) which can be used to prove any equality of quantum operations in the qubit setting [Bac14; JPV17; NW17; Vil19]. However, this comes at a major cost: in general a ZX-diagram cannot be straightforwardly related to computation in the QTM or circuit models. It turns that they *can* be related to MBQCs, and then flow conditions can sometimes be used to extract a quantum circuit from a ZX-diagram [Dun+20; Bac+21].

The literature on MBQC has therefore been quite extensive, but falls short in one way: it has been restricted mostly to the case of qubits, where quantum theory allows for many other types of systems. As its title suggests, this thesis is concerned with extending the previous work on the measurement calculus beyond the setting of qubits. We will consider the case of *qudits*, which are a quantum version of the dit or d -state bit, and of *continuous variables*, which means tackling some of the problems of infinite-dimensional quantum theory. We show that in either case, a slightly modified measurement calculus can be given a suitable semantics, and introduce flow conditions for each case. We then use these flow conditions to show that the corresponding MBQC is equivalent to a quantum circuit, and construct an explicit quantum circuit extraction algorithm for each case.

Qudit quantum computation

Qudit quantum computation, of course, is quantum computation where the qubits are replaced with qudits. Since qubits are modelled as two-dimensional vector spaces, and qudits correspond to d -dimensional vector spaces for an integer d , studying qudit quantum computation involves some subtler mathematics. When d is a prime number, these mathematics exhibit many similarities to the qubit case [Got99; de 12], and this is the case on which we shall concentrate.

In principle, many physical systems are qudits, and so it makes little sense to discard them outright because of their relative complexity. In fact, in some physical implementations, qubits are encoded into naturally d -level systems by ignoring all but the first two levels [Fri+18; Kli+03]. Some proof-of-concept experiments have begun to explore the various qudit systems available [BW08; Nee+09; Erh+18; Gao+19], opening the way for the construction of qudit-based quantum computers.

From a complexity-theoretic perspective, little work has been done on qudits. This can be mostly attributed to the fact that we cannot expect to obtain a super-polynomial speed-up over the qubit case. That said, recent work suggests that it is possible to reduce the depth of quantum circuits asymptotically compared to the qubit case by using qutrits (for which $d = 3$) [Gok+19]. This of course beats the constant improvement owed to the binary-to-ternary compression, and suggests there is more to be discovered in yet higher dimensions, as seen in [Kik+20]. Results

have also been obtained for improved noise tolerance in quantum key distribution with qudits [CGL99], as well as for the size of optimal quantum error correcting codes [BT00; Cer+02; SS10]. Furthermore, if one wants to work with registers of n qubits as fundamental data structure, rather than acting directly on the qubits themselves, then such a register can be represented as a qudit of dimension $d = 2^n$, and results obtained for qudits naturally cover this case.

Qudit MBQC has seen even less work. A recent review paper [Wan+20] states “measurement-based qudit quantum computing is unexplored to date.” It is straightforward to see that quantum teleportation can be adapted for qudits, and preliminary work has been done on generalising graph states to the qudit setting [Zho+03; BB07a]. These qudit graph state have been realised experimentally [Rei+19]. To my knowledge, our papers on the subject [Boo+21; BP21] are the first formal study of qudit MBQC.

Continuous variable quantum computation

Continuous-variable (CV) quantum computation¹ can broadly be defined as quantum computation where information is encoded in the state of a collection of quantum particles in free space [LB99; BP03; Bv05]. Such a quantum system is typically modelled as a specific type of *infinite-dimensional* vector space known as a *Hilbert space* [Hal13]. It is necessary to introduce such infinities in order to obtain a description which allows for unbounded positions and momenta as observable quantities. This comes at a cost: the theory of Hilbert spaces is much more mathematical in order to tame these infinities.

Nevertheless, CV quantum computation has been an active area of research in the last twenty years. The CV equivalent of the qubit is often called a qumode, because the mathematics of a free quantum particle are identical to those of a quantization mode of the electromagnetic field [FT20], and there is an entirely analogous CV quantum circuit description for computations. It was established early on that an intelligent encoding of qubits into qumodes yields a performant quantum error correction code by taking advantage of the inherent redundancy in such an encoding [GKP01]. This has lead to one of the main classes of quantum error correcting codes [Mic+16; Alb+18], and aroused interest in CV architectures which take advantage of them [Men14; SCC19; FAF20].

¹There is an unfortunate overloading of the term “continuous variables” in the literature. We mean the model of quantum computation introduced by Lloyd and Braunstein [LB99] and which encodes information in the position and momentum observables of particles in free space. This is not to be confused with the more generic term referring to computation where the observable quantities correspond to real numbers rather than integers. The model of Lloyd and Braunstein is one such model but there are in theory many others.

CV computation also has implementational advantages over the discrete variable case. As far as I know, the largest entangled states observed experimentally to date (in terms of number of involved systems) remain those obtained in CV optical experiments using time-multiplexing, beating their discrete counterparts by many orders of magnitude [Yok+13; Yos+16]. That said, there of course remain challenges to a CV quantum computer. Firstly, while it is relatively easier to generate entanglement in CV, there are other operations necessary for quantum speed-up, dubbed *non-Gaussian* operations. They are much more difficult to obtain since they correspond to interactions typically observed only at very high energies or in very specific states of matter, although some progress has been made on this aspect [Miy+16; Kon+21a; Kon+21b]. Secondly, genuinely CV quantum error correction codes have proved elusive. This is partially because it has been shown that no satisfactory CV code is possible without non-Gaussian operations [ESP02; NFC09; Vui+19], but even when assuming access to such operations, results tackling natural classes of errors have only recently been obtained [NGJ20; Hao+21].

CV MBQC fares somewhat better than the qudit case. There are once again analogous protocols for teleporting CV quantum states [BK98] while enacting corresponding programmable transformations, and these can be used to define CV MBQC in an approach close to MBQC by consumption of entanglement. This has been used to define CV graph states [ZB06; MFv11], and describe a CV one-way quantum computer [Men+06; Gu+09]. One of the main issues in CV MBQC is that the gate teleportation, and by extension more general measurement-based computations, can only be obtained physically as an approximation to the desired, ideal protocol. This complication can be treated in different ways [SWB18], but we treat it as a problem of mathematical convergence of the physical protocol to the ideal one [Wil18; PLB18; SH08]. This means more generality in the types of computations which can be considered, but we must settle for somewhat weaker conclusions and more technical proofs.

Summary of results

After a preliminary chapter 1, chapters 2 to 5 generalise the qubit theory to qudit MBQC for odd prime dimensions. Chapter 6 is concerned with continuous variable MBQC. The dependencies between chapters is mostly linear, although chapter 6 repeats multiple results from chapter 4, albeit in a somewhat altered setting. We detail the contents of each chapter in what follows.

Chapter 1 A preliminary chapter, which details the results we need from the mathematical theory of Hilbert spaces. All of these statements can be found in

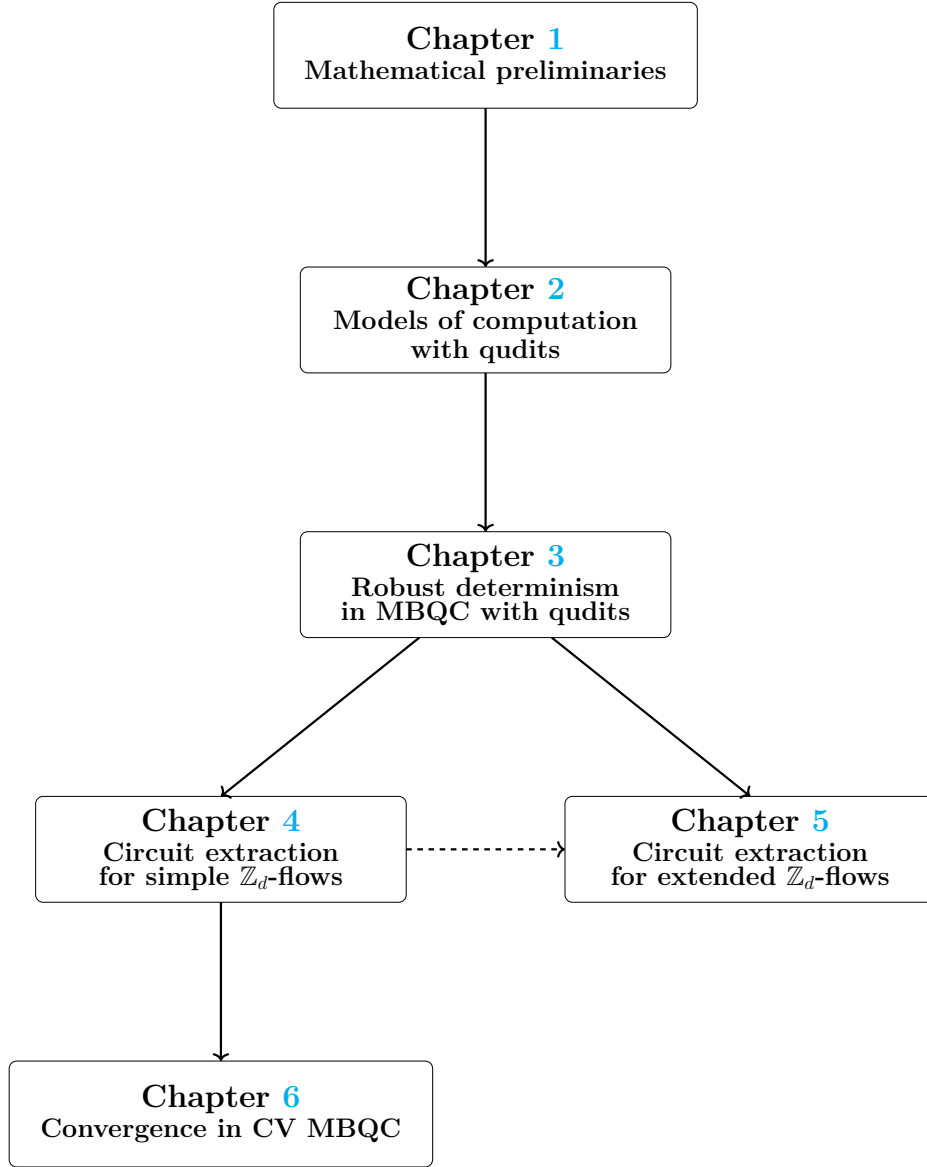


Figure 0.2: Breakdown of chapter interdependencies. Chapter 5 does not depend on any of the results of chapter 4, but there many similar techniques are applied in a much simpler setting. Chapter 6 could in principle be read immediately after chapter 1, but the chapters leading up to it build up ideas and intuition without which the chapter would lack a lot of motivation.

standard textbooks on the matter, but I found it convenient to collect them in a single place to reference from other chapters. We also detail the axioms of quantum mechanics for both pure and mixed states.

Chapter 2. This chapter introduces the measurement calculus for qudits. It is first necessary to introduce measurement spaces, labelled collections of measurements which are each associated to a predetermined “correction” operator. These spaces are thoroughly characterised, then used to define qudit measurement patterns (the terms of the measurement calculus), and their Hilbert space semantics. We then discuss determinism, relate measurement patterns to edge-weighted graphs, and define qudit graph states.

Chapter 3. After introducing our novel qudit flow condition, $\mathbb{Z}_d$ -flow, we show that it recovers g-flow in the case $d = 2$. We then prove that a qudit measurement pattern is robustly deterministic if and only if the underlying open graph has $\mathbb{Z}_d$ -flow. Finally, we present a polynomial-time algorithm that finds a $\mathbb{Z}_d$ -flow for an open graph whenever it has one, and show that the resulting MBQC has optimal computational depth.

Chapter 4. The first chapter on the circuit extraction problem. We produce a circuit extraction procedure for measurement patterns with *simple* $\mathbb{Z}_d$ -flow. To do so, we first show how to use *star pattern transformation* to extract a circuit from a causal flow, then relate any simple $\mathbb{Z}_d$ -flow to a sequence of causal flows. The chapter also introduces circuit-graph hybrid diagrams, which are used to represent partially extracted patterns, and shows how to sequentially compose two patterns.

Chapter 5. This chapter presents a quantum circuit extraction algorithm for any $\mathbb{Z}_d$ -flow. First, we need to consider the action of local-Clifford operations on measurement patterns with $\mathbb{Z}_d$ -flows and their semantics, which we decompose as *local scalings* and *local complementations*. This action is then used in formulating the extraction algorithm, along with some ideas from chapter 4. We conclude with some more worked out examples and a discussion of possible improvements.

Chapter 6. Continuous variable MBQC presents some different problems than the qudit case. We first prove the convergence of the CV quantum gate teleportation protocol, then show how to give a semantics and *squeezing*-dependant semantics for CV-MBQC. Then, we introduce $\mathbb{R}$ -flow, and adapt the circuit extraction algorithm of chapter 4 to show that every CV measurement pattern with $\mathbb{R}$ -flow converges to a unitary in the infinite-squeezing limit.

Publications

This thesis is based on the results contained in the following papers:

- Robert I. Booth and Damian Markham. “Flow Conditions for Continuous Variable Measurement-Based Quantum Computing”. Submitted to Quantum, Apr. 2021. arXiv: [2104.00572](#)
- Robert I. Booth et al. “Outcome Determinism in Measurement-Based Quantum Computation with Qudits”. Submitted to Quantum, Sept. 2021. arXiv: [2109.13810](#)
- Robert I. Booth and Simon Perdrix. “Extracting Reversible Circuits from Measurement-Based Quantum Computations with Higher-Dimensional Systems”. In preparation, 2021

MATHEMATICAL PRELIMINARIES

We begin, as all theses in quantum information must, with a discussion of the axioms of quantum mechanics. This will serve in part as a refresher for our kind readers, but mostly to introduce notations and conventions used throughout the remaining chapters. Our presentation follows the so-called mathematical formulation of quantum mechanics, started by John von Neumann in the late 1920s.

He found that the nascent theory of Hilbert spaces and their linear operators provided a natural mathematical framework for unifying the different attempts at explaining the observations of quantum physics which had been made in the previous years [von27; von30]. These ideas were neatly summarised in his book [von32; von18], and we present them here. The books of Brian C. Hall [Hal13] and of Valter Moretti [Mor17] were also extensively consulted throughout the writing of this thesis. The material on mixed state quantum theory is harder to find in one place. Amongst the best sources are the textbooks of Karl Kraus [Kra83], Alexander Holevo [Hol01] and Masahito Hayashi [Hay17]. All results in this chapter are stated without proof, since they can be found in many textbooks, including those cited.

1.1 Hilbert spaces

Hilbert spaces generalise the Euclidian spaces familiar from classical geometry, and conserve many of their properties. They also provide a good model for the states of a quantum system.

Definition 1.1. A Hilbert space is a $\mathbb{C}$ -linear space $\mathcal{H}$, along with an inner product $\langle -, - \rangle_{\mathcal{H}} : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$ such that for any $x, y, z \in \mathcal{H}$ and $\lambda \in \mathbb{C}$,

- $\langle x, y \rangle = \overline{\langle y, x \rangle}$;
- $\langle x, y + \lambda z \rangle = \langle x, y \rangle + \lambda \langle x, z \rangle$;
- $\langle x, x \rangle = 0$ if and only if $x = 0$;

and furthermore $\mathcal{H}$ is complete with respect to the norm $\|x\|_{\mathcal{H}} = \sqrt{\langle x, x \rangle}$.

We make the somewhat unconventional choice of taking the inner product to be right-linear (and thus, left-antilinear), which matches the “bra-ket” notation common in the quantum information and quantum physics literature. When the Hilbert space is clear, we will drop the indices and simply write $\langle x, y \rangle$ and $\|x\|$ for the inner product and norm.

Example 1.2. A first example of Hilbert space is given by $\mathbb{C}^d$ for any $d \in \mathbb{N}$, with its usual complex inner product: $\langle x, y \rangle = \sum_{n=1}^d \overline{x_n} y_n$. Later, we shall call a system modelled by such a Hilbert space a *qudit*.

Example 1.3. Extending this construction, consider the space $\ell^2(\mathbb{N})$ of infinite sequences $(x_n)_{n \in \mathbb{N}}$ such that

$$\sum_{n \in \mathbb{N}} |x_n|^2 < \infty, \quad (1.1)$$

with element-wise operations and inner product

$$\langle x, y \rangle = \sum_{n \in \mathbb{N}} \overline{x_n} y_n. \quad (1.2)$$

$\ell^2(\mathbb{N})$ is a Hilbert space called the space of square-summable sequences.

Example 1.4. Let (X, μ) be a measure space, and write $\mathcal{L}^2(X, \mu)$ the space of functions $f : X \rightarrow \mathbb{C}$ such that

$$\int_X |f(x)|^2 d\mu(x) < \infty \quad (1.3)$$

with point-wise operations and with an inner product given by

$$\langle f, g \rangle = \int_X \overline{f(x)} g(x) d\mu(x), \quad (1.4)$$

Define an equivalence relation

$$f \sim g \quad \text{if} \quad \langle f - g, f - g \rangle = 0, \quad (1.5)$$

then the quotient space $\mathcal{L}^2(X, \mu) := \mathcal{L}^2(X, \mu) / \sim$ is a Hilbert space called the space of square-integrable functions on (X, μ) where the inner product is given by calculating (1.4) on representatives.

If G is a Hausdorff locally compact abelian group, then there is a unique translation invariant measure on G , the *Haar measure* μ_G , and we will write $\mathcal{L}^2(G) := \mathcal{L}^2(G, \mu_G)$. Of particular interest in the final chapter of this thesis is $\mathcal{L}^2(\mathbb{R})$, which will model the state space of a single particle with one degree of freedom. Borrowing from quantum optics, we shall call such a quantum system a *qumode*.

There is one subtlety here: we will frequently make arguments viewing elements of $\mathcal{L}^2(\mathbb{R})$ as actual functions $\mathbb{R} \rightarrow \mathbb{C}$, but it must be understood that these implicitly correspond to representatives of the $\sim$ -equivalence classes and that one must be careful that the arguments lift to the quotient.

It was a key result of the early work of von Neumann that despite quite different constructions, many of these Hilbert spaces coincide.

Definition 1.5. *An isomorphism of Hilbert spaces is a bijective linear map $\mathcal{H} \rightarrow \mathcal{I}$ which furthermore preserves the norm. In this case, we say that $\mathcal{H}$ and $\mathcal{I}$ are isomorphic and we write $\mathcal{H} \cong \mathcal{I}$.*

It turns out that all of the examples of Hilbert spaces introduced above have an important property: they contain countable dense subsets (w.r.t. the topology generated by the norm). Leveraging this property, called *separability*, von Neumann showed that:

Proposition 1.6. *A separable Hilbert space has an orthonormal basis of at most countable cardinality.*

This in turn implies the following isomorphisms, by identifying basis elements:

$$\mathcal{L}^2(\mathbb{Z}_d) \cong \mathbb{C}^d \quad \text{and} \quad \mathcal{L}^2(\mathbb{R}) \cong \ell^2(\mathbb{N}). \quad (1.6)$$

All the Hilbert spaces we will encounter from chapter 2 onwards will take one of these two forms. In the case of finite-dimensional Hilbert spaces, we use the *Dirac* notation for representing elements of the Hilbert space: a state $\psi \in \mathcal{L}^2(\mathbb{Z}_d)$ is written $|\psi\rangle$. $\langle\psi|$ represents the map $\mathcal{L}^2(\mathbb{Z}_d) \rightarrow \mathbb{C} : \phi \mapsto \langle\psi, \phi\rangle$, and in particular, $\langle\psi|\phi\rangle = \langle\psi, \phi\rangle$. We avoid using this notation for infinite-dimensional Hilbert spaces as it is not as practical. We will often need to consider a representative function for a state, and the Dirac notation is unwieldy for that purpose: we either use $\phi(x) = \langle x|\phi\rangle$, which implies that $|x\rangle \in \mathcal{L}^2(X)$, but there is (in general) no such vector, or $\phi(x) = |\phi\rangle(x)$ which is notationally confusing. We chose to use neither and skip the Dirac notation altogether in Hilbert spaces of functions.

1.1.1 Operators on Hilbert spaces

An *operator*, or linear operator, is a linear map $\mathcal{H} \rightarrow \mathcal{I}$ between Hilbert spaces. While Hilbert spaces are fairly “nice” objects (in that they preserve most of the properties of finite-dimensional vector spaces), this is not the case for their linear operators. As we shall see towards the end of this thesis, many of the operators which come up naturally in quantum physics exhibit some of these complications.

It is then useful to consider operators which are not defined on the whole of $\mathcal{H}$, but only on a (dense) subspace. In that case, we shall write $D(T) \subseteq \mathcal{H}$ the domain of the operator $T : \mathcal{H} \rightarrow \mathcal{I}$. As is standard, we typically write application of an operator on $x \in \mathcal{H}$ as $Tx = T(x)$, and the composition of two operators such that $T(D(T)) \subseteq D(S)$ as $ST = S \circ T$. Finally, $I_{\mathcal{H}}$ denotes the identity map on $\mathcal{H}$ (and we often drop the subscript when it is obvious).

We define the *operator norm* of $T : \mathcal{H} \rightarrow \mathcal{I}$ as

$$\|T\| := \sup\{\|Tx\|_{\mathcal{I}} \mid x \in \mathcal{H} \text{ and } \|x\|_{\mathcal{H}} = 1\}, \quad (1.7)$$

and say that T is *bounded* if $\|T\| < \infty$. Then,

Proposition 1.7. *Let $T : \mathcal{H} \rightarrow \mathcal{I}$ be a bounded linear operator between Hilbert spaces. Then there is a unique bounded linear operator $T^* : \mathcal{I} \rightarrow \mathcal{H}$ such that for any $x \in \mathcal{H}$ and $y \in \mathcal{I}$, $\langle y, Tx \rangle_{\mathcal{I}} = \langle T^*y, x \rangle_{\mathcal{H}}$. T^* is called the adjoint of T .*

We write $\mathfrak{B}(\mathcal{H})$ the set of bounded operators on a Hilbert space $\mathcal{H}$,¹ and it is straightforwardly characterised as follows:

Proposition 1.8. *Let $T : \mathcal{H} \rightarrow \mathcal{I}$ be a linear operator, then T is continuous if and only if it is bounded.*

This is a problem, since many important quantities—see example 1.9—correspond to unbounded linear operators, which therefore cannot be continuously defined on the whole Hilbert space.

Example 1.9. Let $\mathcal{P} \subseteq \mathcal{L}^2(\mathbb{R})$ be the space of functions of the form $p(x)e^{-x^2}$ where p is a polynomial, and consider the following operators on $\mathcal{P}$:

$$Qf(x) := xf(x) \quad \text{and} \quad Pf(x) := i\frac{df}{dx}(x). \quad (1.8)$$

Then $\mathcal{P}$ is a dense subset of $\mathcal{L}^2(\mathbb{R})$, and Q and P are unbounded linear operators on $\mathcal{P}$ which correspond the position and momentum of a free particle in state f (at least in a first approach). As a consequence of the previous discussion, they cannot be continuously extended to $\mathcal{L}^2(\mathbb{R})$.

¹The set of bounded operators on a Hilbert space is the canonical example of von Neumann algebra, although we omit such a construction since we have no need for it.

This brings us to another important consideration: unlike for bounded operators defined on the whole of $\mathcal{H}$, the domain of unbounded operators is actually a matter of some importance. First of all, there are states $f \in \mathcal{L}^2(\mathbb{R})$ on which the action of neither Q nor P is well-defined. Worse, Q can be extended to act on some functions $f \in \mathcal{L}^2(\mathbb{R})$ which are not differentiable, so that Pf is not defined. This is a bit of a problem if we want to model the state space for a physical particle, and therefore we would like to find a common dense domain for both Q and P .

The issue of finding “nice” domains also comes up when we try to find adjoints for unbounded operators. In general, the adjoint T^* of an unbounded operator T will itself be unbounded, and therefore we need to specify a dense domain for T^* . Typically, this domain differs from $D(T)$.

Definition 1.10. *Let A be an unbounded operator on $\mathcal{H}$, then the adjoint A^* of A is defined by:*

- *the domain of A^* is the subset $D(A^*)$ of $\mathcal{H}$ consisting in vectors ψ such that the linear map $\mathcal{H} \rightarrow \mathbb{C} : \phi \mapsto \langle \psi, A\phi \rangle$ is bounded;*
- *for $\psi \in D(A^*)$, $A^*\psi$ is defined to be the unique vector $\phi \in \mathcal{H}$ such that $\langle \phi, \xi \rangle = \langle \psi, A\xi \rangle$ for all $\xi \in D(A)$.*

Unicity of $A^*\psi$ is assured by the Riesz representation theorem.

1.1.2 Some important classes of operators

Isometries and unitaries A bounded operator $T : \mathcal{H} \rightarrow \mathcal{I}$ is an *isometry* if for any $\psi \in \mathcal{H}$, $\|T\psi\|_{\mathcal{I}} = \|\psi\|_{\mathcal{H}}$. This is equivalent to requiring that $TT^* = I_{\mathcal{I}}$. T is a *unitary* if it is an isometry and furthermore, $T^*T = I_{\mathcal{H}}$.

Positive operators We say that an operator T on $\mathcal{H}$ is *positive* if $\langle \psi, T\psi \rangle \geq 0$ for all $\psi \in \mathcal{H}$.

Self-adjoint operators An unbounded operator A on $\mathcal{H}$ is *symmetric* if for any $\psi, \phi \in D(A)$, $\langle \psi, A\phi \rangle = \langle A\psi, \phi \rangle$. It is *self-adjoint* if $D(A^*) = D(A)$ and $A^*\psi = A\psi$ for all $\psi \in D(A)$.

In other words, A is self-adjoint if A^* and A are the *same operator* with *identical domains*. All self-adjoint operators are of course symmetric, but not all symmetric operators are self-adjoint. The following standard example demonstrates the difference.

Example 1.11. Let $D(A) \subseteq \mathcal{L}^2([0, 1])$ be the subspace of continuously differentiable functions ψ such that $\psi(0) = \psi(1) = 0$, and put $A\psi := i \frac{d\psi}{dx}$. Then a simple calculation using integration by parts shows that A is symmetric. However, for

any continuously differentiable ϕ (without boundary condition), $\phi \in D(A^*)$ so the domain of A^* is strictly bigger than the domain of A .

While the definition of self-adjointness is more complicated, it turns out to be the right one to make. For example, the all-important spectral theorem applies to self-adjoint operators but not to all symmetric operators.

Normal operators An operator $T : \mathcal{H} \rightarrow \mathcal{H}$ is *normal* if $T^*T = TT^*$. The importance to us of this definition is that both self-adjoint and unitary operators $\mathcal{H} \rightarrow \mathcal{H}$ are clearly normal, which allows us to state some results about both types of operators in one go (see for example theorem 1.16).

Projections A bounded operator P on $\mathcal{H}$ is a *projection* if $PP = P$. The set of all projections on $\mathcal{H}$ is denoted $\mathcal{P}(\mathcal{H})$.

If $\psi \in \mathcal{H}$ there is an associated projection P_ψ given by $P_\psi\phi := \langle \psi, \phi \rangle \psi$ for any $\phi \in \mathcal{H}$.

Definition 1.12. Let (X, Ω) be a measurable space. Then a map $P : \Omega \rightarrow \mathcal{P}(\mathcal{H})$ is a projection-valued measure or PVM if

- $P(\emptyset) = 0$ and $P(X) = I$;
- for any sequence $(E_n)_{n \in \mathbb{N}} \subseteq \Omega$ of pairwise disjoint subsets of X ,

$$P\left(\bigcup_{n \in \mathbb{N}} E_n\right) = \sum_{n \in \mathbb{N}} P(E_n), \quad (1.9)$$

where the series converges in the strong operator norm;

- for all $A, B \in \Omega$, $P(A \cap B) = P(A)P(B)$.

In particular, if P is such a PVM, then for any $\psi \in \mathcal{H}$, the map $\Omega \rightarrow \mathbb{R} : E \mapsto \sqrt{\langle \psi, P(E)\psi \rangle}$ defines a measure, which furthermore is a probability measure if $\|\psi\| = 1$.

1.1.3 The spectral theorem and functional calculi

If P is a PVM defined on some measurable space (X, Ω) and acting in $\mathcal{H}$, then for each $\psi \in \mathcal{H}_1$, we define a probability measure by

$$\begin{aligned} \mu_\psi : \Omega &\longrightarrow \mathbb{R}^+ \\ E &\longmapsto \langle \psi, P(E)\psi \rangle. \end{aligned} \quad (1.10)$$

Theorem 1.13 (Functional calculus). *Let P be a PVM on a measurable space (X, Ω) , and $f : X \rightarrow \mathbb{C}$ a measurable function. Define a subspace of $\mathcal{H}$ by*

$$D(f) = \left\{ \psi \mid \int_X |f(x)|^2 d\mu_\psi < \infty \right\}. \quad (1.11)$$

Then $D(f)$ is dense in $\mathcal{H}$, and there exists a unique unbounded operator $\int_X f dP$ with domain $D(f)$ such that

$$\left\langle \psi, \int_X f dP \psi \right\rangle = \int_X f(x) d\mu_\psi, \quad (1.12)$$

for any $\psi \in D(f)$.

Suppose T is an operator on $\mathcal{H}$, then the resolvent set of T is the set of all $\lambda \in \mathbb{C}$ for which there exists some bounded operator B such that for all $\psi \in \mathcal{H}$, $B\psi \in D(T)$ and $(T - \lambda I)B\psi = \psi$. The complement of the resolvent set of T in $\mathbb{C}$ is called the spectrum and denoted $\text{sp}(T)$.

Proposition 1.14. *If A is a self-adjoint operator, then $\text{sp}(A) \subseteq \mathbb{R}$.*

Proposition 1.15. *If U is a unitary operator, then $\text{sp}(U) \subseteq \mathbb{T}$.*

Theorem 1.16 (Spectral theorem). *Let T be a normal operator on $\mathcal{H}$. Then there is a unique PVM P_T on $\text{sp}(T)$, called the spectral measure of T , such that*

$$T = \int_{\text{sp}(T)} id dP_T. \quad (1.13)$$

We are only going to be interested in the two following cases:

1. T is self-adjoint, in which case $\text{sp}(T) \subseteq \mathbb{R}$; in this case we typically extend (1.13) to $\mathbb{R}$ as $\int_{\mathbb{R}} \chi_{\text{sp}(T)} dP_T$.
2. T is unitary, in which case $\text{sp}(T) \subseteq \mathbb{T}$, the unit circle.

If P_A is the spectral measure of some normal operator A , and $f : \text{sp}(A) \rightarrow \mathbb{C}$ is a measurable function, then we write

$$f(A) := \int_{\text{sp}(A)} f dP_A. \quad (1.14)$$

1.1.4 Tensor products

Tensor products are a particularly important way of constructing, from two Hilbert spaces, a third Hilbert space. They will be used to model the joint state space of two quantum systems.

If $\mathcal{H}$ and $\mathcal{I}$ are two Hilbert spaces, we can construct an inner product space $\mathcal{H} \bar{\otimes} \mathcal{I}$ as follows. Elements of $\mathcal{H} \bar{\otimes} \mathcal{I}$ are expressions of the form $\sum_{j=1}^n \psi_j \otimes \phi_j$ where $\psi_j \in \mathcal{H}$, $\phi_j \in \mathcal{I}$ and $n \in \mathbb{N}$. The expression $\psi \otimes \phi$ is assumed to be linear with respect to both arguments, so that

$$c(\psi \otimes \phi) = (c\psi) \otimes \phi = \psi \otimes (c\phi), \quad (1.15)$$

$$(\psi_1 + \psi_2) \otimes \phi = \psi_1 \otimes \phi + \psi_2 \otimes \phi, \quad (1.16)$$

$$\psi \otimes (\phi_1 + \phi_2) = \psi \otimes \phi_1 + \psi \otimes \phi_2. \quad (1.17)$$

The inner product on $\mathcal{H} \bar{\otimes} \mathcal{I}$ is defined by linearity from

$$\langle \psi_1 \otimes \phi_1, \psi_2 \otimes \phi_2 \rangle = \langle \psi_1, \psi_2 \rangle \langle \phi_1, \phi_2 \rangle. \quad (1.18)$$

There is only one problem: the linear space $\mathcal{H} \bar{\otimes} \mathcal{I}$ is not complete with respect to the norm induced by this inner product. The solution is simple: we take the tensor product $\mathcal{H} \otimes \mathcal{I}$ to be the completion of $\mathcal{H} \bar{\otimes} \mathcal{I}$ with respect to that norm. It should be clear that the tensor product of Hilbert spaces is associative up to isomorphism of Hilbert spaces, so the construct generalises to any finite number of factors. If $(\mathcal{H}_j)_{j \in J}$ is a finite collection of Hilbert spaces, we write $\bigotimes_{j \in J} \mathcal{H}_j$ their tensor product, and

$$\mathcal{H}^{\otimes J} = \bigotimes_{j \in J} \mathcal{H}, \quad \mathcal{H}^{\otimes n} = \bigotimes_{j \in \{1, 2, \dots, n\}} \mathcal{H}, \quad (1.19)$$

for brevity, where $n \in \mathbb{N}$.

Then, we have the following useful isomorphisms: whenever J is a finite set of cardinality $n \in \mathbb{N}$,

$$\mathcal{L}^2(G^J) \cong \bigotimes_{j \in J} \mathcal{L}^2(G), \quad \mathcal{H}^{\otimes J} \cong \mathcal{H}^{\otimes n} \quad \text{and} \quad \mathcal{H} \otimes \mathbb{C}^n \cong \mathcal{H}^{\otimes n}. \quad (1.20)$$

Finally, if A and B are bounded operators on $\mathcal{H}$ and $\mathcal{I}$ respectively, there is a unique bounded operator $A \otimes B$ on $\mathcal{H} \otimes \mathcal{I}$ such that

$$(A \otimes B)(\psi \otimes \phi) = (A\psi) \otimes (B\phi). \quad (1.21)$$

for all $\psi \in \mathcal{H}$ and $\phi \in \mathcal{I}$.

Similarly, if A and B are (not necessarily bounded) self-adjoint operators on $\mathcal{H}$ and $\mathcal{I}$ respectively, there is a unique self-adjoint operator $A \otimes B$ on $\mathcal{H} \otimes \mathcal{I}$ such that

$$(A \otimes B)(\psi \otimes \phi) = (A\psi) \otimes (B\phi). \quad (1.22)$$

for all $\psi \in D(A)$ and $\phi \in D(B)$.

When considering operators on $\mathcal{H}^{\otimes n}$, and if T is an operator on $\mathcal{H}$, then we will often write

$$T_j = \underbrace{I \otimes I \otimes \cdots \otimes \underbrace{T}_{\substack{j\text{-th position} \\ n \text{ times}}} \otimes \cdots \otimes I}_{n \text{ times}}. \quad (1.23)$$

T_j is an operator on $\mathcal{H}^{\otimes n}$ which we say “acts on the j -th subsystem”. This construction generalises via the isomorphism in equation 1.20 to the case of the operator T_j acting on $\mathcal{H}^{\otimes J}$, where $j \in J$.

1.2 Pure state quantum mechanics

We are now ready to state the axioms of quantum theory in terms of Hilbert spaces. As described informally, the state of a quantum system is a vector in a Hilbert space, and the Hilbert space of a composite system is described by a tensor product. Formally, we have:

Axiom P.1 (Pure states). *A state of a quantum system with Hilbert space $\mathcal{H}$ is a vector $\psi \in \mathcal{H}$ such that $\|\psi\| = 1$.*

Axiom P.2 (Composite systems). *A state of a composite of two quantum systems with respective Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ is a state in $\mathcal{H}_1 \otimes \mathcal{H}_2$.*

Axiom P.3 (Expectation values). *The expectation value of an operator $A \in \mathfrak{B}(\mathcal{H})$ for a given state $\psi \in \mathcal{H}$ is given by $\langle A \rangle = \langle \psi, A\psi \rangle$.*

In practice, the only values of the quantum system which are accessible are those which can be measured:

Axiom P.4 (Measurements). *An observable on a Hilbert space $\mathcal{H}$ is a projection-valued measure $P : \Omega \rightarrow \mathcal{P}(\mathcal{H})$ on some measurable space Ω .*

If $E \in \Omega$ and the system is the state $\psi \in \mathcal{H}$ the probability of obtaining outcome $x \in E$ from the measurement is $\mu_\psi(E)$. The state of the system immediately after the measurement is then

$$\psi_E := \frac{P(E)\psi}{\|P(E)\psi\|} = \frac{P(E)\psi}{\mu_\psi(E)}. \quad (1.24)$$

Given the spectral theorem, any self-adjoint operator is associated to a canonical PVM and therefore to a measurement. Thus, physicist often call self-adjoint operators *observables* since they correspond to the observable properties of the system.

An immediate implication of these axioms is that transformations of a quantum system must preserve “statefulness”, in other words they must map unit-norm

vectors to unit norm vectors. We further impose that these transformations must be linear, which results in the following description of transformations:

Axiom P.5 (Transformations). *A transformation of a quantum system with Hilbert space $\mathcal{H}$ is described by an isometry $\mathcal{H} \rightarrow \mathcal{I}$ for some Hilbert space $\mathcal{I}$.*

This axiom includes the possibility of embedding a quantum system into a larger one. If we exclude this, then transformations on a quantum system are given by unitaries $\mathcal{H} \rightarrow \mathcal{H}$.

1.3 Mixed state quantum mechanics

Now, we want to describe quantum states that are probabilistic mixtures of pure quantum states. Think of the state obtained by flipping a coin and outputting the state ψ if heads and ϕ if tails. This is a key concern given that if we perform a measurement and discard the outcome, then the result in general is precisely such a mixture of states each of which takes the form of equation (1.24). To do so, we need to model states as a specific kind of operator on $\mathcal{H}$ rather than simply as elements of $\mathcal{H}$.

If A is a bounded, self-adjoint and positive operator on $\mathcal{H}$, then we define the *trace* of A to be

$$\mathrm{tr}[A] = \sum_{j \in J} \langle e_j, A e_j \rangle, \quad (1.25)$$

for an arbitrarily chosen² basis $(e_j)_{j \in J}$ of $\mathcal{H}$. If $\mathrm{tr}[A] < +\infty$, we say that A is *trace-class*. A (not necessarily self-adjoint) bounded operator T is trace-class if the self-adjoint operator $\sqrt{T^*T}$ (defined using the functional calculus, theorem 1.13) is trace-class. We write $\mathfrak{T}(\mathcal{H})$ the set of trace-class operators on $\mathcal{H}$.

Definition 1.17. *A density operator on a Hilbert space $\mathcal{H}$ is a trace-class, self-adjoint and positive operator ρ on $\mathcal{H}$ such that $\mathrm{tr}[\rho] = 1$. We denote $\mathfrak{D}(\mathcal{H})$ the set of density operators on $\mathcal{H}$.*

Example 1.18. In the Hilbert space $\mathbb{C}$, it is straightforward to see that 1 is the unique density operator.

Firstly, we can recover the set of pure states $\mathcal{H}$ as density operators:

Proposition 1.19. *If $\psi \in \mathcal{H}$ is a pure state, then $P_\psi \in \mathfrak{D}(\mathcal{H})$, where as before P_ψ is the projector along the normalised state ψ .*

²Importantly, the value of $\mathrm{tr}(A)$ is independent of the choice of basis.

So, all pure states embed into this formulation by the map $\mathcal{H} \rightarrow \mathfrak{D}(\mathcal{H}) : \psi \mapsto P_\psi$. This axiom and the name “mixed state” is made clear by the following result:

Proposition 1.20. *Let $\rho \in \mathfrak{D}(\mathcal{H})$ be a density operator, then there is a (non-unique) sequence of positive real numbers $(c_j)_{j \in J} \in [0, 1]$ and a sequence of states $(\psi_j)_{j \in J} \in \mathcal{H}$ such that $\rho = \sum_{j \in J} c_j P_{\psi_j}$ and $\sum_{j \in J} c_j = 1$.*

We can interpret this sum as a classical probabilistic mix of the pure states ψ_j , which is for example the output of a process that produces state ψ_j with probability c_j . It follows that density operators provide a good representation for a quantum system in a mixed state:

Axiom M.1 (Mixed states). *A (mixed) state on a quantum system with Hilbert space $\mathcal{H}$ is described by a density operator $\rho \in \mathfrak{D}(\mathcal{H})$.*

Like for pure states, a state of a composite quantum system is given by a state on the tensor product of Hilbert spaces:

Axiom M.2 (Composite systems). *A state on a composite of two quantum systems with respective Hilbert spaces $\mathcal{H}$ and $\mathcal{I}$ is a state on $\mathcal{H} \otimes \mathcal{I}$, i.e. an operator in $\mathfrak{D}(\mathcal{H} \otimes \mathcal{I})$.*

In fact, the trace can be used to define a metric on $\mathfrak{D}(\mathcal{H})$, called the *trace distance* and given by $d(A, B) = \text{tr}[A - B]$. Although we will not need it for a long time (in fact, until chapter 6) we state the following important property:

Proposition 1.21. *$\mathfrak{D}(\mathcal{H})$ is a complete separable metric space with the metric defined by the trace distance.*

The corresponding norm is called the *trace norm*, and it more or less corresponds to the Hilbert space norm for density operators:

Proposition 1.22. *If $\psi \in \mathcal{H}$, then $\text{tr}[P_\psi] = \|\psi\|_{\mathcal{H}}$.*

Proposition 1.23. *$\mathfrak{T}(\mathcal{H})$ is an ideal in $\mathfrak{B}(\mathcal{H})$: whenever $T \in \mathfrak{T}(\mathcal{H})$ and $A \in \mathfrak{B}(\mathcal{H})$, $AT \in \mathfrak{T}(\mathcal{H})$ and $TA \in \mathfrak{T}(\mathcal{H})$.*

Proposition 1.24. *The trace is cyclical: if $A_j \in \mathfrak{T}(\mathcal{H})$ for each $j \in J$ with J finite, and σ is a cyclic permutation of J , then*

$$\text{tr} \left[\prod_{j \in J} A_{\sigma(j)} \right] = \text{tr} \left[\prod_{j \in J} A_j \right]. \quad (1.26)$$

Given these two properties, it is clear that the generalisation of axiom P.3 to mixed states should be given by:

Axiom M.3 (Expectation values). *If $A \in \mathfrak{B}(\mathcal{H})$, the expectation value of A for a state ρ is given by $\langle A \rangle = \text{tr}[A\rho] = \text{tr}[\rho A]$.*

Measurement are described once again by PVMs:

Axiom M.4. *An observable on a Hilbert space $\mathcal{H}$ is a projection-valued measure $P : \Omega \rightarrow \mathcal{P}(\mathcal{H})$ on some measurable space (X, Ω) .*

If the system is in the state $\rho \in \mathfrak{D}(\mathcal{H})$ outcome probabilities are described by the probability measure on (X, Ω) ,

$$\mu_\rho^P(E) = \text{tr}(P(E)\rho). \quad (1.27)$$

If a measurement is made with outcome $E \in \Omega$, the state of the system immediately after the measurement is

$$\rho_E := \frac{P(E)\rho P(E)}{\text{tr}(P(E)\rho)}. \quad (1.28)$$

1.3.1 Quantum channels

We say a linear map $\Phi : \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{I})$ is *positive* if whenever $A \in \mathfrak{B}(\mathcal{H})$ is positive, $\Phi[A]$ is also positive.

Definition 1.25. *A quantum channel between Hilbert spaces $\mathcal{H}$ and $\mathcal{I}$ is a linear map $\Phi : \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{I})$ that furthermore is:*

- trace-preserving: *for any $A \in \mathfrak{T}(\mathcal{H})$, $\text{tr}[\Phi[A]] = \text{tr}[A]$; and,*
- completely positive: *for every $n \in \mathbb{N}$, the linear map $\Phi \otimes I_n : \mathfrak{T}(\mathcal{H} \otimes \mathbb{C}^n) \rightarrow \mathfrak{T}(\mathcal{I} \otimes \mathbb{C}^n)$ is positive.*

The set of all quantum channels $\mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{I})$ will be written $\mathfrak{C}(\mathcal{H}, \mathcal{I})$, and the application of a quantum channel Φ on a state ρ as $\Phi[\rho]$.

Then, quantum channels model transformations on mixed quantum states:

Axiom M.5. *A transformation from a quantum system with Hilbert space $\mathcal{H}$ to one with Hilbert space $\mathcal{I}$ is described by a quantum channel map $\Phi : \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{I})$.*

For any unitary $U \in U(\mathcal{H})$, there is an associated quantum channel given by conjugation: $\Gamma_U(T) := UTU^*$. If P_ψ is the projection along $\psi \in \mathcal{H}$, it is clear that $\Gamma_U(P_\psi) = P_{U\psi}$, and once again the pure theory is recovered via the projections.

The conditions in definition 1.25 can be straightforwardly motivated. The first is clearly necessary for a quantum channel to map density operators to density operators, i.e. for the quantum channel to preserve statefulness. The second is also about preserving statefulness, but in a more subtle way. It is necessary to guarantee positivity of the channel obtained by performing Φ on part of a larger system and ignoring the rest.

Example 1.26. We have already seen an example of a very simple quantum channel: the trace on $\mathcal{H}$ is the unique quantum channel $\mathcal{H} \rightarrow \mathbb{C}$. This justifies the square-bracket notation we have used thus far for the trace.

A particularly important quantum channel is obtained by tracing out a single subsystem in a tensor product:

Theorem 1.27. *Suppose that $\rho \in \mathfrak{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Then there is a unique density operator $\text{tr}_2[\rho] \in \mathfrak{D}(\mathcal{H}_1)$ with the property that for any $A \in \mathfrak{B}(\mathcal{H})$,*

$$\text{tr}[\text{tr}_2[\rho]A] = \text{tr}[\rho(A \otimes I)]. \quad (1.29)$$

We call $\text{tr}_2[\rho]$ the partial trace of ρ with respect to $\mathcal{H}_2$, and the function $\mathfrak{D}(\mathcal{H}_1 \otimes \mathcal{H}_2) \rightarrow \mathfrak{D}(\mathcal{H}_1) : \rho \mapsto \text{tr}_2[\rho]$ is a quantum channel.

This extends straightforwardly to density operators in a finite tensor product of Hilbert spaces $\bigotimes_{j \in J} \mathcal{H}_j$, and we obtain for each $k \in J$, a quantum channel

$$\text{tr}_k : \mathfrak{D}\left(\bigotimes_{j \in J} \mathcal{H}_j\right) \rightarrow \mathfrak{D}\left(\bigotimes_{j \in J \setminus \{k\}} \mathcal{H}_j\right), \quad (1.30)$$

called the *partial trace over $\mathcal{H}_k$* .

The following description of quantum channels, due to Karl Kraus, is particularly useful, especially (but not only) in finite-dimensions:

Theorem 1.28 (Kraus decompositions). *$\Phi : \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{J})$ is a quantum channel if and only if there is an at most countable index set J and a collection of linear operators $(K_j : \mathcal{H} \rightarrow \mathcal{J})_{j \in J}$ such that for any $\rho \in \mathfrak{T}(\mathcal{H})$,*

$$\Phi[\rho] = \sum_{j \in J} K_j \rho K_j^* \quad \text{and} \quad \sum_{j \in J} K_j K_j^* = I_{\mathcal{J}}. \quad (1.31)$$

This allows us to describe a typical way in which quantum channels arise in the finite-dimensional case. A measurement process, described by a PVM P , in which the information on the actual outcome of the measurement is not conserved is a quantum channel described by a collection of Kraus operators (K_m) . Each operator K_m is the map obtained applying the projection $P(\{m\})$ corresponding to the outcome m . Intuitively, this corresponds to the classical probabilistic mix of the pure states that one would have obtained from axiom P.4 given outcome m .

The Kraus formulation of quantum channels has a couple of drawbacks. Firstly, the collection of operators $(A_j : \mathcal{H} \rightarrow \mathcal{J})_{j \in J}$ is non-unique. Secondly, in the infinite-dimensional case we often want to consider measurements with uncountable outcome sets (such as the real numbers). Then, these measurement can be associated to quantum channels, and they have Kraus decompositions by theorem 1.28, but

no Kraus decomposition where the operators correspond to measurement outcomes as above. The theorem can be reformulated in the following essentially equivalent way, due to William Stinespring [Sti55], which will also prove very useful:

Theorem 1.29 (Stinespring dilation). *$\Phi : \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{I})$ is a quantum channel if and only if there is a Hilbert space $\mathcal{J}$ and an isometry $T : \mathcal{H} \rightarrow \mathcal{I} \otimes \mathcal{J}$ such that for any $\rho \in \mathfrak{T}(\mathcal{H})$*

$$\Phi[\rho] = \text{tr}_{\mathcal{J}}[T\rho T^*]. \quad (1.32)$$

FORMAL MODELS OF QUANTUM COMPUTATION WITH QUDITS

This is an introductory chapter for the computational models that we will reason about in the following few chapters. It introduces two models for qudit quantum computation:

- *quantum circuits*, which are used to represent reversible quantum computations;
- the *measurement calculus*, which makes explicit use of quantum measurements to transform an input state while consuming subsystems of the total, composite quantum system. It is therefore deemed an “irreversible” model.

In section 2.1 we will first define some unitary operations that are omnipresent when talking about qudit MBQC, before moving on to quantum circuits. We also introduce a circuit notation for measurements which extends the quantum circuit model and allows one to (somewhat clumsily) represent measurement calculus computations in terms of quantum circuits. Then section 2.2 will introduce the measurement calculus, a formal model for reasoning about measurement-based quantum computation. It is one of the main objects of study in this thesis, and defining it for qudits requires a careful consideration of the types of measurement which should be allowed. The correct formulation of measurements will be captured in the notion of *measurement spaces*, which are studied in subsection 2.2.1.

Some of the results in this chapter, in particular in sections 2.2 and 2.3 are based on our article, [Boo+21].

It is worthwhile to take a second at this point to discuss the interplay between these two models, since a major part of this thesis will be dedicated to translating from one to the other. It is easy, using the circuit notation for measurements, to map any computation described in the measurement calculus into the quantum circuit picture. However, this comes at a major cost: the resulting circuit is not unitary and corresponds (in general) to a CPTP map as described in chapter 1. We would much rather have a method for obtaining a reversible quantum circuit (without measurements). This is not always possible, but chapters 4 and 5 provide complete algorithms for doing so whenever it *is* possible.

2.1 The quantum circuit model

Throughout this thesis, d denotes an odd prime number, and $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$ the ring of integers with arithmetic modulo d . We also put $\omega := e^{i\frac{2\pi}{d}}$, and let $\mathbb{Z}_d^*$ be the group of units of $\mathbb{Z}_d$. Since d is prime, $\mathbb{Z}_d$ is a field and $\mathbb{Z}_d^* = \mathbb{Z}_d \setminus \{0\}$ as a set. Many of our results apply with small modifications for the case $d = 2$, but since this case has been extensively studied already, we omit it for the sake of simplicity.

The Hilbert space of a single qudit [Got99; Wan+20] is $\mathcal{H} := \mathcal{L}^2(\mathbb{Z}_d)$, and we write $U(\mathcal{H})$ the group of unitary operators acting on $\mathcal{H}$. Throughout the qudit part of this thesis, we shall use the Dirac notation. A state $\psi \in \mathcal{H}$ will be written $|\psi\rangle$ and decomposed along a fixed choice of basis: $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \psi(n) |n\rangle$.

Given such a choice of basis, we have the following standard operators on $\mathcal{H}$, also known as the *clock* and *shift* operators:

$$Z|m\rangle := \omega^m |m\rangle \quad \text{and} \quad X|m\rangle := |m+1\rangle \quad \text{for any } m \in \mathbb{Z}_d. \quad (2.1)$$

In particular, note that $ZX = \omega XZ$. Any operator of the form $\omega^k X^a Z^b$ for $k, a, b \in \mathbb{Z}_d$ is called a *Pauli operator*, although we will often drop the phase ω^k as it is of little importance in most cases. We say a Pauli operator is *trivial* if it is proportional to the identity. The Paulis are further related by the *Fourier* operator,

$$F|m\rangle = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \omega^{mn} |n\rangle \quad \text{s.t.} \quad FXF^* = Z \quad \text{and} \quad FZF^* = X^{-1}, \quad (2.2)$$

and the *phase* operator,

$$P|k\rangle = \omega^{\frac{k(k+1)}{2}} |k\rangle \quad \text{s.t.} \quad PXP^* = XZ \quad \text{and} \quad PZP^* = Z. \quad (2.3)$$

Equations (2.1)–(2.3) imply that both X and Z , and in fact every Pauli has spectrum $\{\omega^k \mid k \in \mathbb{Z}_d\}$, and in turn a simple counting argument shows that each

eigenvalue has multiplicity 1. We label the eigenvectors of a Pauli Q by their (unique) eigenvalues: for any $k \in \mathbb{Z}_d$, $|k : Q\rangle$ is the eigenvector of Q associated with eigenvalue ω^k .

Together, the Fourier and phase operators generate a subgroup of $U(\mathcal{H})$ called the *Clifford group* [Got99; Cla06]. An element of this subgroup which is of particular interest to us is the *multiplier*: for any $k \in \mathbb{Z}_d^*$,

$$M(k) |n\rangle := |kn\rangle \quad \text{s.t.} \quad M(k)XM(k)^* = X^k \quad \text{and} \quad M(k)ZM(k)^* = Z^{k^{-1}}. \quad (2.4)$$

Finally, we will also use the Z -rotation operator, $R_Z(\alpha) |x\rangle := e^{i\alpha x} |x\rangle$ for $\alpha \in \mathbb{T}^{d-1}$.

All of the operators presented so far act on a single qudit. To make multiple qudits interact, we use the *controlled- Z* operator (also, controlled phase), which acts on $\mathcal{H} \otimes \mathcal{H}$,

$$E |m\rangle |n\rangle := \omega^{mn} |m\rangle |n\rangle. \quad (2.5)$$

It is important to emphasise a key difference between the qudit and the qubit case: when $d \neq 2$, none of these operators are self-inverse. In fact, if Q is a Pauli and I the identity operator on $\mathcal{H}$, we have:

$$Q^d = I, \quad E^d = I \otimes I \quad \text{and} \quad F^4 = I. \quad (2.6)$$

As a result, they are not self-adjoint either, something which needs to be taken into account when describing measurements.

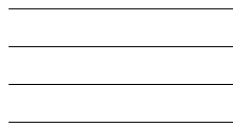
2.1.1 Reversible quantum circuits

Quantum circuits are a simple graphical representation for unitary operations acting on a fixed number of quantum systems, and built from a set of elementary unitary operations called *quantum gates*. In our case, we consider a register V of qudits corresponding to the Hilbert space $\mathcal{H}^{\otimes V}$. The set of quantum gates will then be

$$\{U_j, E_{j,k}^\lambda \mid U \in U(\mathcal{H}), \lambda \in \mathbb{Z}_d, j, k \in V\}, \quad (2.7)$$

where the indices indicate on which qudit the gates act, as described in section (1.1.4). This gate set is universal in the usual sense [NC10; SK17a; SK17b]: the group it generates is equal to $U(\mathcal{H}^{\otimes V})$.

A quantum circuit is comprised of a set of n wires, each of which is identified with a quantum system with Hilbert space $\mathcal{H}$ undergoing some unitary evolution, and which together represent a unitary $\mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$. The simplest quantum circuit consists in only the wires, and represents the identity $I^{\otimes n}$. For $n = 4$ this gives:



Operations from the gate set acting on the subsystems are represented as boxes superimposed on the corresponding wires:

$$- \boxed{X^a Z^b} - \quad - \boxed{R_Z(\alpha)} - \quad - \boxed{F} - .$$

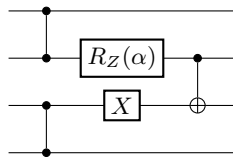
For the two-qubit operation E , we use a special notation:

$$\text{Diagram of } E^k \text{ gate} = \text{Diagram of } k \text{ gate},$$

which we in turn use to define the *controlled-X* or *CX* gate:

$$\text{Diagram 1} = \text{Diagram 2}.$$

A generic quantum circuit is read from left to right and evaluated by successively applying the quantum gates on the qudits corresponding to the wires in the circuit. Left-to-right juxtaposition of gates in the same quantum circuit corresponds to composition as functions. Here is another simple example of a quantum circuit when $n = 4$:



and this circuit is interpreted as the unitary

$$(I \otimes CX_{2,3} \otimes I) \circ (I \otimes R_Z(\alpha) \otimes X \otimes I) \circ (E_{1,2} \otimes E_{3,4}), \quad (2.8)$$

where the indices indicate on which subsystem each gate acts.

Any quantum circuit which is built in this way is reversible, since by reversing the order of all the gates and taking their adjoints, we obtain the adjoint of the whole circuit. This is the inverse of the unitary represented by the original quantum circuit. In particular, *every quantum circuit built in this way represents a unitary operation on $\mathcal{H}$.*

2.1.2 State preparation and measurements

The quantum circuit representation can be extended to include either state preparation or measurements of quantum systems. State preparations are easy once we introduce some notation for labelling input and output states to a quantum circuit:

$$|\phi\rangle \text{---} \boxed{X} \text{---} |\psi\rangle \quad .$$

$|\phi\rangle$ represents an input state to the circuit, and $|\psi\rangle$ is the output obtained by applying the unitary corresponding to the circuit on $|\phi\rangle$. In this case, the circuit describes an equation $|\psi\rangle = X |\phi\rangle$. State preparation is simply represented as a fixed input state. For example, the quantum circuit that entangles an input with the state $|0\rangle$ is

$$\begin{array}{c} \text{---} \\ |0\rangle \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad .$$

No gates are allowed to act on a wire before the state label, and the interpretation of state preparation is then just the map:

$$\begin{aligned} \mathcal{H}^{\otimes n} &\longrightarrow \mathcal{H}^{\otimes n+1} \\ |\psi\rangle &\longmapsto |\psi\rangle \otimes |\phi\rangle \end{aligned} \quad (2.9)$$

As a result, a quantum circuit built from the unitary fragment plus state preparations *represents an isometry* $\mathcal{H}^{\otimes m} \rightarrow \mathcal{H}^{\otimes n}$ with $m \leq n$ and $n - m$ being the number of prepared states.

Measurements are a little bit more subtle. Recall from chapter 1 that a measurement is given by a PVM $P : \Omega \rightarrow \mathbb{R}$. In the case of qudits, the σ -algebra Ω is finite, and we interpret the outcome $k \in \Omega$ as classical data output by the measurement. A measurement can then be represented by a box that has a quantum input and a classical output, which we draw as a doubled wire:

$$\text{---} \boxed{P} = \quad .$$

For example, the famous *gate teleportation protocol* is represented as

$$\begin{array}{c} \text{---} \\ |0 : Q\rangle \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{M} \\ \text{---} \end{array} \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \begin{array}{c} \boxed{X^m} \\ \text{---} \end{array} \quad ,$$

where we have further used the outcome m of the measurement to control the unitary gate X^m (which of course must appear after the measurement has taken place). Any qudit which is both initialised and measured within a quantum circuit is called an *auxiliary qudit*.

Now, following the discussion in chapter 1, the operation represented by a measurement is no longer unitary. If the outcomes of measurements are always discarded by the end of the computation, a quantum circuit where ℓ systems are inputs, m are prepared and n are measured corresponds to a CPTP map $\mathfrak{D}(\mathcal{H}^{\otimes \ell}) \rightarrow \mathfrak{D}(\mathcal{H}^{\otimes (\ell+m-n)})$.

If one wishes to keep track of the exact outcomes of measurements throughout the computation, it becomes necessary in principle to extend the axioms of section 1.3. One needs access to a “classical” register which records the outcomes of measurements, and which can be modelled as an extra interacting quantum system, or as an external structure. However, in this thesis we do not need this structure: we will always assume that measurement outcomes are discarded by the end of the computation.

2.2 The measurement calculus

The measurement calculus was first introduced in [DKP07] as a rigorous mathematical model for studying measurement-based quantum computation with qubits, and various extensions to the measurement calculus have been studied [Dan+09; Per06]. In this section we explicit another extension where the quantum systems under consideration are taken to be qudits.

Inherent in the measurement calculus is the idea of *outcome determinism*. Put informally, when is it possible to use measurement-outcome dependant operations to eliminate the probabilistic nature of quantum measurements in order to obtain a computation that does not depend on the result of any given measurement? In order to be able to attack this question at all, we need to impose restrictions on the kinds of measurements which we allow in the model. This leads naturally to our introduction of *measurement spaces*, which can be thought of as collections of “correctable” measurements labelled by the kind of correction which needs to be made.

2.2.1 Measurement spaces

For MBQC with qubits, it is well-established that by using a Pauli X , Y or Z as an acausal correction operator, it is possible to perform deterministic MBQCs on graph states where the measurements are taken from the plane on the Bloch sphere orthogonal to the chosen Pauli correction [Bro+07]. Since there are three Pauli operators for qubits, this yields three allowable measurement “planes” for MBQC.

This interpretation is not as clear in the qudit case, partly because Pauli operators are self-adjoint only in the case $d = 2$, but mostly because the geometry of the Bloch “space” is not as intuitive in the general case. Instead, we describe

a qudit-measurement by a unitary matrix M : given its spectral decomposition $M = \sum_i \lambda_i P_i$, the measurement of M is the measurement given by the PVM $\{P_i\}$. In the context of MBQC, we would like to have a distinguished measurement outcome, the one that does not need corrections, so we assume that all measurements have a fixpoint.

Definition 2.1. M is a fixpoint unitary if $M^*M = MM^* = I$ and there is a non-zero $|\phi\rangle \in \mathcal{H}$ s.t. $M|\phi\rangle = |\phi\rangle$. Given $(a, b) \in \mathbb{Z}_d^2 \setminus \{(0, 0)\}$, the measurement space $\mathcal{M}(a, b)$ is defined as $\mathcal{M}(a, b) := \{\text{fixpoint unitaries } M \text{ s.t. } X^a Z^b M = \omega M X^a Z^b\}$.

It should be pointed out that the commutation relation used to define the measurement space $\mathcal{M}(a, b)$ is somewhat arbitrary. We could have chosen instead to use the relation

$$X^a Z^b M = \omega^p M X^a Z^b \quad \text{for some } p \in \mathbb{Z}_d^*. \quad (2.10)$$

However, nothing is lost by considering only $p = 1$, since if M satisfies equation (2.10), then

$$X^{p^{-1}a} Z^{p^{-1}b} M = \omega^{p^{-1}p} M X^{p^{-1}a} Z^{p^{-1}b} = \omega M X^{p^{-1}a} Z^{p^{-1}b}, \quad (2.11)$$

(where this calculation is formally carried out using $p^{-1} = \frac{d+1}{p}$) which implies that $M \in \mathcal{M}(p^{-1}a, p^{-1}b)$.

In fact, this construction is very analogous to one used in qudit quantum error correction where the M are called detectable errors [Got99]. The main point of this definition is that the Pauli $X^a Z^b$ can be used to translate the eigenvectors of any measurement in the corresponding measurement space:

Proposition 2.2. If $M \in \mathcal{M}(a, b)$ for some non-zero $(a, b) \in \mathbb{Z}_d^2$, then the spectrum of M is $\{\omega^m \mid m \in \mathbb{Z}_d\}$, each eigenvalue has multiplicity 1, and M is special unitary. Denoting $|0 : M\rangle$ the fixpoint of M , then $|m : M\rangle := (X^a Z^b)^{-m} |0 : M\rangle$ is an eigenvector of M associated with eigenvalue ω^m .

Proof. By assumption, if $M \in \mathcal{M}(a, b)$ then M has a fixpoint $M|0 : M\rangle = |0 : M\rangle$. Letting $Q = X^a Z^b$, it follows from the commutation relation that

$$MQ|0 : M\rangle = \omega^{-1}QM|0 : M\rangle = \omega^{-1}Q|0 : M\rangle, \quad (2.12)$$

so $Q|0 : M\rangle$ is an eigenvector of M associated with eigenvalue ω^{-1} . Repeating this procedure, we find that $|k : M\rangle = Q^{-k}|0 : M\rangle$ is an eigenvector of M associated with eigenvalue ω^k , and a counting argument shows that each of these eigenvalues must have multiplicity 1. Now, we have that $\det(M) = \prod_{k \in \mathbb{Z}_d} \omega^k = 1$. $\square$

This means that the Pauli $X^a Z^b$ can be used as correction for any measurement in the corresponding measurement space, and we will use this extensively in chapter 3. Although there is not as nice a geometric picture for the collection of all measurements as the Bloch sphere, qudit measurement spaces do retain some of the structure of qubit measurement planes.

Proposition 2.3. $\omega^k X^x Z^z \in \mathcal{M}(a, b)$ if and only if $bx - az = 1$.

Proof. $\omega^k X^a Z^b X^x Z^z = \omega^k \omega^{bx} X^{a+x} Z^{b+z} = \omega^{bx-az} \omega^k X^x Z^z X^a Z^b$. $\square$

Proposition 2.4. For any two non-commuting Pauli operators P, Q , there exists a unique $(a, b) \in \mathbb{Z}_d^2$ s.t. $P, Q \in \mathcal{M}(a, b)$.

Proof. Given P and Q we can solve a linear system to find (a, b) s.t. $P, Q \in \mathcal{M}(a, b)$. This linear system has a unique solution. $\square$

Notice that when $d > 2$, two distinct pairs of non commuting Pauli operators can lead to the same measurement space, e.g. the pairs $(X, X^2 Z^{d-1})$ and $(Z, X^3 Z^{d-2})$ both belong to the same measurement space. For this reason, it is more convenient to identify a measurement space by the corresponding pair $(a, b) \in \mathbb{Z}_d^2$, i.e. a choice of Pauli corrector.

As in the qubit case, pairs of measurements within the same measurement space $\mathcal{M}(a, b)$ are still related to each other by rotations around the “correction” axis $X^a Z^b$:

Proposition 2.5. Let $X^a Z^b$ be a non-trivial Pauli operator and $N \in \mathcal{M}(a, b)$. Then $M \in \mathcal{M}(a, b)$ if and only if there is a special unitary $U \in SU(d)$ such that $M = UNU^*$ and $[U, Q] = 0$.

Proof. ($\implies$) If $M \in \mathcal{M}(a, b)$ then $\text{sp}(M) = \text{sp}(N) = \{\omega^k \mid k \in \mathbb{Z}_d\}$ and each eigenvalue has multiplicity one. It follows that M and N are similar so that there is a unitary U such that $M = UNU^*$.

Furthermore, by proposition 2.2 and writing $Q = X^a Z^b$, the eigenvector $|k : M\rangle$ of M can be obtained as $Q^{-k} |0 : M\rangle$, from which it also follows that $|k+1 : M\rangle = Q |k : M\rangle$. But, we also have $MU |k+1 : N\rangle = UNU^*U |k+1 : N\rangle = \omega^{k+1} U |k+1 : N\rangle$ from which it follows that

$$QU |k : N\rangle = Q |k : M\rangle = |k+1 : M\rangle = U |k+1 : N\rangle = UQ |k : N\rangle. \quad (2.13)$$

This is true for any $k \in \mathbb{Z}_d$, and since N is unitary its eigenvectors form a basis for $\mathcal{H}$. We deduce that $QU = UQ$.

Finally, it is clear we can choose U to be special unitary, since for any unit norm $\lambda \in \mathbb{C}$, $(\lambda U)N(\lambda U)^* = |\lambda|^2 UNU^* = UNU^*$.

($\Leftarrow$) Let $M = UNU^*$ such that $[U, Q] = 0$, then we have

$$MQ = UNU^*Q = UNQU^* = \omega UQNU^* = \omega QUNU^* = \omega QM. \quad (2.14)$$

Furthermore, M and N have the same spectrum, and in particular M has a fixpoint since N does. Then, $M \in \mathcal{M}(a, b)$. $\square$

In turn, this allows us to recover a parametrisation of measurement spaces much closer to the qubit case, where a measurement is given by angles relative to a reference Pauli axis of the Bloch sphere.

Corollary 2.6 (Measurement angles). *For any non-zero $(a, b) \in \mathbb{Z}_d^2$, a measurement $M \in \mathcal{M}(a, b)$ is characterised by $d - 1$ angles $\vec{\theta} = (\theta_1, \dots, \theta_{d-1}) \in [0, 2\pi)^{d-1}$, up to a choice of reference axis $P \in \mathcal{M}(a, b)$.*

Proof. Fix some $P \in \mathcal{M}(a, b)$, then by the proposition, every $M \in \mathcal{M}(a, b)$ is such that $M = UPU^*$, and in particular $[U, X^a Z^b] = 0$. This implies that in the eigenbasis of $X^a Z^b$, U takes the form of a diagonal matrix $\text{diag}(e^{i\theta_k} \mid k \in \mathbb{Z}_d)$ with $\theta_k \in [0, 2\pi)$. Since $\det(U) = 1$, we have that $\sum_{k=0}^{d-1} \theta_k = 0$ and one of these phases is redundant. Then, U and by extension, M , is uniquely determined by the $d - 1$ phases $\{\theta_k\}_{k=1}^{d-1}$ (and the arbitrary choice of P). $\square$

2.2.2 Measurement patterns

Given that we are interested in procedures with an emphasis on measurements and corrections conditioned on the outcomes of measurements, the quantum circuit description of computations is not very practical for our needs. Instead, we describe an MBQC by a sequence of commands, called a measurement pattern. Here, we formally describe the syntax of measurement patterns, assuming that a choice of reference axis has been made for each measurement space.

Definition 2.7 ([DKP07]). *A $\mathbb{Z}_d$ -measurement term on a register V of qudits consists in a finite ordered sequence of V -indexed commands chosen from:*

- N_u : initialisation of a qudit u in the state $|0 : X\rangle = F|0\rangle$;
- $E_{u,v}^\lambda$: application of E^λ on qudits u and v for some $\lambda \in \mathbb{Z}_d$, with $u \neq v$;
- $M_u^{a,b}(\vec{\theta})$: measurement of qudit u in the measurement space $\mathcal{M}(a, b)$ with angles $\vec{\theta}$;
- $X_u^{m_v}$ and $Z_u^{m_v}$: Pauli corrections acting on qudit u and depending on the outcome m_v of the measurement of qudit v .

A measurement term is runnable if no commands act on a qudit $v \in V$ before it is initialised (except initialisations) or after it is measured; and no commands

depend on the outcome of a measurement before it is made. A runnable measurement term is called a $\mathbb{Z}_d$ -measurement pattern.

We often drop explicit mentions of the field $\mathbb{Z}_d$ when it is obvious.

The outcome m_v of a given measurement can be described as a signal which communicates its value across a control structure for the MBQC. The syntax for corrections then binds that signal to a given correction.

Following Sanselme and Perdrix [SP17], measurement patterns can be equivalently represented as labelled graphs. Then, following [Zho+03], these measurement patterns are universal for all qudit quantum circuits.

Notation. A $\mathbb{Z}_d$ -graph G is a loop-free undirected $\mathbb{Z}_d$ -edge-weighted graph on a set V of vertices. We will identify the graph G with its symmetric adjacency matrix $G \in \mathbb{Z}_d^{V \times V}$ (for some arbitrary ordering of the rows and columns). If $A, B \subseteq V$, we will also denote $G[A, B]$ the submatrix of G obtained by keeping only the rows corresponding to elements of A and the columns corresponding to elements of B . If $A \subseteq V$, then we denote $1_A \in \mathbb{Z}_d^V$ the column vector whose u -th element is 1 if $u \in A$, 0 otherwise. Similarly we consider $\mathbb{Z}_d$ -multisets of vertices where each vertex occurs with a multiplicity in $\mathbb{Z}_d$ and we will identify the $\mathbb{Z}_d$ -multiset with column vectors in $\mathbb{Z}_d^V$. The size of a multiset is defined by $|A| = \sum_{u \in V} A(u) \in \mathbb{Z}_d$. $x^\top$ is the transpose of x . Given a single qudit Pauli operator P and a multiset A , let $P_A := \bigotimes_{u \in V} P_u^{A(u)}$.

The commands of a measurement pattern satisfy the following identities, for every $u, v \in V$ such that $u \neq v$ and $a, b \in \mathbb{Z}_d$:

$$X_u Z_v = Z_v X_u, \quad X_u Z_u \simeq Z_u X_u, \quad Z^a Z^b = Z^{a+b} \quad (2.15)$$

$$X_u M_v = M_v X_u, \quad Z_u M_v = M_v Z_u, \quad X^a X^b = X^{a+b} \quad (2.16)$$

$$E_{u,v} X_u = X_u Z_v E_{u,v}, \quad E_{u,v} Z_u = Z_u E_{u,v}, \quad E_{u,v} = E_{v,u} \quad (2.17)$$

where we use the notation $A \simeq B$ to mean that there is a phase $e^{i\alpha}$ such that $A = e^{i\alpha} B$. It was shown by Danos, Kashefi, and Panangaden [DKP07] that any runnable measurement pattern can be rewritten using these commutation relations to the standard form¹:

$$\left(\prod_{v \in O^c}^{\prec} X_{\mathbf{x}(v)}^{m_v} Z_{\mathbf{z}(v)}^{m_v} M_v^{a_v, b_v}(\vec{\theta}_v) \right) \left(\prod_{(u,v) \in G} E_{u,v}^{G_{uv}} \right) \left(\prod_{v \in I^c} N_v \right), \quad (2.18)$$

where I, O are subsets of V , $\mathbf{x}, \mathbf{z}$ are functions $O^c \rightarrow \mathbb{Z}_d^V$, $\prec$ describes an order on O^c for measurement (equivalently, the order of the product), m_v is the outcome

¹They worked in the qubit setting but their proof is purely symbolic. Rewriting $U^\lambda = \prod_{k=0}^\lambda U$ where U is any unitary from equations (2.15)-(2.17), and applying their standardisation procedure results in a pattern of the form (2.18).

of the measurement M_v , G is the matrix of a $\mathbb{Z}_d$ -graph on the vertex set V , and $(u, v) \in G$ identifies an edge in the graph G . The functions $\mathbf{x}, \mathbf{z}$ implicitly describe a weaker measurement order: the transitive closure of the relation $\{(u, v) \mid \mathbf{x}(v)_u \neq 0 \text{ or } \mathbf{z}(v)_u \neq 0\}$ gives a strict partial order $\prec_{\mathbf{x}, \mathbf{z}}$ on O^c . The measurement order $\prec$ must agree with $\prec_{\mathbf{x}, \mathbf{z}}$, and in fact any measurement order that agrees with $\prec_{\mathbf{x}, \mathbf{z}}$ gives a valid standard form.

This motivates the following definition [DK06; Bro+07; Bac+21]:

Definition 2.8. *An open $\mathbb{Z}_d$ -graph is a triple (G, I, O) where G is a $\mathbb{Z}_d$ -graph over V , and $I, O \subseteq V$ are distinguished sets of vertices which identify inputs and outputs in an MBQC.*

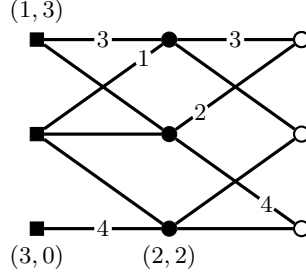
A labelled open $\mathbb{Z}_d$ -graph is a tuple (G, I, O, λ) where (G, I, O) is an open $\mathbb{Z}_d$ -graph and $\lambda : O^c \rightarrow \mathbb{Z}_d^2 \setminus \{(0, 0)\}$ assigns a measurement space to each measured vertex.

If (G, I, O, λ) is a labelled open $\mathbb{Z}_d$ -graph, we let

$$\mathcal{M}(\lambda) := \{\mathbf{M} : O^c \rightarrow U(\mathcal{H}) \mid (\forall v \in O^c) : \mathbf{M}(v) \in \mathcal{M}(\lambda(v))\}, \quad (2.19)$$

which is the set of choices of measurements across the whole open graph that agree with the labelling. Then the form (2.18) describes a 1-to-1 correspondence between measurement patterns and tuples $(G, I, O, \lambda, \mathbf{x}, \mathbf{z}, \mathbf{M})$, where (G, I, O, λ) is a labelled open $\mathbb{Z}_d$ -graph, $\mathbf{x}, \mathbf{z}$ are functions $O^c \rightarrow \mathbb{Z}_d^V$, and $\mathbf{M} \in \mathcal{M}(\lambda)$. $\mathbf{M}$ gives the measurement to be made at each non-output vertex, and $\mathbf{x}, \mathbf{z}$ describe corresponding outcome-dependant corrections. We shall call such a tuple a $\mathbb{Z}_d$ -MBQC. The labelling λ is technically required since the syntax of measurements in equation (2.18) depends on the labelling, but as we shall see in the next section, once the choice of $\mathbf{M}$ is made, λ has no effect on the actual computation carried out by the $\mathbb{Z}_d$ -MBQC (the semantics of the measurement pattern).

When we represent open graphs in figures, we represent input vertices as squares vertices, and outputs as white vertices. The edge weights are represented as usual for colored graphs. For labelled open graphs, labelling of each non-output vertex is written next to the corresponding vertex. Unlabelled vertices correspond to the label $(0, 1)$, and unweighted edges are assumed to have weight 1. Here is an example:



2.2.3 Semantics and determinism

A $\mathbb{Z}_d$ -MBQC $(G, I, O, \lambda, \mathbf{x}, \mathbf{z}, \mathbf{M})$ describes an inherently probabilistic computation with $d \times |O^c|$ possible branches (one for each set of measurement outcomes). For an input state $|\phi\rangle \in \mathcal{H}^{\otimes I}$ and set of outcomes $\vec{m} \in \mathbb{Z}_d^{O^c}$, the corresponding branch in a Kraus decomposition (theorem 1.28) is given by:

$$A_{\vec{m}}^{\mathbf{M}}(|\phi\rangle) := \left(\prod_{v \in O^c}^{\prec} X_{\mathbf{x}(v)}^{m_v} Z_{\mathbf{z}(v)}^{m_v} \langle m_v : \mathbf{M}(v) | v \rangle \right) \left(\prod_{(u,v) \in G} E_{u,v}^{G_{uv}} \right) \left(|\phi\rangle \bigotimes_{u \in I^c} |0 : X\rangle \right), \quad (2.20)$$

which clearly depends on the choice of measurements $\mathbf{M}$. We call the tuple $(G, I, O, \lambda, \mathbf{x}, \mathbf{z})$ a *programmable $\mathbb{Z}_d$ -MBQC*, and encode this dependence in the following definition:

Definition 2.9. *Let $(G, I, O, \lambda, \mathbf{x}, \mathbf{z})$ be a programmable $\mathbb{Z}_d$ -MBQC, then its semantics for a choice of measurements $\mathbf{M} \in \mathcal{M}(\lambda)$ are given by a map defined as:*

$$\begin{aligned} \llbracket G, I, O, \lambda, \mathbf{x}, \mathbf{z} \rrbracket_{\mathbf{M}} &:= \mathfrak{D}(\mathcal{H}^{\otimes I}) \longrightarrow \mathfrak{D}(\mathcal{H}^{\otimes O}) \\ \rho &\longmapsto \sum_{\vec{m} \in \mathbb{Z}_d^{O^c}} A_{\vec{m}}^{\mathbf{M}} \rho A_{\vec{m}}^{\mathbf{M}*}, \end{aligned} \quad (2.21)$$

and which takes values in the set of CPTP maps $\mathcal{H}^{\otimes I} \rightarrow \mathcal{H}^{\otimes O}$.

An MBQC is said to be *deterministic* if the output state never depends on the outcomes of the measurements. This is equivalent to saying that all branches (2.20) are proportional, in which case the pattern is described by the single Kraus operator $K_{\vec{0}}$, corresponding to obtaining outcome 0 for all measurements. This is by construction a correction-less branch since we have then obtained the “preferred” outcome of each measurement. However, a problem comes up if $K_{\vec{0}} = 0$, in which case two deterministic $\mathbb{Z}_d$ -MBQCs can have the same open $\mathbb{Z}_d$ -graph but implement different maps. See [DK06; Bro+07; SP17] for examples.

To exclude these pathological cases, a stronger determinism condition was introduced by Danos and Kashefi [DK06]: a measurement pattern is *strongly*

deterministic if all branch maps are equal up to a global phase. In particular, strongly deterministic measurement patterns implement isometries.

Now, the original purpose of flow was to obtain sufficient and necessary conditions for deciding when such an MBQC is deterministic. However, a characterisation of strong determinism is still an open question, even in the case of qubits. Instead, we restrict our attention to a yet stronger form of determinism, which is both more tractable and arguably more practical [SP17]:

Definition 2.10 (Robust determinism). *A programmable $\mathbb{Z}_d$ -MBQC $(G, I, O, \lambda, \mathbf{x}, \mathbf{z})$ is robustly deterministic if for any $\prec_{\mathbf{x}, \mathbf{z}}$ -lowerset² $S \subseteq O^c$ and any $\mathbf{M} \in \mathcal{M}(\lambda|_S)$, the MBQC $(G, I, O \cup S^c, \lambda|_S, \mathbf{x}|_S, \mathbf{z}|_S, \mathbf{M})$ is strongly deterministic.*

In other words, the MBQC is robustly deterministic if any partial computation is strongly deterministic. Robust determinism is equivalent to the uniformly and stepwise strong determinism of Browne et al. [Bro+07] in the qubit case.

Since the computation implemented by a robustly deterministic MBQC does not depend on the corrections chosen, but only the open graph and the choice of measurements, we simplify the semantics notation in that case to:

$$\llbracket G, I, O, \lambda \rrbracket_{\mathbf{M}} := \sqrt{d \times |O^c|} A_0^{\mathbf{M}}. \quad (2.22)$$

The scalar factor accounts for the fact that the branch maps are not normalised (in fact, the norm of the branch $\|A_{\vec{m}}|\psi\rangle\|$ encodes the probability of obtaining that branch for a given input [DKP07], a trivial piece of information for a robustly deterministic MBQC in which all branches have equal probability of occurring).

2.2.4 Causal flow

All of the preceding discussion begets an obvious question: when is a given measurement pattern robustly deterministic? *Causal flow* was introduced in [DK06] as a graph-theoretical tool for finding robustly deterministic MBQCs. It was the first step in the framework we present in this thesis, and allows only the simplest kinds of corrections. Writing $N(u)$ the neighbourhood of u in a given graph, causal flow is defined as follows:

Definition 2.11 ([DK06]). *An open $\mathbb{Z}_d$ -graph (G, I, O) has a causal flow $(f, \prec)$ if f is a map $O^c \rightarrow I^c$ and $\prec$ a partial order on V such that for any $i \in O^c$,*

1. $i \prec f(i)$;
2. $G_{i, f(i)} \neq 0$;

²If $\prec$ is a partial order on V , then a $\prec$ -lowerset is a subset $S \subseteq V$ such that if $u \prec v$ for some $v \in S$, then $u \in S$.

3. for every $j \in N(f(i)) \setminus \{i\}$, $i \prec j$.

The name reflects the fact that a causal flow can always be viewed as a sequence of single gate teleportations with intermediate controlled- Z operations. When we perform measurements in the corresponding pattern, each input is teleported onto a subsequent vertex in the graph, and thus can be seen to “flow” across the graph state³.

The partial order $\prec$ gives an order for measurement, and the function f identifies, for each measurement $i \in O^c$, a single vertex $f(i)$ which is used for corrections. Condition (1) encodes the fact that this vertex $f(i)$ must not have been measured when we try to perform the correction for i . Condition (2) implies that $f(i)$ is a neighbour of i in the graph G : this is necessary for the kind of corrections which we consider: performing an X^{-1} gate at $f(i)$ has the equivalent effect of applying a Z gate at every neighbour of $f(i)$ (see proposition 2.12). Then, condition (3) is needed to make sure that no previously measured vertex, other than i , is affected by this correction. The remaining Z gates acting in $N(f(i)) \setminus \{i\}$ can be corrected for by applying Z^{-1} .

When only measurements in $\mathcal{M}(0, 1)$ are allowed, causal flow was shown to give rise to a robustly deterministic $\mathbb{Z}_d$ -MBQC $(G, I, O, \mathbf{x}_f, \mathbf{z}_f)$ given by:

$$\mathbf{x}_f(u) = -G_{u,f(u)}^{-1} 1_{\{f(u)\}} \quad \text{and} \quad \mathbf{z}_f(u) = -G_{u,f(u)}^{-1} G 1_{N(f(u)) \setminus \{u\}}, \quad (2.23)$$

which is well-defined by condition 2 of definition 2.11.

In [DK06], this result is stated only in the case of qubits, but it can be easily adapted for qudits. They rely on the relations (2.15)-(2.17), with only two additions, which relate specific preparations and measurements to corrections: for any $u \in O^c$, $v \in I$ and $m \in \mathbb{Z}_2$,

$$\langle 0 : X | R_Z(\alpha) = M_u(\alpha) Z^{m_u} \quad \text{and} \quad X_u^m N_u = N_u. \quad (2.24)$$

These relations hold identically over $\mathcal{L}^2(\mathbb{Z}_d)$ if one takes instead $m \in \mathbb{Z}_d$. As a result, the causal flow condition also applies for qudits, and the resulting measurement pattern $(G, I, O, \mathbf{x}_f, \mathbf{z}_f)$ is robustly deterministic.

³This intuition will later be formalised in terms of *path covers* of the open graph [de 08], but we will not encounter them until chapter 4. Each input corresponds to the starting point of a path that traverses the graph from the inputs to the outputs, identifying the vertices of (G, I, O) that will be “traversed” by each input through subsequent teleportations.

2.3 Graph states

For an open graph (G, I, O) and an arbitrary input state $|\phi\rangle \in \mathcal{H}^{\otimes I}$, we write

$$|G(\phi)\rangle = \left(\prod_{(u,v) \in G} E_{u,v}^{G_{u,v}} \right) \left(|\phi\rangle \bigotimes_{u \in I^c} |0 : X\rangle_u \right), \quad (2.25)$$

which we call an *open graph state*, and put $E_G = \prod_{(u,v) \in G} E_{u,v}^{G_{u,v}}$. Open graph states are resource states for the MBQCs which we describe in this chapter. In the case $I = \emptyset$, we recover the well-known qudit graph states [Zho+03; MMP13]. The stabilisers of an open graph state are given by:

Proposition 2.12 (Open graph stabilisers). *Let (G, I, O) be an open $\mathbb{Z}_d$ -graph, and assume Q is a product of Paulis. Then, $Q|G(\phi)\rangle = |G(\phi)\rangle$ for all $|\phi\rangle \in \mathcal{H}^{\otimes I}$ if and only if there is a multiset $A \in \mathbb{Z}_d^V$ such that $A_v = 0$ for all $v \in I$ and*

$$Q = \omega^{\frac{A^\top G A}{2}} X_A Z_{GA}. \quad (2.26)$$

Proof. The stabilisers of $|G(\phi)\rangle$ are simply the stabilisers of $|\phi\rangle \bigotimes_{u \in I^c} |0 : X\rangle$ conjugated by E_G . It is clear that the stabiliser group of $|0 : X\rangle$ is generated by X^m for all $m \in \mathbb{Z}_d$. Since no Pauli stabilises every $|\psi\rangle \in \mathcal{H}$, it follows that the stabiliser group of $|\phi\rangle \bigotimes_{u \in I^c} |0 : X\rangle$ is of the form X_A for some $A \in \mathbb{Z}_d^V$ such that $A_v = 0$ if $v \in I$. Now, we have

$$E_G X_k^{A_k} E_G^* = \prod_{(u,v) \in G} E_{u,v}^{G_{u,v}} X_k^{A_k} \prod_{\substack{u,v \in V \\ u < v}} E_{u,v}^{G_{u,v}} = X_k^{A_k} \prod_{v \in V} Z_v^{G_{vk} A_k} = X_{A_k} Z_{GA_k}, \quad (2.27)$$

so that

$$E_G X_A E_G^* = E_G \prod_{k \in V} X_k^{A_k} E_G^* = X_k^{A_k} \prod_{v \in V} Z_v^{G_{vk} A_k} \quad (2.28)$$

$$= \prod_{k \in V} X_{A_k} Z_{GA_k} = \omega^{\sum_{k \in V} A_k^\top G \sum_{k \in V} A_k} X_{\sum_{k \in V} A_k} Z_{\sum_{k \in V} G A_k} \quad (2.29)$$

$$= \omega^{A^\top G A} X_A Z_{GA}, \quad (2.30)$$

as claimed. $\square$

ROBUST DETERMINISM IN MEASUREMENT-BASED QUANTUM COMPUTATION WITH QUDITS

We are now ready to begin our study of MBQC proper. This chapter is primarily concerned with finding a characterisation of robust determinism in measurement patterns over a finite cyclic field $\mathbb{Z}_d$. This characterisation will take the form of a linear algebraic condition which relates to the connectivity of the open graph (G, I, O) via its adjacency matrix G . It generalises the two previous flow conditions that were introduced to characterise robust determinism in MBQC with qubits only: causal flow and g-flow.

Causal flow was introduced by Danos and Kashefi [DK06], and was described in section 2.2.4. However, it turned out to be too restrictive a condition. While it is sufficient for robust determinism, only the simplest kinds of corrections were allowed and there are many open graphs corresponding to robustly deterministic patterns that do not have causal flow. This led to the formulation of *generalised flow* or *g-flow* [Bro+07] which was subsequently proven to be a necessary and sufficient condition for a qubit measurement pattern to be robustly deterministic [PSM]. Generalised flow is briefly described in section 3.1.1 of this chapter.

The g-flow condition was originally stated in terms of parity conditions on

The results in this chapter are based on our article, [Boo+21], and the work was presented at the 19th International Conference on Quantum Physics and Logic as well as the Sixth International Conference for Young Quantum Information Scientists.

the neighbourhoods of measured vertices in the labelled open graph (G, I, O, λ) . These conditions can straightforwardly be interpreted as equations in a linear space over the finite field $\mathbb{Z}_2$ (see proposition 3.5). Generalising this construction to the case of any prime d , we get our novel flow condition, $\mathbb{Z}_d$ -flow, which is presented in section 3.1. Then, we show that $\mathbb{Z}_d$ -flow is both sufficient and, in section 3.2, necessary for a $\mathbb{Z}_d$ -measurement pattern to be robustly deterministic. Finally, in section 3.3 we present a polynomial-time algorithm which finds a $\mathbb{Z}_d$ -flow for an input open graph whenever one exists.

This chapter builds on the constructions introduced in chapter 2. Beyond the definitions of measurement patterns and robust determinism which are of course ubiquitous, we make frequent use of the following:

- $\mathbb{Z}_d$ -flow is closely linked to the existence of Pauli stabilisers of open graph states, proposition 2.12; they are essential in the proofs that $\mathbb{Z}_d$ -flow is both necessary and sufficient for robust determinism;
- the proof that $\mathbb{Z}_d$ -flow is necessary for robust determinism relies extensively on the characterisation of measurement spaces from section 2.2.1.

3.1 $\mathbb{Z}_d$ -flow is sufficient for robust determinism

This leads us to the statement of our novel flow condition. It is a strict generalisation of gflow to qudits, which must take into account the additional freedom in open graphs described in section 2.2. Recall that, if $A, B \subseteq V$, $G[A, B]$ is the submatrix of G obtained by keeping only the rows corresponding to elements of A and the columns corresponding to elements of B .

Definition 3.1. A labelled open $\mathbb{Z}_d$ -graph (G, I, O, λ) has a $\mathbb{Z}_d$ -flow (C, Λ) if $C \in \mathbb{Z}_d^{V \times V}$ and Λ is a totally ordered partition of V such that

1. $\forall u \in O^c, \lambda(u) = (C_{uu}, (GC)_{uu})$;
2. $C[I, V] = 0$ and $C[V, O] = 0$;
3. for any $M, N \in \Lambda$,
 - $C[M, M]$ and $(GC)[M, M]$ are diagonal;
 - whenever $M < N$, $C[M, N] = (GC)[M, N] = 0$.

If $\lambda(u) = (0, 1)$ for all $u \in O^c$, we say that (C, Λ) is a simple $\mathbb{Z}_d$ -flow, otherwise it is extended. We call Λ a layer decomposition of (G, I, O, λ) for C and the elements of Λ are layers.

If (G, I, O, λ) is a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) , then we obtain a runnable MBQC $(G, I, O, \lambda, \mathbf{x}_C, \mathbf{z}_C)$ by imposing

$$\mathbf{x}_C(v) := (C_{\bullet v} - \lambda(v)_1 1_{\{v\}}) \quad \text{and} \quad \mathbf{z}_C(v) := ((GC)_{\bullet v} - \lambda(v)_2 1_{\{v\}}), \quad (3.1)$$

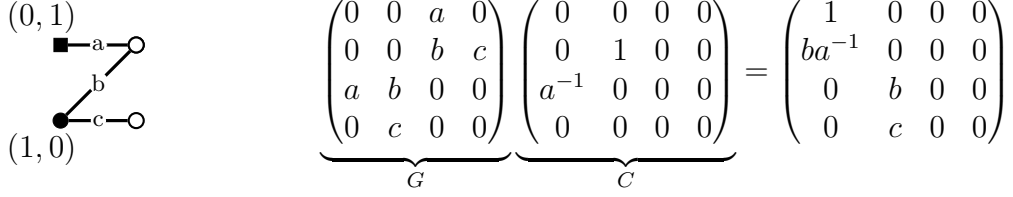


Figure 3.1: An example of a labelled open graph (left) with corresponding $\mathbb{Z}_d$ -flow (right). The inputs of the open graph are square vertices, and the outputs are white. The labelling is written in parentheses next to the unmeasured vertices. The edge weights can take any values in $\mathbb{Z}_d$ with the only constraint being that a must be invertible. We measure the input vertex before the auxiliary non-output, which gives the corresponding layer decomposition.

where $M_{\bullet v}$ is the v -th column of a matrix M .

The layer decomposition Λ describes a (partial) measurement order for the non-output qudits: the qudits can be measured in any totalisation of the order induced on O^c by the order of Λ , and qudits within the same layer can be measured simultaneously. This order is a (not necessarily strict) extension of the order induced by $\mathbf{x}_C, \mathbf{z}_C$ as described in section 2.2.2.

The u -th columns (minus the u -th element) of C and GC then respectively describe where to apply X and Z corrections for the measurement of vertex $u \in O^c$. If u belongs to layer $L \in \Lambda$, the elements in $C_{\bullet u}$ and $(GC)_{\bullet u}$ corresponding to vertices in layers $L < K$ then express the back-action of these corrections on qudits that have already been measured. These matrix elements must consequently be zero for there to be no unwanted back-action. The elements in $C_{\bullet u}$ and $(GC)_{\bullet u}$ that corresponds to vertices in the same layer as u must also be 0, since those vertices can be measured before u . These considerations impose condition 3.

Condition 2 follows from the fact that the outputs are not measured and thus no correction is needed. Furthermore, we cannot apply X corrections at an input vertex, since our proof of robust determinism relies on the fact that $X_u N_u = N_u$.¹ Finally, the u -th element of $C_{\bullet u}$ and $(GC)_{\bullet u}$ describes the effective correction applied at vertex u , $X_{uu}^C Z^{(GC)_{uu}}$, when we follow this procedure. This effective correction must match the measurement space assigned to u so that we can use the back-action to perform the correction, which implies condition 1.

Then this MBQC is deterministic and implements an isometry:

Theorem 3.2. *Suppose the labelled open graph (G, I, O, λ) has $\mathbb{Z}_d$ -flow (C, Λ) , then the programmable MBQC $(G, I, O, \lambda, \mathbf{x}_C, \mathbf{z}_C)$ is runnable and robustly deterministic.*

¹Equivalently, by proposition 2.12, the open graph stabiliser have X components only on non-input vertices of the graph.

Furthermore, for a given choice of measurements $\mathbf{M}$, it realises the isometry $\llbracket G, I, O \rrbracket_{\mathbf{M}} = \mathcal{H}^{\otimes I} \rightarrow \mathcal{H}^{\otimes O} : \sqrt{d \times |O^c|} \otimes_{u \in O^c} \langle 0 : \mathbf{M}(u) | E_G N_{I^c}$.

Proof. Assume (G, I, O, λ) has a $\mathbb{Z}_d$ -flow (C, Λ) . We perform the measurements in the order given by any totalisation of the order induced by Λ on V . We measure qudit u with a M -measurement, and we obtain a classical outcome $s_u \in \mathbb{Z}_d$. Let $Q_u := X_u^{C_{uu}} Z_u^{(GC)_{uu}}$ then by lemma 2.5, the action of any measurement in $\mathcal{M}(\lambda(u))$ correspond to the application on qudit u of the projector $\langle m : M | = \langle 0 : M | Q_u^{s_u}$. Thus a correction must consist in simulating the application of $Q_u^{-s_u}$ on u . The definition of $\mathbb{Z}_d$ -flow implies that C and GC must be lower triangular, so that $X_{(C\{u\}) \setminus \{u\}} Z_{(GC\{u\}) \setminus \{u\}}$ acts only on unmeasured qudits, where $A \setminus \{u\}$ removes all the occurrences of u in A :

$$A \setminus \{u\} = v \mapsto \begin{cases} 0 & \text{if } u = v \\ A(v) & \text{otherwise} \end{cases}. \quad (3.2)$$

Then by proposition 2.12 we have that:

$$X_{(C\{u\}) \setminus \{u\}}^{s_u} Z_{(GC\{u\}) \setminus \{u\}}^{s_u} |G\rangle = X_{(C\{u\}) \setminus \{u\}}^{s_u} Z_{(GC\{u\}) \setminus \{u\}}^{s_u} Q_u^{s_u} Q_u^{-s_u} |G\rangle \quad (3.3)$$

$$= X_{(C\{u\}) \setminus \{u\}}^{s_u} Z_{(GC\{u\}) \setminus \{u\}}^{s_u} Q_u^{-s_u} |G\rangle = Q_u^{-s_u} |G\rangle. \quad (3.4)$$

As a consequence, the correction $X_{(C\{u\}) \setminus \{u\}}^{s_u} Z_{(GC\{u\}) \setminus \{u\}}^{s_u}$ is runnable and makes the computation uniformly deterministic.

Since all the branch maps are equal, the computation is strongly deterministic, and since we have considered only a single measurement and the associated corrections, it is stepwise deterministic.

In [DK06] it was shown that if a measurement pattern is strongly deterministic then it implements an isometry. Since we correct each measurement to the outcome $m = 0$, it is clear after renormalising that the final isometry is given by $\mathcal{H}^{\otimes I} \rightarrow \mathcal{H}^{\otimes O} : \sqrt{d \times |O^c|} \prod_{u \in O^c} \langle 0 : M_u | E_G N_{I^c}$ as claimed. $\square$

3.1.1 Recovering gflow

Generalised flow was originally formulated in terms of a partial order on the vertices to be measured. If $A \subseteq V$, we write $\text{Odd}(A)$ the subset $\bigcup_{a \in A} N(a)$ of vertices that are neighbours of an odd number of elements of A . Then:

Definition 3.3 ([Bro+07]). *A labelled open $\mathbb{Z}_2$ -graph (G, I, O, λ) has g-flow if there exists a map $g : O^c \rightarrow 2^{I^c}$ and a partial order $\prec$ on V such that for all $i \in O^c$,*

- *if $j \in g(i)$ and $i \neq j$ then $i \prec j$;*

- if $j \preceq i$ and $i \neq j$ then $j \notin \text{Odd}(g(i))$;
- if $\lambda(i) = (0, 1)$ then $i \notin g(i)$ and $i \in \text{Odd}(g(i))$;
- if $\lambda(i) = (1, 1)$ then $i \in g(i)$ and $i \in \text{Odd}(g(i))$;
- if $\lambda(i) = (1, 0)$ then $i \in g(i)$ and $i \notin \text{Odd}(g(i))$.

These parity conditions of the connectivity of the open graph can be reinterpreted as linear equations over $\mathbb{Z}_2$, as we see here.

In the case of $\mathbb{Z}_d$ -flow, it is straightforward to see that the order of the layer decomposition Λ induces a (non-unique) partial order on the vertices V . Given a partial order $\prec$ on the vertices V , then there is of course a (also non-unique) ordered partition of V that agrees with $\prec$. Since either of these orders are only used to describe the measurement order for the vertices of the graph, we can write the $\mathbb{Z}_d$ -flow condition in terms which are closer to [Bro+07]:

Lemma 3.4 (Partial order $\mathbb{Z}_d$ -flow). *(G, I, O, λ) has a $\mathbb{Z}_d$ -flow if and only if there exists $C \in \mathbb{Z}_d^{V \times V}$ and a partial order $\prec$ on V such that*

1. $\forall u \in O^c, \lambda(u) = (C_{uu}, (GC)_{uu})$;
2. $C_{uv} = 0$ whenever $u \in I$ or $v \in O$;
3. when the columns and rows of G and C are ordered according to any totalisation of $\prec$, C and GC are lower triangular.

It is straightforward from this formulation to recover the gflow condition, using the intuition that the parity conditions in the original formulation correspond to linear equations over $\mathbb{Z}_2$: we interpret $g(i) \in 2^{I^c}$ as an element of $\mathbb{Z}_2^{I^c}$ which is embedded into $\mathbb{Z}_2^V$ by padding it with zeros. This then corresponds to the column $C_{\bullet, i}$, and the g-flow conditions are then equivalent to those of $\mathbb{Z}_2$ -flow:

Proposition 3.5. *A labelled open $\mathbb{Z}_2$ -graph (G, I, O, λ) has a gflow if and only if it has a $\mathbb{Z}_2$ -flow.*

We omit the formal proofs of these statements, which involve technical calculations of matrix elements and therefore are not particularly informative.

3.2 $\mathbb{Z}_d$ -flow is necessary for robust determinism

It has been shown in the qubit case that any measurement pattern that is robustly deterministic is such that the underlying open graph has a gflow [Bro+07; PSM].² We generalise this result to the case of qudits:

²Note that the claimed proof in [Bro+07] is mistaken. The mistake is corrected by the original authors in the upcoming article [PSM]. The work in this section also corrects the original mistake (in particular the proof of lemma 3.7), but I do not claim the first correct proof.

Theorem 3.6. *If $(G, I, O, \lambda, \mathbf{x}, \mathbf{z})$ is a robustly deterministic $\mathbb{Z}_d$ -MBQC, then the underlying labelled open $\mathbb{Z}_d$ -graph (G, I, O, λ) has a $\mathbb{Z}_d$ -flow (C, Λ) such that $\mathbf{x} = \mathbf{x}_C$ and $\mathbf{z} = \mathbf{z}_C$.*

3.2.1 A technical lemma

Our proof of theorem 3.6 relies crucially on the following technical lemma, which we prove in this section. The idea is that we need to identify the open graph state of an arbitrary robustly deterministic measurement pattern with the open graph state of an open graph³ with $\mathbb{Z}_d$ -flow. However, we in principle only have access to the projected states after measurements have been made. Therefore, it is necessary to show that the set of measurements $\mathcal{M}(\lambda)$ is rich enough to allow us to identify two states which have identical projections on all measurements. Put formally,

Lemma 3.7. *Let (G, I, O, λ) be a labelled open $\mathbb{Z}_d$ -graph, $|\phi\rangle, |\phi'\rangle \in (\mathcal{H}^{\otimes V})_1$ and $R \subseteq V$. For any $\mathbf{M} \in \mathcal{M}(\lambda|_R)$ and $\vec{m} \in \mathbb{Z}_d^R$, put $|\vec{m} : \mathbf{M}\rangle = \bigotimes_{r \in R} |m_r : \mathbf{M}(r)\rangle$. If, for every such $\vec{m}$ and $\mathbf{M}$, we have*

$$\langle \vec{m} : \mathbf{M} | \phi \rangle \simeq \langle \vec{m} : \mathbf{M} | \phi' \rangle \quad \text{and} \quad \|\langle \vec{m} : \mathbf{M} | \phi \rangle\| = \frac{1}{\sqrt{d^{|R|}}} = \|\langle \vec{m} : \mathbf{M} | \phi' \rangle\|, \quad (3.5)$$

then there is a subset $L \subseteq R$, $\vec{x}, \vec{y} \in \mathbb{Z}_d^L$ and $|\psi\rangle \in \mathcal{H}^{\otimes V \setminus L}$ such that

$$|\phi\rangle \simeq |\psi\rangle \bigotimes_{n \in L} |x_n : Q_n\rangle \quad \text{and} \quad |\phi'\rangle \simeq |\psi\rangle \bigotimes_{n \in L} |y_n : Q_n\rangle. \quad (3.6)$$

We build up to the proof of lemma 3.7 itself in a sequence of smaller results. Firstly:

Lemma 3.8. *Let $|\phi\rangle$ be a state of a register V of qudits, $Q = X^a Z^b$ a Pauli operator and fix some $v \in V$. If for every measurement $M \in \mathcal{M}(a, b)$ of the qudit v and every $m \in \mathbb{F}$, we have*

$$\|\langle m : M | \phi \rangle\| = \frac{1}{\sqrt{d}} \quad (3.7)$$

then $|\phi\rangle$ has a Schmidt decomposition of the form

$$|\phi\rangle = \sum_{x \in \mathbb{Z}_d} c_x |x : Q\rangle \otimes |\psi_x\rangle, \quad (3.8)$$

where $|x : Q\rangle$ is an eigenvector of Q associated with eigenvalue ω^x , and we take the coefficients c_x to be real and non-negative.

³Open graph states were defined in section 2.3.

Proof. Pick some $M \in \mathcal{M}(a, b)$, we can write

$$|\phi\rangle = \sum_{m \in \mathbb{Z}_d} |m : M\rangle |\phi_m\rangle \quad \text{where} \quad |\phi_m\rangle := \langle m : M | \phi \rangle \quad (3.9)$$

and $\|\langle m : M | \phi \rangle\| = \frac{1}{\sqrt{d}}$.

Letting $\{|\psi_m\rangle\}$ be the collection of vectors obtained by orthonormalising $\{|\phi_m\rangle\}$, we can expand $|\phi\rangle$ in this basis:

$$|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{m, n \in \mathbb{Z}_d} \Psi_{mn} |m : M\rangle |\psi_n\rangle, \quad \text{and for any } m \in \mathbb{Z}_d, \quad \|\Psi_{m\bullet}\|^2 = 1 \quad (3.10)$$

where Ψ is therefore a $d \times p$ matrix such that p is the dimension of the subspace of $\mathcal{H}^{\otimes V}$ generated by the $|\phi_m\rangle$ and we denote $\Psi_{m\bullet}$ the m^{th} line vector of Ψ .

We know that, for every rotation U in $SU(d)$ preserving Q and every M in $\mathcal{M}(a, b)$, $UMU^\dagger$ is also in $\mathcal{M}(a, b)$. The group of all such rotations acts on Ψ from the left via the Hilbert space representation, and this action is generated by the rotations of the form $V_M^{-1} R_{k,l}(\xi) V_M$, where V_M is the d -dimensional discrete Fourier transform matrix in the eigenbasis of M , and $R_{k,l}(\xi)$ is the diagonal matrix given by $k \in \mathbb{Z}_d$, $l \in \mathbb{Z}_d^*$ and $\xi \in \mathbb{R}$, by

$$R_{k,l}(\xi)_{mm} := \begin{cases} e^{-i\xi} & \text{if } m = k; \\ e^{i\xi} & \text{if } m = k + l; \\ 1 & \text{otherwise.} \end{cases} \quad (3.11)$$

Explicitly, V_M is given by $\langle m : M | V_M | n : M \rangle = \omega^{mn}$. According to equation (3.7), applying a rotation preserving Q to v preserves the outcomes' probabilities. As such, we deduce that the action of rotations $V_M^{-1} R_{k,l}(\xi) V_M$ on matrix Ψ will preserve the norm of its line vectors. Namely, for every $k \in \mathbb{Z}_d$, $l \in \mathbb{Z}_d^*$ and $\xi \in \mathbb{R}$,

$$\|\Psi_{m\bullet}\|^2 = \|(D_{k,l,\xi}\Psi)_{m\bullet}\|^2 \quad \text{where} \quad D_{k,l,\xi} := V_M^{-1} R_{k,l}(\xi) V_M. \quad (3.12)$$

Below, we explicit the right side of this equality to find which Ψ satisfy equation (3.12). First, we compute the row vectors of the transformed matrix:

$$(D_{k,l,\xi}\Psi)_{m\bullet} = \Psi_{m\bullet} + \frac{1}{d} \sum_{\alpha \in \mathbb{Z}_d} \Psi_{\alpha\bullet} \left(\omega^{k(m-\alpha)} (e^{-i\xi} - 1) + \omega^{(k+l)(m-\alpha)} (e^{i\xi} - 1) \right) \quad (3.13)$$

$$= \Psi_{m\bullet} + P_m^{k,l,1} \sin \xi + P_m^{k,l,2} (\cos \xi - 1) \quad (3.14)$$

where

$$P_m^{k,l,1} := -\frac{2}{d} \sum_{\alpha \in \mathbb{Z}_d} \Psi_{\alpha \bullet} \omega^{(k+\frac{l}{2})(m-\alpha)} \sin\left(\frac{\pi l}{d}(m-\alpha)\right) \text{ and} \quad (3.15)$$

$$P_m^{k,l,2} := \frac{2}{d} \sum_{\alpha \in \mathbb{Z}_d} \Psi_{\alpha \bullet} \omega^{(k+\frac{l}{2})(m-\alpha)} \cos\left(\frac{\pi l}{d}(m-\alpha)\right). \quad (3.16)$$

We rewrite equation (3.12) as,

$$\|\Psi_{m\bullet}\|^2 = \|(D_{k,l,\xi}\Psi)_{m\bullet}\|^2 \quad (3.17)$$

$$= \|\Psi_{m\bullet} + P_m^{k,l,1} \sin \xi + P_m^{k,l,2}(\cos \xi - 1)\|^2 \quad (3.18)$$

$$= \|\Psi_{m\bullet}\|^2 + A + B \sin \xi + C \cos \xi + D \cos 2\xi + E \sin 2\xi, \quad (3.19)$$

from which we deduce:

$$A + B \sin \xi + C \cos \xi + D \cos 2\xi + E \sin 2\xi = 0. \quad (3.20)$$

We specify these five alphabetic constants while emphasising that only the expression of D will be used thereafter:

$$A := \frac{3}{2} \|P_m^{k,l,2}\|^2 - 2 \operatorname{Re}(\Psi_{m\bullet} P_m^{k,l,2*}) + \frac{1}{2} \|P_m^{k,l,1}\|^2, \quad (3.21a)$$

$$B := 2 \operatorname{Re}(\Psi_{m\bullet} P_m^{k,l,1*}) - 2 \operatorname{Re}(P_m^{k,l,1} P_m^{k,l,2*}), \quad (3.21b)$$

$$C := 2 \operatorname{Re}(\Psi_{m\bullet} P_m^{k,l,2*}) - 2 \|P_m^{k,l,2}\|^2, \quad (3.21c)$$

$$D := \frac{1}{2} \left(\|P_m^{k,l,2}\|^2 - \|P_m^{k,l,1}\|^2 \right), \quad (3.21d)$$

$$E := 2 \operatorname{Re}(P_m^{k,l,1} P_m^{k,l,2*}), \quad (3.21e)$$

where $P_m^{k,l,i*}$ denotes the complex conjugate of $P_m^{k,l,i}$.

We know that $\{\cos(m\xi), \sin(n\xi)\}_{m,n \in \mathbb{N}}$ forms an orthogonal set in the space of periodic functions of period 2π with respect to the Hermitian form $\langle f, g \rangle := \int_{-\pi}^{\pi} f^*(t)g(t)dt$, and as such, the five alphabetic constants of the left side of equation (3.20) must be zero.

We develop the two terms of the constant D , $\forall m, k \in \mathbb{Z}_d$, $l \in \mathbb{Z}_d^*$, and obtain:

$$\|P_m^{k,l,1}\|^2 = \frac{4}{d^2} \sum_{\alpha, \alpha' \in \mathbb{Z}_d} \Psi_{\alpha}^* \bullet \Psi_{\alpha'} \bullet \omega^{(k+\frac{l}{2})(\alpha-\alpha')} \cos\left(\frac{\pi l}{d}(m-\alpha)\right) \cos\left(\frac{\pi l}{d}(m-\alpha')\right), \quad (3.22a)$$

$$\|P_m^{k,l,2}\|^2 = \frac{4}{d^2} \sum_{\alpha, \alpha' \in \mathbb{Z}_d} \Psi_{\alpha}^* \bullet \Psi_{\alpha'} \bullet \omega^{(k+\frac{l}{2})(\alpha-\alpha')} \sin\left(\frac{\pi l}{d}(m-\alpha)\right) \sin\left(\frac{\pi l}{d}(m-\alpha')\right). \quad (3.22b)$$

Using the addition formulas of trigonometry, we deduce,

$$D = \frac{2}{d^2} \sum_{\alpha, \alpha' \in \mathbb{Z}_d} \Psi_{\alpha}^* \bullet \Psi_{\alpha'} \bullet \omega^{(k+\frac{l}{2})(\alpha-\alpha')} \cos\left(\frac{\pi l}{d}(2m-\alpha-\alpha')\right) = 0. \quad (3.23)$$

We introduce the following change of variables $2\beta := \alpha + \alpha'$ and $2\beta' := \alpha - \alpha'$, such that we obtain,

$$\forall k, n \in \mathbb{Z}_d \text{ and } l \in \mathbb{Z}_d^*, \quad \sum_{\beta, \beta' \in \mathbb{Z}_d} \omega^{2(k+\frac{l}{2})\beta'} \Psi_{\beta+\beta'}^* \bullet \Psi_{\beta-\beta'} \bullet \cos\left(\frac{2\pi l}{d}(m-\beta)\right) = 0. \quad (3.24)$$

Now, for any $l \in \mathbb{Z}_d^*$, the square matrix given by $\Omega_{k,\beta'} := \omega^{2(k+\frac{l}{2})\beta'}$ is invertible. As a consequence, we deduce from the previous equation that $\forall m \in \mathbb{Z}_d$ and $\forall l \in \mathbb{Z}_d^*$,

$$\sum_{\beta \in \mathbb{Z}_d} \Psi_{\beta+\beta'}^* \bullet \Psi_{\beta-\beta'} \bullet \cos\left(\frac{2\pi l}{d}(m-\beta)\right) = 0. \quad (3.25)$$

Developing the cosine, we obtain

$$\begin{aligned} \cos\left(\frac{2\pi l m}{d}\right) \sum_{\beta \in \mathbb{Z}_d} \Psi_{\beta+\beta'}^* \bullet \Psi_{\beta-\beta'} \bullet \cos\left(\frac{2\pi l \beta}{d}\right) \\ + \sin\left(\frac{2\pi l m}{d}\right) \sum_{\beta \in \mathbb{Z}_d} \Psi_{\beta+\beta'}^* \bullet \Psi_{\beta-\beta'} \bullet \sin\left(\frac{2\pi l \beta}{d}\right) = 0, \end{aligned} \quad (3.26)$$

from which we deduce, using again the argument used in equation (3.20), that $\forall l \in \mathbb{Z}_d^*$,

$$\sum_{\beta \in \mathbb{Z}_d} \Psi_{\beta+\beta'}^* \bullet \Psi_{\beta-\beta'} \bullet \cos\left(\frac{2\pi l \beta}{d}\right) = 0, \quad (3.27a)$$

$$\sum_{\beta \in \mathbb{Z}_d} \Psi_{\beta+\beta'\bullet}^* \Psi_{\beta-\beta'\bullet} \sin\left(\frac{2\pi l\beta}{d}\right) = 0. \quad (3.27b)$$

These equations force the following conclusion: for all $\beta \in \mathbb{Z}_d$, the Hermitian product of $\Psi_{\beta+\beta'\bullet}$ and $\Psi_{\beta-\beta'\bullet}$ depends only of β' , namely:

$$\Psi_{\beta+\beta'\bullet}^* \Psi_{\beta-\beta'\bullet} = r_{\beta'}. \quad (3.28)$$

At this point, we define a “Fourier transform” of our line vectors $\Psi_{m\bullet}$ as

$$\Psi_{\gamma\bullet}^F := \frac{1}{\sqrt{d}} \sum_{m \in \mathbb{Z}_d} \Psi_{m\bullet} \omega^{m\gamma}. \quad (3.29)$$

This tranformation is invertible as:

$$\Psi_{m\bullet} = \frac{1}{\sqrt{d}} \sum_{\gamma \in \mathbb{Z}_d} \Psi_{\gamma\bullet}^F \omega^{-m\gamma}, \quad (3.30)$$

so that going back to $|\phi\rangle$,

$$|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{m,n \in \mathbb{Z}_d} \Psi_{mn} |m\rangle |\psi_n\rangle \quad (3.31)$$

$$= \frac{1}{d} \sum_{m,n \in \mathbb{Z}_d} \left(\sum_{\gamma \in \mathbb{Z}_d} \Psi_{\gamma n}^F \omega^{-m\gamma} \right) |m\rangle |\psi_n\rangle \quad (3.32)$$

$$= \frac{1}{d} \sum_{m,\gamma \in \mathbb{Z}_d} \omega^{-m\gamma} |m\rangle \sum_{n \in \mathbb{Z}_d} \Psi_{\gamma n}^F |\psi_n\rangle \quad (3.33)$$

$$= \frac{1}{\sqrt{d}} \sum_{\gamma \in \mathbb{Z}_d} |-\gamma : Q\rangle |\psi_{\gamma}^F\rangle, \quad (3.34)$$

where $|\psi_{\gamma}^F\rangle := \sum_{n \in \mathbb{Z}_d} \Psi_{\gamma n}^F |\psi_n\rangle$. Making good use of equation (3.28), we find that for $\gamma_1, \gamma_2 \in \mathbb{Z}_d$

$$\langle \psi_{\gamma_1}^F | \psi_{\gamma_2}^F \rangle = \sum_{n \in \mathbb{Z}_d} \Psi_{\gamma_1 n}^{F*} \Psi_{\gamma_2 n}^F \langle \psi_n | \psi_n \rangle \quad (3.35)$$

$$= \sum_{n \in \mathbb{Z}_d} \Psi_{\gamma_1 n}^{F*} \Psi_{\gamma_2 n}^F \quad (3.36)$$

$$= \frac{1}{d} \sum_{n \in \mathbb{Z}_d} \left(\sum_{m_1, m_2 \in \mathbb{Z}_d} \Psi_{m_1 n}^* \Psi_{m_2 n} \omega^{-m_1 \gamma_1 + m_2 \gamma_2} \right) \quad (3.37)$$

$$= \frac{1}{d} \sum_{m_1, m_2 \in \mathbb{Z}_d} \left(\sum_{n \in \mathbb{Z}_d} \Psi_{m_1 n}^* \Psi_{m_2 n} \right) \omega^{-m_1 \gamma_1 + m_2 \gamma_2} \quad (3.38)$$

$$\text{according to equation (3.28),} \quad = \frac{1}{d} \sum_{m_1, m_2 \in \mathbb{Z}_d} r_{\frac{m_1 - m_2}{2}} \omega^{-m_1 \gamma_1 + m_2 \gamma_2} \quad (3.39)$$

$$= \frac{1}{d} \sum_{\alpha_1, \alpha_2 \in \mathbb{Z}_d} r_{\alpha_2} \omega^{-(\alpha_1 + \alpha_2) \gamma_1 + (\alpha_1 - \alpha_2) \gamma_2} \quad (3.40)$$

$$\text{summing over } \alpha_1, \quad = \sum_{\alpha_2 \in \mathbb{Z}_d} r_{\alpha_2} \omega^{-\alpha_2 (\gamma_1 + \gamma_2)} \delta_{\gamma_1, \gamma_2}. \quad (3.41)$$

The family $\{|\psi_\gamma^F\rangle\}_{\gamma \in \mathbb{Z}_d}$ forms an orthogonal family. Note that, depending on the value of the r_α , some $|\psi_\gamma^F\rangle$ can be of norm 0. Nevertheless, whenever the condition of equation (3.7) is met, we have a valid Schmidt decomposition of $|\phi\rangle$ of the form

$$\frac{1}{\sqrt{d}} \sum_{\gamma \in \mathbb{Z}_d} |-\gamma : Q\rangle |\psi_\gamma^F\rangle. \quad (3.42)$$

□

Lemma 3.9. *Let $|\phi\rangle, |\phi'\rangle$ be two states of a register V of qudits, $Q = X^a Z^b$ a non-trivial Pauli operator and fix some $v \in V$. If for every measurement $M \in \mathcal{M}(a, b)$ of the qudit v and every $m \in \mathbb{Z}_d$, we have*

$$\langle m : M | \phi \rangle \simeq \langle m : M | \phi' \rangle \quad \text{and} \quad \|\langle m : M | \phi \rangle\| = \frac{1}{\sqrt{d}} = \|\langle m : M | \phi' \rangle\|, \quad (3.43)$$

then at least one of the following holds:

1. $|\phi\rangle \simeq |\phi'\rangle$;
2. $|\phi\rangle$ and $|\phi'\rangle$ are separable and there are $x, y \in \mathbb{Z}_d$ and $|\psi\rangle \in \mathcal{H}^{\otimes V \setminus \{v\}}$ such that

$$|\phi\rangle = |x : Q\rangle_v \otimes |\psi\rangle \quad \text{and} \quad |\phi'\rangle \simeq |y : Q\rangle_v \otimes |\psi\rangle, \quad (3.44)$$

where $|x : Q\rangle$ is an eigenvector of Q associated with eigenvalue ω^x .

Proof. Assume that both $|\phi\rangle, |\phi'\rangle$ have Schmidt rank 1. According to the previous lemma, we can write both states as

$$|\phi\rangle = |x : Q\rangle \otimes |\psi_x\rangle \quad \text{and} \quad |\phi'\rangle = |y : Q\rangle \otimes |\psi'_y\rangle, \quad (3.45)$$

using equation (3.43),

$$|\psi_x\rangle = \sqrt{d} \langle 0 : M | \phi \rangle = e^{i\alpha} \sqrt{d} \langle 0 : M | \phi' \rangle = e^{i\alpha} |\psi'_y\rangle, \quad (3.46)$$

and we are clearly in subcase (2) of the main lemma.

Now, assuming the Schmidt rank along the partition $\{v; V \setminus \{v\}\}$ of both $|\phi\rangle$ and $|\phi'\rangle$ is greater than or equal to 2. According to the previous lemma,

$$|\phi\rangle = \sum_{x \in \mathbb{Z}_d} c_x |x : Q\rangle \otimes |\psi_x\rangle \quad \text{and} \quad |\phi'\rangle = \sum_{x \in \mathbb{Z}_d} c'_x |x : Q\rangle \otimes |\psi'_x\rangle. \quad (3.47)$$

Then, for any $m, k, l \in \mathbb{Z}_d$, and any $\xi \in \mathbb{T}^d$, we have

$$\langle m : M | \phi \rangle = e^{i\alpha_m} \langle m : M | \phi' \rangle, \quad (3.48)$$

$$\langle m : M | D_{k,l,\xi} | \phi \rangle = e^{i\beta(k,l,\xi,m)} \langle m : M | D_{k,l,\xi} | \phi' \rangle, \quad (3.49)$$

where $D_{k,l,\xi}$ is defined as in equation (3.12) and β is a function of the different parameters which define the rotation. Developing the right-hand side of the previous equation we find

$$\langle m : M | D_{k,l,\xi} | \phi' \rangle = \sum_x c'_x \langle m : M | D_{k,l,\xi} | x : Q \rangle |\psi'_x\rangle \quad (3.50)$$

$$= \sum_x \left[\omega^{mx} + \frac{1}{d} \sum_n \omega^{nx} \left(\omega^{k(m-n)} (e^{-i\xi} - 1) + \omega^{(k+l)(m-n)} (e^{i\xi} - 1) \right) \right] c'_x |\psi'_x\rangle. \quad (3.51)$$

Likewise, for the left-hand side, we have for any $m, k, l \in \mathbb{Z}_d$, and any $\xi \in \mathbb{T}^d$,

$$\langle m : M | D_{k,l,\xi} | \phi \rangle \quad (3.52)$$

$$= \langle m : M | \phi \rangle + \frac{1}{d} \sum_n \left(\omega^{j(m-n)} (e^{-i\xi} - 1) \omega^{(j+k)(m-n)} (e^{i\xi} - 1) \right) \langle n : M | \phi \rangle \quad (3.53)$$

$$= e^{i\alpha_m} \langle m : M | \phi' \rangle + \frac{1}{d} \sum_n \left(\omega^{j(m-n)} (e^{-i\xi} - 1) \omega^{(j+k)(m-n)} (e^{i\xi} - 1) \right) e^{i\alpha_n} \langle n : M | \phi' \rangle \quad (3.54)$$

$$= \sum_x \left[e^{i\alpha_m} \omega^{mx} + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{nx} \left(\omega^{k(m-n)} (e^{-i\xi} - 1) \omega^{(k+l)(m-n)} (e^{i\xi} - 1) \right) \right] c'_x |\psi'_x\rangle, \quad (3.55)$$

where we have used equation (3.48) between the first two lines. By identifying components along the orthonormal basis elements $\{|\psi'_x\rangle\}$ and removing terms

where $c'_x = 0$, we can write equation (3.49) as

$$\begin{aligned} & e^{i\beta(j,k,\xi,m)} \left(\omega^{mx} + \frac{1}{d} \sum_n \omega^{nx} \omega^{k(m-n)} (e^{-i\xi} - 1) + \frac{1}{d} \sum_n \omega^{nx} \omega^{(k+l)(m-n)} (e^{i\xi} - 1) \right) \\ &= \omega^{mx} e^{i\alpha_m} + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{nx} \omega^{k(m-n)} (e^{-i\xi} - 1) + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{nx} \omega^{(k+l)(m-n)} (e^{i\xi} - 1). \end{aligned} \quad (3.56)$$

Since $|\phi'\rangle$ has Schmidt rank of at least 2, we can find $y, z \in \mathbb{Z}_d$ such that $y \neq z$, $c'_y \neq 0$ and $c'_z \neq 0$. For the next part, let $k = y$ and $l = z - y$ such that the phase of $D_{k,l,\xi}$ is applied on the two non-zero components.

From now on, we note $\beta(\xi, m) := \beta(y, z - y, \xi, m)$. Taking the coefficients along $|\psi'_y\rangle$, we rewrite the previous equation, for any $\xi \in \mathbb{T}$ and $m \in \mathbb{Z}_d$, as

$$\begin{aligned} & e^{i\beta(\xi,m)} \omega^{my} e^{-i\xi} \\ &= \omega^{my} e^{i\alpha_m} + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{ny} \omega^{y(m-n)} (e^{-i\xi} - 1) + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{ny} \omega^{z(m-n)} (e^{i\xi} - 1), \end{aligned} \quad (3.57)$$

taking the coefficients along $|\psi'_z\rangle$ we extract a different equation,

$$\begin{aligned} & e^{i\beta(\xi,m)} \omega^{mz} e^{i\xi} \\ &= \omega^{mz} e^{i\alpha_m} + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{nz} \omega^{y(m-n)} (e^{-i\xi} - 1) + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{nz} \omega^{z(m-n)} (e^{i\xi} - 1). \end{aligned} \quad (3.58)$$

Finally, for any $\xi \in \mathbb{T}$ and $m \in \mathbb{Z}_d$,

$$e^{i\beta(\xi,m)} = e^{i\xi} e^{i\alpha_m} + \frac{1}{d} \sum_n e^{i\alpha_n} (1 - e^{i\xi}) + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{(z-y)(m-n)} (e^{i2\xi} - e^{i\xi}) \quad (3.59)$$

and

$$e^{i\beta(\xi,m)} = e^{-i\xi} e^{i\alpha_m} + \frac{1}{d} \sum_n e^{i\alpha_n} \omega^{(y-z)(m-n)} (e^{-i2\xi} - e^{-i\xi}) + \frac{1}{d} \sum_n e^{i\alpha_n} (1 - e^{-i\xi}). \quad (3.60)$$

So, the right sides of both equations are equal. However, we can use again the argument below equation (3.21), $\{e^{m\xi}\}_{m \in \mathbb{N}}$ is an orthogonal set in the space of periodic functions. As such, taking the terms in $e^{2\xi}$ and e^ξ ,

$$\sum_n e^{i\alpha_n} \omega^{(z-y)(m-n)} = 0 \quad (3.61a)$$

$$e^{i\alpha_m} - \frac{1}{d} \sum_n e^{i\alpha_n} - \sum_n e^{i\alpha_n} \omega^{(z-y)(m-n)} = 0. \quad (3.61b)$$

Instantly, we get, for all m ,

$$e^{i\alpha_m} = \frac{1}{d} \sum_n e^{i\alpha_n} \quad \text{and in particular} \quad e^{i\alpha_m} = e^{i\alpha_0}. \quad (3.62)$$

We note this common phase α , and this implies by direct calculation that

$$c_x |\psi_x\rangle = e^{i\alpha} c'_x |\psi'_x\rangle \quad (3.63)$$

Based on this result, we can conclude that we are in subcase (1) of the lemma:

$$|\phi\rangle = \sum_x c_x |x : Q\rangle \otimes |\psi_x\rangle, \quad (3.64)$$

$$= \sum_x |x : Q\rangle \otimes (c_x |\psi_x\rangle), \quad (3.65)$$

$$= \sum_x |x : Q\rangle \otimes (e^{i\alpha} c'_x |\psi'_x\rangle), \quad (3.66)$$

$$= e^{i\alpha} \sum_x c'_x |x : Q\rangle \otimes |\psi'_x\rangle, \quad (3.67)$$

$$= e^{i\alpha} |\phi'\rangle, \quad (3.68)$$

as desired.

We have shown that any choice of $|\psi\rangle, |\psi'\rangle$ which verify the conditions of equation (3.43) must fall into either subcase (1) or (2) of the lemma, and we are done. $\square$

Finally, we are ready to prove the main lemma:

Proof of lemma 3.7. The proof proceeds by induction on the size of R . The case $|R| = 0$ is trivial, and the case $|R| = 1$ is lemma 3.9. Assume the statement is true for some non-empty R , if $R = V$ we are done since the induction cannot continue. If this is not the case, pick $u \in V \setminus R$. If

$$\begin{aligned} (\langle m : \mathbf{M}(u) | \otimes \langle \vec{m} : \mathbf{M} |_R) |\phi\rangle &\simeq (\langle m : \mathbf{M}(u) | \otimes \langle \vec{m} : \mathbf{M} |_R) |\phi'\rangle \\ \text{and} \quad \left\| \sqrt{d^{|R|}} (\langle m : \mathbf{M}(u) |_u \otimes \langle \vec{m} : \mathbf{M} |_R) |\phi\rangle \right\| &= \frac{1}{\sqrt{d}} \end{aligned} \quad (3.69)$$

hold for all $m \in \mathbb{F}$, then by lemma 3.9 we have one of the following cases:

1. $\langle \vec{m} : \mathbf{M} |\phi\rangle \simeq \langle \vec{m} : \mathbf{M} |\phi'\rangle$ and $\|\langle \vec{m} : \mathbf{M} |\phi\rangle\| = \frac{1}{\sqrt{d^{|R|}}}$ for any $\vec{m} \in \mathbb{Z}_d^R$ so that by the induction hypothesis we are done.
2. For each $\vec{m} \in \mathbb{Z}_d^R$, there are $x, y \in \mathbb{Z}_d$ and $|\psi_{\vec{m}:\mathbf{M}}\rangle \in \mathcal{H}^{\otimes V \setminus \{u\}}$ such that $\langle \vec{m} : \mathbf{M} |\phi\rangle \simeq |x : Q_u\rangle_u \otimes |\psi_{\vec{m}:\mathbf{M}}\rangle$ and $\langle \vec{m} : \mathbf{M} |\phi'\rangle \simeq |y : Q_u\rangle_u \otimes |\psi_{\vec{m}:\mathbf{M}}\rangle$.

In the latter case, make some arbitrary choice of measurements $\mathbf{M} : R \rightarrow U(\mathcal{H})$, and expand $|\phi\rangle$ in their common eigenbases:

$$|\phi\rangle = \sum_{n \in \mathbb{Z}_d} \sum_{\vec{a} \in \mathbb{Z}_d^R} c(n, \vec{a}) |n : Q_u\rangle_u \otimes |\vec{a} : \mathbf{M}\rangle_R \otimes |\phi(a)\rangle. \quad (3.70)$$

Then in particular, we have that for any choice $\vec{m} \in \mathbb{Z}_d^R$,

$$\langle \vec{m} : \mathbf{M} | \phi \rangle = \sum_{n \in \mathbb{Z}_d} c(n, \vec{m}) |n : Q_u\rangle_u \otimes |\phi(n, \vec{m})\rangle \simeq |x : Q_u\rangle_u \otimes |\psi_{\vec{m} : \mathbf{M}}\rangle, \quad (3.71)$$

which implies that $c(n, \vec{m}) = 0$ whenever $n \neq x$, and we have $|\phi\rangle = |x : Q_u\rangle \otimes |\psi_x\rangle$, where

$$|\psi_x\rangle = \sum_{\vec{m} \in \mathbb{Z}_d^R} c(x, \vec{m}) |\vec{m} : \mathbf{M}\rangle \otimes |\phi(x, \vec{m})\rangle. \quad (3.72)$$

Similarly $\langle \vec{m} : \mathbf{M} | \phi' \rangle \simeq |y : Q_u\rangle \otimes |\psi'_y\rangle$. It follows that for any $\vec{m} \in \mathbb{Z}_d^R$, we must have $\langle \vec{m} : \mathbf{M} | \psi_x \rangle \simeq |\psi_{\vec{m} : \mathbf{M}}\rangle$ and $\langle \vec{m} : \mathbf{M} | \psi'_y \rangle \simeq |\psi_{\vec{m} : \mathbf{M}}\rangle$, so that $\langle \vec{m} : \mathbf{M} | \psi_x \rangle \simeq \langle \vec{m} : \mathbf{M} | \psi'_y \rangle$. Then, by the induction hypothesis, there is $L \subseteq R$ and $\vec{x}, \vec{y} \in \mathbb{Z}_d^{L \cup \{u\}}$ such that $|\phi\rangle = |\psi\rangle \otimes_{v \in L \cup \{u\}} |x_u : Q_u\rangle$ and $|\phi'\rangle = |\psi\rangle \otimes_{v \in L \cup \{u\}} |y_u : Q_u\rangle$, and we are done. $\square$

3.2.2 Proof of the converse theorem

Proof of theorem 3.6. Let $\prec$ be the order on O^c , and consider the last measurement made according to some totalisation of $\prec$. Suppose it is made at vertex u . Let $\mathbf{M} : O^c \rightarrow U(\mathcal{H})$ be such that $\mathbf{M}(v) \in \mathcal{M}(\lambda(v))$ for all $v \in O^c$. Performing the measurement with outcome m , there is a corresponding correction $X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m$ that acts only on outputs, and which induces the branch map:

$$|G(\phi)\rangle \mapsto X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m \left(\langle m : \mathbf{M}(u) | \bigotimes_{v \in O^c \setminus \{u\}} \langle 0 : \mathbf{M}(v) | \right) |G(\phi)\rangle \quad (3.73)$$

$$= X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m \left(\bigotimes_{v \in O^c} \langle 0 : \mathbf{M}(v) | \right) Q_u^m |G(\phi)\rangle, \quad (3.74)$$

$$= \left(\bigotimes_{v \in O^c} \langle 0 : \mathbf{M}(v) | \right) X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m |G(\phi)\rangle \quad (3.75)$$

$$= \bigotimes_{v \in O^c} \langle 0 : \mathbf{M}(v) | G(\phi) \rangle. \quad (3.76)$$

By the uniformity condition, this equation is true for any choice of measure-

ments in $\prod_{v \in O^c} \mathcal{M}(\lambda(v))$. In particular, for any $\mathbf{M} \in \mathcal{M}(\lambda)$, by proposition 2.5 we have $Q_v^{-m} \mathbf{M}(v) Q_v^m \in \mathcal{M}(\lambda(v))$, and

$$\langle 0 : Q_v^{-m} \mathbf{M}(v) Q_v^m | = \langle 0 : \mathbf{M}(v) | Q_v^m = \langle m : \mathbf{M}(v) |. \quad (3.77)$$

It follows that for any choice of measurements $\mathbf{M}$ and any $\vec{m} \in \mathbb{Z}_d^{O^c}$,

$$\langle \vec{m} : \mathbf{M} | X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m | G(\phi) \rangle = \langle \vec{m} : \mathbf{M} | G(\phi) \rangle, \quad (3.78)$$

so by lemma 3.7, there is a subset $L \subseteq O^c$, vectors $\vec{x}, \vec{y} \in \mathbb{Z}_d^{|L|}$ and a state $|\psi\rangle \in \mathcal{H}^{\otimes V \setminus L}$ such that

$$X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m | G(\phi) \rangle \simeq |\psi\rangle \bigotimes_{n \in L} |x_n : Q_n\rangle \quad \text{and} \quad |G(\phi)\rangle \simeq |\psi\rangle \bigotimes_{n \in L} |y_n : Q_n\rangle. \quad (3.79)$$

Then,

$$X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m |\psi\rangle \bigotimes_{n \in L} |x_n : Q_n\rangle \simeq X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m | G(\phi) \rangle \quad (3.80)$$

$$\simeq |G(\phi)\rangle \simeq |\psi\rangle \bigotimes_{n \in L} |y_n : Q_n\rangle. \quad (3.81)$$

If $u \notin L$, then since the corrections only act on outputs this implies that

$$(X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m |\psi\rangle) \bigotimes_{n \in L} |x_n : Q_n\rangle \simeq |\psi\rangle \bigotimes_{n \in L} |y_n : Q_n\rangle, \quad (3.82)$$

so we must have $x_n = y_n$ for all $n \in L$.

If $u \in L$,

$$(X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m |\psi\rangle) \bigotimes_{n \in L} |x_n : Q_n\rangle \quad (3.83)$$

$$\simeq (X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m |\psi\rangle) \otimes Q_u^m |x_u : Q_u\rangle \bigotimes_{n \in L \setminus \{u\}} |x_n : Q_n\rangle, \quad (3.84)$$

$$\simeq (X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m |\psi\rangle) \otimes \omega^{m x_u} |x_u : Q_u\rangle \bigotimes_{n \in L \setminus \{u\}} |x_n : Q_n\rangle, \quad (3.85)$$

$$\simeq |\psi\rangle \otimes |y_u : Q_u\rangle \bigotimes_{n \in L \setminus \{u\}} |y_n : Q_n\rangle, \quad (3.86)$$

which also implies that $x_n = y_n$ for all $n \in L$. Then,

$$X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m Q_u^m | G(\phi) \rangle \simeq |G(\phi)\rangle, \quad (3.87)$$

and $X_{\mathbf{x}(u)}Z_{\mathbf{z}(u)}Q_u$ stabilises the graph state for any $m \in \mathbb{Z}_d$, up to a phase $e^{i\alpha}$. By proposition 2.12 there is some multiset $C_{\bullet u} \in \mathbb{Z}_d^V$ such that

$$e^{i\alpha}X_{\mathbf{x}(u)}Z_{\mathbf{z}(u)}Q_u = \omega^{C_{\bullet u}^\top GC_{\bullet u}}X_{C_{\bullet u}}Z_{GC_{\bullet u}} \quad \text{and} \quad (C_{\bullet u})_v = 0 \quad \text{if} \quad v \in I. \quad (3.88)$$

The corrections act only on outputs, so that the factor of $X_{C_{\bullet u}}Z_{GC_{\bullet u}}^{-1}$ acting on u must be Q_u . This implies that $X_{C_{uu}}Z_{(GC)_{uu}}^{-1} \simeq Q_u$, so that $\lambda(u) = ((C_{\bullet u})_u, (GC_{\bullet u})_u)$, and furthermore, that $(C_{\bullet u})_v = (GC_{\bullet u})_v = 0$ if $v \notin O \cup \{u\}$ since $X_{\mathbf{x}(u)}^m Z_{\mathbf{z}(u)}^m$ acts only on outputs. Furthermore, tensor products of Paulis form a basis of the space of linear operators, so that we must have

$$\mathbf{x}(v) := (C_{\bullet v} - \lambda(v)_1 1_{\{v\}}) \quad \text{and} \quad \mathbf{z}(v) := ((GC)_{\bullet v} - \lambda(v)_2 1_{\{v\}}). \quad (3.89)$$

Now, consider the open graph $(G, I, O \cup \{u\})$. Since $(G, I, O, \lambda, \mathbf{x}, \mathbf{z})$ is robustly deterministic, we can repeat the same procedure on the new open graph

$$(G, I, O \cup \{u\}, \lambda|_{(O \cup \{u\})^c}, \mathbf{x}|_{(O \cup \{u\})^c}, \mathbf{z}|_{(O \cup \{u\})^c}), \quad (3.90)$$

obtaining $C_{\bullet v}$ for the last measured vertex v in $O^c \setminus \{u\}$. This procedure eventually terminates, and we end up with a column vector $C_{\bullet w}$ for each $w \in O^c$. Let $C \in \mathbb{Z}_d^{V \times V}$ be the matrix whose u -th column is $C_{\bullet u}$, or 0 if $u \in O$. Then from the equations in lemma 3.15 we see that the pair $(C, <)$ gives an $\mathbb{Z}_d$ -flow for (G, I, O, λ) by lemma 3.4. Furthermore, it is also clear from equations (6.56) and (3.89) that $\mathbf{x} = \mathbf{x}_C$ and $\mathbf{z} = \mathbf{z}_C$. $\square$

3.3 A polynomial-time algorithm for $\mathbb{Z}_d$ -flow

In this section we formulate an algorithm for finding $\mathbb{Z}_d$ -flow for a given labelled open graph. It is constructed in such a way that it always finds a $\mathbb{Z}_d$ -flow (C, Λ) with optimal depth, in that the cardinality of Λ is minimal over all possible $\mathbb{Z}_d$ -flows. This algorithm is strongly inspired by the analogous algorithm for finding gflows for open $\mathbb{Z}_2$ -graphs [MP08], and its generalisations to multiple measurement planes [Bac+21] and to finding $\mathbb{R}$ -flows [BM21] in continuous-variable quantum computing.

input: A labelled open $\mathbb{Z}_d$ -graph (G, I, O, λ)

output: A $\mathbb{Z}_d$ -flow (C, Λ) or **fail**

- 1: **procedure** Z-FLOW(G, I, O, λ)
- 2: find $L := \{u \in V \mid (\forall v \in V) : G_{uv} = 0\}$ $\triangleright$ Isolated vertices
- 3: layer(0) := $O \cup L$
- 4: $C := 0_{|V| \times |V|}$

```

5:   return Z-FLOW-AUX( $G, I, O \cup L, \lambda|_{O^c \setminus L}, C, \text{layer}, 1$ )

6: procedure Z-FLOW-AUX( $G, I, O, \lambda, C, \text{layer}, k$ )
7:    $L := \emptyset$  ▷ Vertices which we are correcting in this layer
8:   for all  $v \in O^c$  do
9:      $(a, b) := \lambda(v)$ 
10:    solve in  $\mathbb{Z}_d$ :  $G[O^c, O \setminus I]\vec{c} = b1_{\{v\}} - aG[O^c, \{v\}]$ 
11:    if there is a solution  $\vec{c}$  then
12:       $L := L \cup \{v\}$  ▷ Assign  $v$  to the current layer
13:       $C[O \setminus I, \{v\}] := \vec{c}$  ▷ The corrections for vertex  $v$ 
14:       $C[\{v\}, \{v\}] := a$ 
15:    if  $L = \emptyset$  then ▷ If we cannot correct for additional vertices, either:
16:      if  $O = V$  then
17:        return  $(C, \text{layer})$  ▷ we have found a  $\mathbb{Z}_d$ -flow; or,
18:      else
19:        fail ▷ there is no  $\mathbb{Z}_d$ -flow.
20:    else
21:       $\text{layer}(k) := L$ 
22:    return Z-FLOW-AUX( $G, I, O \cup L, \lambda|_{O^c \setminus L}, C, \text{layer}, k + 1$ )
    
```

3.3.1 Correctness

The core of the algorithm is the loop line 8. Letting $n = |V|$, $\ell = |O|$ and $\ell' = |O \setminus I|$ at a given call to Z-FLOW-AUX, note that $\ell' \leq \ell \leq n$. The loop amounts to solving $n - \ell$ systems of $n - \ell$ equations in ℓ' variables. Let x_v be the right hand side of equation line 10. Solving the system can be done by transforming the matrix

$$\left[G[O^c, O \setminus I] \mid x_{v_1} \mid \cdots \mid x_{v_{n-\ell}} \right] \quad (3.91)$$

to upper echelon form. This can be done in time $O(n^3)$ by Gaussian elimination, and backsubstituting to find the corresponding $\vec{c}_j$ to each x_j takes time $O(n^2)$ or for all solutions $O(n^3)$ since there are at most n backsubstitutions to perform. Finally, since each call to Z-FLOW-AUX either eliminates a vertex or terminates, the algorithm recurses at most n times. The total complexity is therefore $O(n^4)$.

Theorem 3.10. *(G, I, O, λ) has a $\mathbb{Z}_d$ -flow if and only if the algorithm above returns a valid $\mathbb{Z}_d$ -flow.*

Proof. It is clear the algorithm terminates, since at each call to Z-FLOW-AUX, the algorithm either passes vertices from $V \setminus O$ to O , returns an $\mathbb{Z}_d$ -flow, or fails. Since V is finite, there are a finite number of recursions after which the algorithm

either returns an $\mathbb{Z}_d$ -flow or fails.

(Outputs a valid $\mathbb{Z}_d$ -flow) Suppose the algorithm terminates with a pair (H, C) . We need to show this defines a valid $\mathbb{F}_q$ -flow. Consider the function Z-FLOW-AUX at a given call, and let $H' := G[O^c, O \setminus I]$ and $h := G[O^c, v]$.

The output columns of C are 0, and since the solution vector x from line 11 never contains an input, the input rows of C are also 0. Hence condition (i) is satisfied.

Similarly, the solution vector x only has rows labelled by vertices $v \geq u$, so C is lower triangular by construction. If the linear equation in line 11 is satisfied, then the entries above $(HC)_{uu}$ in the u -th column of HC will be 0. Hence (ii) is satisfied. Indeed, for any $u > v$, $(HC)_{vu} = \sum_w H_{vw}C_{wu} = \sum_{w < u} H_{vw}C_{wu} + H_{vu}C_{uu} + \sum_{w > u} H_{vw}C_{wu} = h_w a + \sum_{w > u} H'_{vw}x_w$. Since $C_{uu} = a$, $H_{vu} = h_v$, $\forall w < u, C_{wu} = 0$, and $\forall w > u, H_{vw} = H'_{vw}$ and $C_{wu} = x_w$. As a consequence $(HC)_{vu} = (ah + H'x)_v = (ah + b\{u\} - ah)_v$.

Finally, for a non-output u , $C_{uu} = a$. As a consequence C is an $\mathbb{F}_q$ -flow for H .

(Outputs a valid layer decomposition) Let L be as in line 21 of the algorithm for some call k to Z-FLOW-AUX. It is clear that the equation line 10 doesn't depend on the vertices in L which appear before or after $\{v\}$ and therefore L is independent of the order in which the elements of L are found. As a result, the output of the algorithm is invariant any permutation of the vertices in L . Since this corresponds tautologically to a permutation of the layer V_k output by the algorithm, and every permutation that preserves the partition can be written as a product of such permutations, the $\mathbb{Z}_d$ -flow found by the graph is invariant under permutations that preserve the layers (whenever the algorithm succeeds).

(Outputs a $\mathbb{Z}_d$ -flow whenever there is one) Assume the algorithm fails, that is, for some call to Z-FLOW-AUX, line 10 has no solution for any remaining unfinished vertices. Let $\bar{O}$ be the third parameter at that function call, and further assume that D is an $\mathbb{Z}_d$ -flow for (G, I, O, λ) .

Let $\bar{D}$ be the matrix obtained by replacing the columns in D corresponding to $\bar{O}$ with zeros and permuted such that the columns $\bar{O}$ appear last. Then, $\bar{D}$ is an $\mathbb{Z}_d$ -flow for $(G, I, \bar{O}, \lambda|_{\bar{O}^c})$. Let $v \in \bar{O}^c$ be the last column before $\bar{O}^c$, and put $c := \bar{D}[\bar{O} \setminus I, \{v\}]$. Then,

$$(G[\bar{O}^c, \bar{O} \setminus I]c)_u = \sum_{j \in \bar{O} \setminus I} G_{uj}c_j = \sum_{j \in \bar{O} \setminus I} G_{uj}\bar{D}_{jv} = \sum_{j \in \bar{O}} G_{uj}\bar{D}_{jv} = \sum_{j \in \bar{O}} G_{uj}D_{jv} \quad (3.92)$$

$$= \sum_{j \in V} G_{uj}D_{jv} - \sum_{j \in \bar{O}^c} G_{uj}D_{jv} = (GD)_{uv} - \sum_{j \in \bar{O}^c} G_{uj}D_{jv} \quad (3.93)$$

$$= b\delta_{u,v} - G_{uv}D_{vv} = b\delta_{u,v} - aG_{uv}. \quad (3.94)$$

As a result, we see that c verifies the equation of line 10, which contradicts the failure of the algorithm. It follows that (G, I, O, λ) cannot have a $\mathbb{Z}_d$ -flow if the algorithm fails. By contrapositive, if (G, I, O, λ) has a $\mathbb{Z}_d$ -flow, the algorithm succeeds. $\square$

Note this procedure can also be adapted to simultaneously find a $\mathbb{Z}_d$ -flow *and* a corresponding labelling, rather than one fixed in advance. First, note that, for the existence of a $\mathbb{Z}_d$ -flow, it suffices to choose measurement planes up to a scalar factor. That is, (C, Λ) is a $\mathbb{Z}_d$ -flow for (G, I, O, λ) with $\lambda(u) = (a, b)$ if and only if it is a $\mathbb{Z}_d$ -flow for (G, I, O, λ') where $\lambda'(u) = (ka, kb)$. Hence we can solve for measurement planes at the same time as C by either fixing $a = 1$ and solving for b in the equation line 10 of the algorithm, or for non-inputs, fixing $b = 1$ and solving for a .

3.3.2 Depth optimality

Our proofs follow the structure of [MP08], which introduced the idea of optimising gflows starting from the last layer and working back. The idea is to find corrections for as many measured vertices as possible at the part of the MBQC when there are the most constraints on possible corrections: when the only vertices left unmeasured are the outputs. This motivates the following definition which allows us to conveniently manipulate layer decompositions “from the back”:

Definition 3.11. *Let (C, Λ) be a $\mathbb{Z}_d$ -flow for a labelled open graph (G, I, O, λ) . Then, the depth of (C, Λ) is $|\Lambda| - 1$. Furthermore, we define an $\mathbb{N}$ -indexing of the elements of Λ by:*

$$\Lambda_k := \max(\Lambda \setminus \{\Lambda_n \mid n < k\}), \quad (3.95)$$

where we note that $\Lambda_m < \Lambda_n$ as elements of Λ if and only if $n > m$, and $\Lambda_k \neq \emptyset$ if and only if k is less than or equal to the depth of (C, Λ) .

This definition of the depth of a $\mathbb{Z}_d$ -flow corresponds to the intuitive interpretation: all measurements (and corresponding corrections) within a layer can be made concurrently, therefore there is an implementation that runs the MBQC in $|\Lambda| - 1$ rounds of measurements (since the outputs are not measured).

Now, we can use this definition to compare the depths of different $\mathbb{Z}_d$ -flows:

Definition 3.12. *Let (C, Λ) and (D, Φ) be $\mathbb{Z}_d$ -flows for a labelled open graph (G, I, O, λ) . Then (C, Λ) is more delayed than (D, Φ) if for each k ,*

$$\left| \bigcup_{n=0}^k \Lambda_n \right| \geq \left| \bigcup_{n=0}^k \Phi_n \right|. \quad (3.96)$$

and this inequality is strict for at least one k . It is maximally delayed if there is no layer decomposition which is more delayed.

Then, we can give a complete characterisation of the layer decompositions of maximally delayed $\mathbb{Z}_d$ -flows, which turn out to be uniquely defined:

Proposition 3.13. *If (C, Λ) is a maximally delayed $\mathbb{Z}_d$ -flow for a labelled open graph (G, I, O, λ) , then $\Lambda_0 = O \cup \{u \in V \mid (\forall v \in V) : G_{uv} = 0\}$ and for $k > 0$,*

$$\Lambda_k = \left\{ u \in \left(O \bigcup_{1 \leq n < k} \Lambda_n \right)^c \mid \exists c \in \mathbb{Z}_d^V \text{ s.t. } \begin{array}{l} (c_u, (Gc)_u) = \lambda(u) \\ \forall v \notin (O \bigcup_{1 \leq n < k} \Lambda_n) \cup \{u\}, c_v = (Gc)_v = 0 \end{array} \right\}. \quad (3.97)$$

In particular, if (C, Λ) and (D, Φ) are maximally delayed $\mathbb{Z}_d$ -flows for the same labelled open graph, then $\Lambda = \Phi$.

This can be understood from the following principle. If a correction exists for the measurement of a vertex that acts only on outputs, then this correction can be performed at any point during the MBQC, since the outputs are never measured and therefore always available for corrections. As a result, we can delay this measurement as much as possible, to the penultimate layer, to give ourselves as much flexibility as possible in corrections for previous layers. Thus, we can put all vertices whose corrections act only on outputs in the penultimate layer Λ_1 . Any vertices which do not verify this property must be in a layer which precedes the penultimate layer, since at the time they are measured there must be non-output vertices which are left unmeasured. This allows us to uniquely characterise Λ_1 .

The rest of the result is proved by an induction on the layers, which we split into several lemmas since they are each fairly technical. Lemmas 3.14 and 3.15 uniquely characterise Λ_0 and Λ_1 respectively for maximally delayed $\mathbb{Z}_d$ -flows, which gives the base case for the induction. Then lemma 3.16 gives the inductive step.

Lemma 3.14. *If (C, Λ) is a maximally delayed $\mathbb{Z}_d$ -flow for an open graph (G, I, O, λ) , then $\Lambda_0 = O \cup \{u \in V \mid (\forall v \in V) : G_{uv} = 0\}$, i.e. the union of the outputs and isolated vertices of (G, I, O, λ) .*

Proof. Let $A := O \cup \{u \in V \mid (\forall v \in V) : G_{uv} = 0\}$, and define a layer decomposition Λ' on (G, I, O, λ) by

$$\Lambda'_k := \Lambda_k \setminus A \quad \text{for } k > 0 \quad \text{and} \quad \Lambda'_0 = \Lambda_0 \cup A. \quad (3.98)$$

Then it is clear that Λ' is more delayed than Λ . Let C' be the matrix obtained by replacing, for every isolated vertex $u \in V$, the u -th column of C by $C_{uu}1_{\{u\}}$.

We show that (C', Λ') is an $\mathbb{Z}_d$ -flow for (G, I, O, λ) .

1. We haven't touched the diagonal elements of C and have only changed the

columns corresponding to isolated vertices. Then

$$(GC')_{uu} = \begin{cases} \sum_v G_{uv} C_{vu} = 0 & \text{if } u \text{ is isolated;} \\ (GC)_{uu} & \text{otherwise} \end{cases} \quad (3.99)$$

and condition (i) of the definition is still verified.

2. Since $C'_{uv} = C_{uv}$ if $u \in I$ or $v \in O$, we have condition (ii) of the definition.
3. For every $m > n \in \mathbb{N}^*$, $C[\Lambda'_m, \Lambda'_n] = (GC)[\Lambda'_m, \Lambda'_n] = 0$, since they are submatrices of $C[\Lambda_m, \Lambda_n] = (GC)[\Lambda_m, \Lambda_n] = 0$, and $C[\Lambda'_m, \Lambda'_m], (GC)[\Lambda'_m, \Lambda'_m]$ are diagonal for the same reason. Also,

$$(GC')[\Lambda'_m, \Lambda'_0]_{uv} = \begin{cases} 0 & \text{if } v \in \Lambda_0 \text{ since otherwise } (C, \Lambda) \text{ is not an } \mathbb{Z}_d\text{-flow;} \\ \sum_{k \in V} G_{uk} C'_{kv} = G_{uu} C_{uu} = 0 & \text{if } v \text{ is isolated;} \\ \sum_{k \in V} G_{uk} C'_{kv} = \sum_{k \in V} G_{uk} C_{kv} = 0 & \text{if } v \in O. \end{cases} \quad (3.100)$$

Finally, it is clear that $C'[\Lambda'_0, \Lambda'_0]$ is diagonal if $C[\Lambda_0, \Lambda_0]$ was, since we have only added zero for outputs or “diagonal” columns for isolated vertices. Therefore we have condition (iii).

As a result, (C', Λ') is an $\mathbb{Z}_d$ -flow for (G, I, O, λ) that is more delayed than (C, Λ) . This implies that we must have $A \subseteq \Phi_0$ if Φ is maximally delayed.

Now assume there is some $v \in \Lambda_0 \setminus O$. We know that $C[\Lambda_0, \Lambda_0]$ is diagonal and that $GC[\Lambda_n, \Lambda_0] = \sum_{k \in \Lambda} G[\Lambda_n, \Lambda_k] C[\Lambda_k, \Lambda_0] = G[\Lambda_n, \Lambda_0] C[\Lambda_0, \Lambda_0]$. If $C_{uu} \neq 0$, then for $GC[\Lambda_0, \Lambda_0]$ to be diagonal and $GC[\Lambda_n, \Lambda_0] = 0$, we must have either $C_{uv} = 0$ or for all $u \in V$, $G_{uv} = 0$ since then $(GC)_{uv} = G_{uv} C_{vv}$ must be 0 if $u \neq v$. In the latter case, v is isolated in the graph G .

In the former case, $G_{uu} C_{uu} = 0$, and we have $(C_{uu}, (GC)_{uu}) = (0, 0)$. But since u is not an output, we must have $(C_{uu}, (GC)_{uu}) = \lambda(u)$, so that (C, Λ) is not a $\mathbb{Z}_d$ -flow for (G, I, O, λ) . As a result, there can be no such u if (C, Λ) is a valid $\mathbb{Z}_d$ -flow. We conclude that $\Lambda_0 = O \cup \{u \in V \mid (\forall v \in V) : G_{uv} = 0\}$. $\square$

Lemma 3.15. *If (C, Λ) is maximally delayed for (G, I, O, λ) , then*

$$\Lambda_1 = \left\{ u \in O^c \mid \exists c \in \mathbb{Z}_d^{|V|} \text{ s.t. } \begin{aligned} & (c_u, (Gc)_u) = \lambda(u) \\ & \forall v \notin O \cup \{u\}, c_v = (Gc)_v = 0 \end{aligned} \right\}. \quad (3.101)$$

Proof. Let (D, Φ) be a maximally delayed $\mathbb{Z}_d$ -flow for (G, I, O, λ) and define c^u as the u -th column of D . The only elements below the diagonal in column $v \in \Phi_1$ of D correspond to Φ_1 or Φ_0 . Since $D[\Phi_1, \Phi_1]$ and $(GD)[\Phi_1, \Phi_1]$ are diagonal, and $\Phi_0 = O$ by lemma 3.14, for any $v \notin O \cup \{u\}$ we must have $D_{vu} = c_v^u = 0$ and

$(GD)_{vu} = (Gc^u)_v = 0$. The condition $\lambda(u) = (c_u, (Gc)_u)$ itself corresponds to part (iii) of the definition of $\mathbb{Z}_d$ -flow. As a result, every maximally delayed $\mathbb{Z}_d$ -flow of (G, I, O, λ) must verify equation (3.101), and there can be no layer decomposition Φ where Φ_1 is not contained in Λ_1 .

Now, assume (G, I, O, λ) is an open graph with $\mathbb{Z}_d$ -flow, that (D, Φ) is a maximally delayed $\mathbb{Z}_d$ -flow and let $u \in \Lambda_1 \setminus \Phi_1$. Let E be the matrix obtained by replacing the u -th column of D by c^u and permuting the u -th column to the start of Φ_1 . Then (E, Ψ) where

$$\Psi_k := \begin{cases} \Lambda_1 \cup \{u\} & \text{if } k = 1; \\ \Lambda_k \setminus \{u\} & \text{otherwise;} \end{cases} \quad (3.102)$$

is a more delayed $\mathbb{Z}_d$ -flow than (D, Φ) . As a result, there can be no such u , so that if (D, Φ) is maximally delayed, $\Phi_1 = \Lambda_1$. $\square$

Lemma 3.16. *If (C, Λ) is a maximally delayed $\mathbb{Z}_d$ -flow of (G, I, O, λ) , (D, Φ) is a maximally delayed $\mathbb{Z}_d$ -flow of $(G, I, O \cup \Lambda_1, \lambda|_{(O \cup \Lambda_1)^c})$, where*

- D is the matrix obtained by replacing the columns of C corresponding to Λ_1 with zeros;
- Φ is given by

$$\Phi_k := \begin{cases} \Lambda_1 \cup O & \text{if } k = 0; \\ \Lambda_{k+1} & \text{otherwise.} \end{cases} \quad (3.103)$$

Proof. It is clear that (D, Φ) is a layer decomposition, since if it were not, this would imply that (C, Λ) is not either.

There cannot be a more delayed $\mathbb{Z}_d$ -flow of $(G, I, O \cup \Lambda_1, \lambda)$ since that would immediately imply that there is a layer decomposition of (G, I, O, λ) that is more delayed than (C, Λ) . $\square$

Proof of proposition 3.13 (by induction). Λ_0 must take the form given in lemma 3.14. Then, a recursive application of lemma 3.16 and lemma 3.15 shows that the layer decomposition of a maximally delayed $\mathbb{Z}_d$ -flow is uniquely defined.

Since the open graph obtained from lemma 3.16 and used to calculate Λ_k with lemma 3.15 is $(G, I, O \cup_{1 \leq n < k} \Lambda_n, \lambda|_{(O \cup_{1 \leq n < k} \Lambda_n)^c})$, it is clear that Λ_k must take the form claimed. $\square$

It now suffices to show that there is a minimal depth $\mathbb{Z}_d$ -flow that is maximally delayed to obtain:

Proposition 3.17. *A maximally delayed $\mathbb{Z}_d$ -flow for an open graph (G, I, O, λ) has minimal depth.*

Proof. First, note that if (C, Λ) is more delayed than (D, Φ) , then in particular,

$$|V| = \left| \bigcup_{n=0}^{|\Lambda|} \Lambda_n \right| \geq \left| \bigcup_{n=0}^{|\Lambda|} \Phi_n \right|, \quad (3.104)$$

so that $|\Lambda| \leq |\Phi|$. Assume now that (D, Φ) has minimal depth, then any $\mathbb{Z}_d$ -flow that is more delayed has the same depth. It follows that either (D, Φ) is maximally delayed and has minimal depth, or there is a maximally delayed $\mathbb{Z}_d$ -flow that is more delayed than (D, Φ) thus has the same depth. But by proposition 3.13, every maximally delayed $\mathbb{Z}_d$ -flow has the same layer decomposition for a given open graph, so that every maximally delayed $\mathbb{Z}_d$ -flow has minimal depth. $\square$

Note however that a minimal depth decomposition is not necessarily maximally delayed. For example, we can always measure the entirety of the inputs first without changing the depth, but this measurement order is not always maximally delayed since this allows us to move inputs into earlier layers. Since the algorithm is constructed such that it finds a maximally delayed $\mathbb{Z}_d$ -flow:

Theorem 3.18. *The algorithm outputs a $\mathbb{Z}_d$ -flow of minimal depth.*

Proof. Assume that the algorithm succeeds with output (D, Φ) . We show that this output $\mathbb{Z}_d$ -flow (D, Φ) is maximally delayed. Firstly, we show that the output flow has $\Phi_1 = \Lambda_1$ from lemma 3.15. We know that $\Phi_1 \subseteq \Lambda_1$ and it is clear from the definition of the algorithm that

$$\Phi_1 = \left\{ u \in O^c \mid \exists \vec{c} \in \mathbb{Z}_d^{|O \setminus I|} \text{ s.t. } G[O^c, O \setminus I] \vec{c} = b1_{\{v\}} - aG[O^c, \{v\}] \right\} \quad (3.105)$$

Let $u \in \Lambda_1$, that is there is some vector $\vec{c} \in \mathbb{Z}_d^{|V|}$ such that

$$\begin{cases} (c_u, (Gc)_u) = \lambda(u) \\ \forall v \notin O \cup \{u\}, c_v = (Gc)_v = 0 \end{cases} \quad (3.106)$$

Then, for any $v \in O^c$,

$$(G[O^c, V]c)_v = \sum_{j \in V} G_{vj} c_j = \sum_{j \in O \cup \{u\}} G_{vj} c_j \quad (3.107)$$

$$= \sum_{j \in O} G_{vj} c_j + aG_{vu} = (Gc)_v + aG_{vu} = b\delta_{vu} + aG_{vu} \quad (3.108)$$

from which we see that $u \in \Phi_1$ whence $\Phi_1 = \Lambda_1$.

Now, Φ_2 is calculated in the next call to Z-FLOW-AUX where the open graph passed as argument is $(G, I, O \cup \Phi_1, \lambda|_{(O \cup \Phi_1)^c})$. Using the same argument as for Φ_1 , Φ_2 must match the layer Λ_2 obtained by applying lemma 3.15 to the $\mathbb{Z}_d$ -flow resulting from 3.16.

Then, using the same recursion as in the proof of proposition 3.13, we see that (D, Φ) is maximally delayed. It follows from proposition 3.17 that the $\mathbb{Z}_d$ -flow output by the algorithm has optimal depth. $\square$

Corollary 3.19. *If (G, I, O, λ) is a labelled open $\mathbb{Z}_d$ -graph with $\mathbb{Z}_d$ -flow, then it has a maximally delayed $\mathbb{Z}_d$ -flow.*

Proof. If (G, I, O, λ) has a $\mathbb{Z}_d$ -flow, then by theorem 3.10 the algorithm finds a (possibly different) $\mathbb{Z}_d$ -flow for (G, I, O, λ) , which by theorem 3.18 is maximally delayed. $\square$

Conclusion and outlook

We have constructed a flow condition that completely characterises robust determinism in measurement patterns over the field $\mathbb{Z}_d$, and an efficient algorithm for finding $\mathbb{Z}_d$ -flow whenever it exists (and says whenever there is no possible $\mathbb{Z}_d$ -flow).

The main open questions we leave unresolved concern the extension of these results to more general kinds of measurement patterns. Most of our work can be extended to the case of an arbitrary finite field $\mathbb{F}$, wherein the equation of definition 6.5 must hold over $\mathbb{F}$ instead of $\mathbb{Z}_d$. The only result which is missing is the necessity of $\mathbb{F}$ -flow for robust determinism, since we have not found a proof of lemma 3.9 which works for any finite field $\mathbb{F}$. It is not much harder to see that any results for $\mathbb{F}$ -flow hold for R -flow, where R is any ring obtained as a cartesian product of fields. This is because the whole construct factorises over this product at the level of the Hilbert space representation of measurement patterns.

These results fall short of my initial goal of characterising robust determinism over any finite abelian group. Any such abelian group can be viewed as a cartesian product of cyclic groups $\mathbb{Z}_n$, but these cannot be given a nice enough ring structure for our work to apply. Already the group $\mathbb{Z}_4$ only admits a single (non-trivial) ring structure, arithmetic modulo 4, and this ring is not treatable by the methods of this chapter.

We also leave open the generalisation to the qudit setting of other extensions to the measurement calculus. Of these, the one which is most tractable to a natural formulation in the qudit setting is Pauli g-flow. This was defined by Browne et al. [Bro+07], and while it has been hypothesised to completely characterise robust determinism for the corresponding measurement patterns, no proof has yet been published, even in the qubit setting.

A QUANTUM CIRCUIT EXTRACTION ALGORITHM FOR SIMPLE $\mathbb{Z}_d$ -FLOWS

In this chapter, we present a first unitary circuit extraction algorithm for measurement patterns over the field $\mathbb{Z}_d$. Having access to such an extraction algorithm is important for a number of reasons. It makes clear the relationship between the circuit model and MBQC and it is important in order to know, for a robustly deterministic MBQC, what isometry it actually implements in comparable terms to the standard model. This has been key in understanding the improvement MBQC brings in the depth (number of subsequent rounds of simultaneous operations) of a computation at the cost of increasing its “width” (number of involved subsystems) [BK09; MHM15]. As stated in the introduction, it has also proved important in the context of the ZX-calculus, as the algorithms related to flow conditions comprise the most general currently known for extracting a circuit from a ZX-calculus diagram [Dun+20; Bac+21].

Here, we consider only the case where all of the measurements are taken from the measurement space $\mathcal{M}(0, 1)$. As a consequence we no longer need to track the labelling λ , and we simply assume that (G, I, O) is a labelled open graph (G, I, O, λ) where $\lambda(u) = (0, 1)$ for all $u \in O^c$. In this setting, imposing the existence of $\mathbb{Z}_d$ -flow, which must therefore be a simple $\mathbb{Z}_d$ -flow (definition 6.5), greatly restricts the possible connectivities for (G, I, O) , and this in turn simplifies the extraction problem.

The circuit extraction algorithm for extended $\mathbb{Z}_d$ -flows presented in chapter 5

The results in this chapter are adapted from our article, [BM21].

(where all measurement spaces are allowed) completely subsumes what we detail here, but we choose to present this simpler algorithm nonetheless for a couple of reasons. On the one hand, the algorithm presented here is much simpler than that of the general case, but some steps of the general algorithm will greatly resemble those used here. It therefore makes pedagogical sense to present this reduced case first. On the other hand, in chapter 6 we will consider how the MBQC formalism can be extended to the setting of continuous variable quantum computing. For various reasons, it is then necessary to have access to a circuit extraction algorithm to define the semantics. It turns out that we can pretty much re-use the algorithm presented here with a few variations.

In section 4.1, we introduce some new constructions. Firstly, we show how to compose the MBQCs of two labelled open graphs with $\mathbb{Z}_d$ -flow, by identifying (a subset of) the outputs of the first with inputs of the latter. Then we present graph-circuit hybrid diagrams, which combine the graphical notation for both open graphs and quantum circuits. This new notation will be used for examples. Finally, we introduce a new condition equivalent to $\mathbb{Z}_d$ -flow with all measurements in $\mathcal{M}(0, 1)$. This condition splits the set of corrections for each layer into its own object, and this will be more practical for the extraction since we will be extracting the MBQCs layer by layer. In section 4.2 we show how to perform the circuit extraction of a causal flow, by a technique known as *star pattern transformation* (SPT) [DK06; BK09]. Then, in section 4.3, we show how to extract any simple $\mathbb{Z}_d$ -flow by relating it to a sequence of causal flows on which we can apply SPT.

4.1 Preliminaries

4.1.1 Composing measurement patterns

The measurement calculus comes with ways of composing measurement patterns [DKP07]. These manipulations will be useful for the extraction of quantum circuits, so we present them here. We use some slightly different conventions which suit the extraction problem more.

Definition 4.1. Let (G, I, O, λ) and (G', I', O', λ') be open graphs on disjoint vertex sets V and V' , and let γ be a bijection $O \rightarrow I'$. Then we define the composition along γ to be the open graph $(\bar{G}, I, \bar{O}, \bar{\lambda})$ on the set of vertices $\bar{V} = V \cup V' \setminus I'$, where $\bar{O} = (O' \setminus I') \cup \gamma^{-1}(O' \cap I')$ and

$$\bar{G}_{uv} := \begin{cases} G_{uv} & \text{if } u, v \in V \\ G'_{\gamma(u), v} & \text{if } u \in O, v \in V' \\ G'_{uv} & \text{if } u, v \in V' \end{cases}, \quad \bar{\lambda}(u) := \begin{cases} \lambda(u) & \text{if } u \in V \\ \lambda' \circ \gamma(u) & \text{if } u \in O \\ \lambda'(u) & \text{if } u \in V' \end{cases}. \quad (4.1)$$

While this definition might seem complicated, it has an intuitive meaning: we paste together the two open graphs by identifying each vertex $u \in O$ with its image by γ . This amounts to feeding the output state of one MBQC into the inputs of another, and from there it is straightforward to see that we should obtain a $\mathbb{Z}_d$ -flow for the total MBQC:

Proposition 4.2. *Let (G, I, O, λ) and (G', I', O', λ') be open graphs on disjoint vertex sets with $\mathbb{Z}_d$ -flows (C, Λ) and (C', Λ') respectively. Then the composition along a bijection $\gamma : O \rightarrow I'$ has a $\mathbb{Z}_d$ -flow given by*

$$\bar{C} = \begin{pmatrix} C & 0 \\ \bar{G}[V' \setminus I, O]C[O, V] & C'[I'^c, I'^c] \end{pmatrix} \quad (4.2)$$

and $\bar{\Lambda}$ the ordered partition of $\bar{V}$ obtained by appending Λ' to Λ .

Furthermore, for any choice of measurements $\mathbf{M} \in \mathcal{M}(\bar{\Lambda})$,

$$\llbracket (G', I', O', \lambda') \circ (G, I, O, \lambda) \rrbracket_{\mathbf{M}} = \llbracket G', I', O', \lambda' \rrbracket_{\mathbf{M}|_{V'}} \circ U_{\sigma} \circ \llbracket G, I, O, \lambda \rrbracket_{\mathbf{M}|_{V \setminus O}}, \quad (4.3)$$

where U_{σ} is a unitary which permutes the subsystems in the output of (G, I, O, λ) to match the correct inputs of (G', I', O', λ') according to γ .

Proof. The composition along γ simply amounts to feeding the output of the MBQC (G, I, O, λ) as an input into (G', I', O', λ') , where each subsystem $u \in O$ is fed into the input $\gamma(u) \in I'$. The semantics, equation (4.3), follows straightforwardly from this remark.

As for the new $\mathbb{Z}_d$ -flow given by $\bar{C}$ we only need to consider the “new edges” between the I' and V' , since we never allow corrections on the inputs when doing the MBQC corresponding to (G', I', O', λ') . Since the corrections for the vertices in V are already correct, we simply need to calculate the new Z corrections from these new edges. $\square$

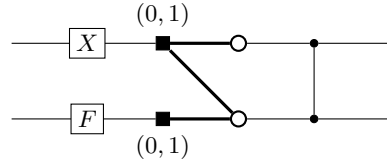
Hopefully, it is clear from this discussion how to do composition of two labelled open graphs where we only identify a subset of O with a subset of I' . This can be formalised using a pair of injective maps

$$O \xleftarrow{\gamma} U \xrightarrow{\delta} I', \quad (4.4)$$

but the construction is even clumsier than what we have just done and therefore not particularly informative. Then, proposition 4.2 holds identically, up to carefully identifying on what qudits the interpretation of (G', I', O', λ') should act. The next section makes this construction clearer still by motivating the unitary U_{σ} of equation (4.3) as a permutation circuit which can be decomposed in terms of SWAP gates.

4.1.2 Graph-circuit hybrid diagrams

In order to present the circuit extraction clearly, we introduce a hybrid representation which is used for partially extracted measurement patterns. For any labelled open graph (G, I, O, λ) , we allow a single incoming quantum wire to be attached to each input, and a single outgoing quantum wire to be attached to each output. The incoming wires connected to the inputs allow one to describe a reversible quantum circuit (i.e. a unitary) which acts on the input state to the MBQC, *before any commands in the pattern are performed*. The outgoing wires connected to outputs form the beginning of another reversible quantum circuit that acts on the output state of the measurement pattern, *after the MBQC is finished*. We allow either the graph part or the circuit part of the diagram to be empty, so that the notation naturally contains both the open graph notation and circuit diagrams as edge cases. If the graph part is empty, we assume that both input and output circuits have the same number of wires, and therefore can be concatenated into one larger overall quantum circuit. As an example, a simple MBQC with some gates acting on the input and followed by a CZ gate on the resulting output state might look like this:



The semantics of such a diagram is defined in the obvious way. Since we are only interested in the case of open graph with $\mathbb{Z}_d$ -flow, the corresponding MBQC is robustly deterministic and therefore corresponds to an isometry. If U_{in} and U_{out} are the unitaries represented by the input and output circuit parts of the diagram respectively, and the graph part is given by (G, I, O, λ) , then for any choice of measurements $\mathbf{M} \in \mathcal{M}(\lambda)$, the semantics of the diagram is $U_{\text{out}} \circ \llbracket G, I, O \rrbracket_{\mathbf{M}} \circ U_{\text{in}}$.

Using this new hybrid notation, we can give a clearer pictorial view of the composition of two measurement patterns. In general, the composition of two diagrams, given in equation (4.3), can be obtained by connecting the wires of (a subset of) the outputs of the former into the wires of (a subset of) the inputs of the latter, up to some permutation of the wires. This permutation is a circuit corresponding to the unitary U_{σ} , and can itself of course be decomposed in terms of SWAP gates.

To illustrate this, consider a pair of labelled open graphs and injective maps as

in equation (4.4):

$$(4.5)$$

where we have suppressed the open graph labelling for simplicity. For any choices of measurements $\mathbf{M}, \mathbf{M}'$ for each open graph, the composition along γ and δ is such that

$$(4.6)$$

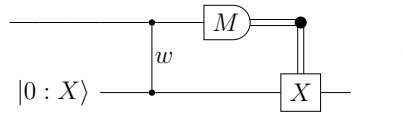
$$(4.7)$$

$$(4.8)$$

where the first line is the graph constructed in definition 4.1. $\mathbf{M} \sqcup \mathbf{M}'$ is obtained by pasting together $\mathbf{M}$ and $\mathbf{M}'$ in the obvious way, and $\bar{\mathbf{M}}$ is obtained by mapping $\mathbf{M} \sqcup \mathbf{M}'$ through the relabelling of vertices in definition 4.1.

4.1.3 Extracting gate teleportations

The key construction which will allow us to extract circuits from MBQCs with $\mathbb{Z}_d$ -flow is the gate teleportation protocol, which as a quantum circuit takes the form



It implements the same unitary as

$$(4.9)$$

where the angle $\alpha \in [0, 2\pi)^d$ is uniquely determined by the choice of measurement $M \in \mathcal{M}(0, 1)$. As a result, we define

$$J(w, \alpha) := M(w)FR_Z(\alpha). \quad (4.9)$$

The gate teleportation protocol can be simply stated in our new notation as

Lemma 4.3. *For any choice of measurement $M \in \mathcal{M}(0, 1)$, there is a unique $\alpha \in [0, 2\pi)^d$ such that*

$$\llbracket \blacksquare \text{---} w \text{---} \bigcirc \rrbracket_M = - \boxed{J(w, \alpha)} \text{---} . \quad (4.10)$$

Proof. The graph has a simple $\mathbb{Z}_d$ -flow given by the matrix

$$C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad (4.11)$$

so by theorem 3.2, we only need to consider the branch map for the measurement outcome 0. If $M \in \mathcal{M}(0, 1)$, by lemma 2.5 there must be a phase $\alpha \in [0, 2\pi)^d$ such that $M = R_Z^*(\alpha)XR_Z(\alpha)$, and in particular $|0 : M\rangle = R_Z^*(\alpha)|0 : X\rangle$. Then, by theorem 3.2 the isometry implemented by the MBQC is given for any input $|\psi\rangle \in \mathcal{H}$ by:

$$\sqrt{d}(\langle 0 : X | R_Z(\alpha) \otimes I)E^w(|\psi\rangle \otimes |0 : X\rangle) \quad (4.12)$$

$$= \sqrt{d}(\langle 0 : X | \otimes M(w))E(R_Z(\alpha)|\psi\rangle \otimes M(w)|0 : X\rangle) \quad (4.13)$$

$$= \sqrt{d}(\langle 0 : X | \otimes M(w))E(|\psi'\rangle \otimes |0 : X\rangle) \quad (4.14)$$

$$= (\langle 0 : X | \otimes M(w)) \sum_{m, n \in \mathbb{Z}_d} \psi'_m \omega^{mn} |m\rangle \otimes |n\rangle \quad (4.15)$$

$$= M(w) \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \psi'_m \omega^{mn} |n\rangle \quad (4.16)$$

$$= M(w)F|\psi'\rangle = M(w)FR_Z(\alpha)|\psi\rangle, \quad (4.17)$$

where we have used the fact that the rotation $R_Z(\alpha)$ commutes with the controlled-phase E . $\square$

Using the work on composition from the previous subsection, we can now state a particularly useful proposition. It is used to extract parts of an MBQC which can be identified with a gate teleportation. This will be the only tool available to us for the actual extraction of a unitary from an MBQC, and the rest of the work will go into relating an open graph with $\mathbb{Z}_d$ -flow to one where this proposition applies.

Proposition 4.4. *Let (G, I, O) be an open graph with simple $\mathbb{Z}_d$ -flow, $u \in O^c$ and $v \in O$ such that $G_{uv} \neq 0$ and for all $w \in V \setminus \{v\}$, $G_{vw} = 0$. Then for any $\mathbf{M} : O^c \rightarrow \mathcal{M}(0, 1)$, there is a unique phase $\alpha \in [0, 2\pi)^d$ such that*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = M(G_{uv})_u F_u R_Z(\alpha)_u \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{\{u\}^c}}, \quad (4.18)$$

where $G' = G[\{v\}^c, \{v\}^c]$, $I' = I \setminus \{v\}$ and $O' = (O \cup \{u\}) \setminus \{v\}$.

Proof. We can see that (G, I, O) is the composition of $\blacksquare \text{---} w \text{---} \bigcirc$ and (G', I', O') along the pair of maps

$$\begin{array}{c} O' \longleftarrow \{*\} \longrightarrow \{\blacksquare\} \\ u \longleftarrow * \longrightarrow \blacksquare \end{array}.$$

It follows that

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \left(\llbracket \blacksquare \text{---} w \text{---} \bigcirc \rrbracket_{\mathbf{M}(u)} \right)_u \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{\{u\}^c}} \quad (4.19)$$

$$= M(G_{uv})_u F_u R_Z(\alpha)_u \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{\{u\}^c}}, \quad (4.20)$$

where we have use lemma 4.3 to extract the teleportation graph. $\square$

A sequence of gate teleportations can then be extracted as the following equation:

$$\left[\begin{array}{c} \blacksquare \text{---} \bullet \text{---} \bullet \text{---} \bigcirc \\ (0,1) \quad (0,1) \quad (0,1) \end{array} \right]_{\mathbf{M}} = \left[\begin{array}{c} \blacksquare \text{---} \bullet \text{---} \bigcirc \text{---} \blacksquare \text{---} \bigcirc \\ (0,1) \quad (0,1) \quad \quad (0,1) \end{array} \right]_{\mathbf{M}} \quad (4.21)$$

$$= \left[\begin{array}{c} \blacksquare \text{---} \bullet \text{---} \bigcirc \text{---} \boxed{J(1, \alpha_3)} \text{---} \\ (0,1) \quad (0,1) \end{array} \right]_{\mathbf{M}|_{\{1,2\}}}, \quad (4.22)$$

where the angle α_3 is obtained by applying lemma 4.3 with the measurement $\mathbf{M}(3)$ of the corresponding vertex. Repeating this procedure sequentially, we obtain a circuit form for the unitary implemented by the measurement pattern:

$$\left[\begin{array}{c} \blacksquare \text{---} \bullet \text{---} \bullet \text{---} \bigcirc \\ (0,1) \quad (0,1) \quad (0,1) \end{array} \right]_{\mathbf{M}} = \text{---} \boxed{J(1, \alpha_1)} \text{---} \boxed{J(1, \alpha_2)} \text{---} \boxed{J(1, \alpha_3)} \text{---} . \quad (4.23)$$

The extraction algorithms presented in this chapter and the next will follow this schema: starting from the outputs, we will show that it is possible to extract a circuit acting after the measurement pattern is completed, and gradually reduce the graph part of the diagram by identifying gate teleportations which can be extracted to the circuit part.

4.1.4 A reformulation of simple $\mathbb{Z}_d$ -flow

In the case of simple $\mathbb{Z}_d$ -flow, i.e. when all the measurement spaces are $\mathcal{M}(0, 1)$, we can rework the condition into an equivalent form which considers, at each step in the MBQC, the specific back-action of corrections on the measured vertices. In order to do so, we first need to decide, for a given vertex u in an open graph (G, I, O) , what vertices will have been measured before it. We skip straight to the case of a set of vertices:

Definition 4.5. Let (G, I, O) be an open graph, $\prec$ a partial order on O^c , and define the past of a subset $L \subseteq O^c$ of vertices of (G, I, O) as

$$P(L) := \{k \in V \mid (\exists j \in L) : k \preceq j\}. \quad (4.24)$$

If Λ is a layer decomposition of (G, I, O) , put $P(k) = \cup_{j \geq k} \Lambda_k$ (the past of layer k). Then the correction matrix G_k^Λ is the matrix $G_k^\Lambda := G[P(k), (P(k) \cup I)^c]$.

$P(L)$ depends on the order $\prec$, but since we only ever consider a single order at once, we omit this from its notation. $P(L)$ can equivalently be defined as the smallest $\prec$ -lower set that contains L . Note that $P(k) = P(\Lambda_k)$ under the order on O^c induced by the ordering of Λ .

G_k^Λ is the subgraph of G which at each step of the MBQC (each layer) describes the back-action of possible corrections made on as-of-yet unmeasured vertices. Viewed this way, simple $\mathbb{Z}_d$ -flow essentially amounts to a condition that assures that this back-action can always be controlled to correct the measurement outcome without inducing new errors in previous layers:

Proposition 4.6. An open $\mathbb{Z}_d$ -graph (G, I, O) has simple $\mathbb{Z}_d$ -flow (C, Λ) if and only if for each k the linear equation

$$G_k^\Lambda \vec{c}_j = \begin{pmatrix} \vec{0}_{P(k) \setminus \Lambda_j} \\ \vec{m} \end{pmatrix} \quad \text{has solutions} \quad \vec{c}_k \in \mathbb{Z}_d^{(P(k) \cup I)^c} \quad \text{for any} \quad \vec{m} \in \mathbb{Z}_d^{\Lambda_k}, \quad (4.25)$$

where $\vec{0}_n$ is a (possibly empty) column vector of n zeros.

Proof. We assume without loss of generality that we only ever measure a single vertex at a time, in other words, that the elements of Λ are singletons in O^c , inducing a total order $<$ on O^c . We also assume that the indices in O come last with respect to $<$ (with some arbitrary order with respect to each other), and that the indices of G are ordered by $<$.

($\implies$) For each $j \in O^c$ let $\vec{c}_j$ be a solution to equation (6.57):

$$A_j^< \vec{c}_j = \begin{pmatrix} \vec{0}_{j-1} \\ m_j \end{pmatrix} \quad \text{for some arbitrary non-zero} \quad m_j \in \mathbb{Z}_d, \quad (4.26)$$

and define the matrix $C \in \mathbb{Z}_d^{|G| \times |G|}$ as the matrix whose i, j -th element is given by

$$C_{ij} := \begin{cases} c_{ji} & \text{if } j \in O^c \text{ and } i \in (P(j) \cup I)^c; \\ 0 & \text{otherwise;} \end{cases} \quad (4.27)$$

where c_{ji} is the i -th element of $\vec{c}_j$. Then, C clearly verifies the properties required of it in the statement: since C is ordered by $<$, there are at least $|P(j)| = j$ zeros above the diagonal in column j , so C is lower triangular with zero diagonal. Furthermore, it is clear that $C_{ij} = 0$ whenever $i \in I$ or $j \in O$.

Since $C_{ij} = 0$ for any $i \in P(j) \cup I$, the j -th column of GC is

$$(GC)_{\bullet j} = \begin{pmatrix} G[P(j), (P(j) \cup I)^c] \cdot C[(P(j) \cup I)^c, \{j\}] \\ G[P(j)^c, (P(j) \cup I)^c] \cdot C[(P(j) \cup I)^c, \{j\}] \end{pmatrix} = \begin{pmatrix} A_j^< \vec{c}_j \\ \vec{x}_j \end{pmatrix} = \begin{pmatrix} \vec{0}_{j-1} \\ m_j \\ \vec{x}_j \end{pmatrix}, \quad (4.28)$$

where $\vec{x}_j$ is a column vector in $\mathbb{Z}_d^{|(P(j)^c)|}$ (which tells us where we need to perform Z -corrections). If $j \in O$, then the j -th column of GC is simply the zero vector. In other words, we have that GC is lower triangular and for any $j \in O^c$, $(GC)_{jj} = m_j$ and we are done.

($\Leftarrow$) Let $<$ be the order of the indices of G , and put $\vec{c}_j := C[(P(j) \cup I)^c, \{j\}]$. We know that $C_{ij} = 0$ if $i \in P(j) \cup I$, since $k \in P(j)$ implies that $k \leq j$, i.e. it is above the diagonal (or is the diagonal element). Then by the definition of $A_j^<$ the j -th column of GC is

$$(GC)_{\bullet j} = G \cdot C_{\bullet j} = \sum_j C_{ij} G_{\bullet j} = \sum_{j \in (P(j) \cup I)^c} C_{ij} G_{\bullet j} = \begin{pmatrix} A_j^< \vec{c}_j \\ \vec{x}_j \end{pmatrix}, \quad (4.29)$$

where $A_j^< \vec{c}_j \in \mathbb{Z}_d^j$ and $\vec{x}_j$ is an unimportant column vector in $\mathbb{Z}_d^{|(P(j)^c)|}$.

Since GC is lower triangular, its j -th column must have $j - 1$ zeros above, so that we have

$$\begin{pmatrix} A_j^< \vec{c}_j \\ \vec{x}_j \end{pmatrix} = \begin{pmatrix} \vec{0}_{j-1} \\ (GC)_{jj} \\ \vec{x}_j \end{pmatrix}. \quad (4.30)$$

Since $(GC)_{jj} \neq 0$, for any $m_j \in \mathbb{Z}_d$,

$$A_j^< (m_j (GC)_{jj}^{-1} \vec{c}_j) = \begin{pmatrix} \vec{0}_{j-1} \\ m_j \\ \vec{x}_j \end{pmatrix}, \quad (4.31)$$

and this is true for each $j \in O^c$, thus (G, I, O) has simple $\mathbb{Z}_d$ -flow. $\square$

4.2 Star pattern transformation

In order to model the computation through the MBQC, the trick is to distinguish between “real” qudits that undergo a unitary transformation through the MBQC (and act like the wires in a circuit undergoing gates), and auxiliary qudits that are consumed in teleportations. In the case of causal flow, things work out nicely as follows.

Definition 4.7 ([de 08]). A path in a graph G is a sequence $(v_n)_{n=0}^{N-1}$ of vertices in G such that for each n , $G_{v_n, v_{n+1}} \neq 0$. A path cover of an open graph (G, I, O) is a collection $\mathcal{P}$ of paths in G such that

- each vertex in G is contained in exactly one path in $\mathcal{P}$;
- each path in $\mathcal{P}$ is either disjoint from I or intersects I only at its initial point;
- each path in $\mathcal{P}$ intersects O only at its final point.

We use the following which also holds for qudits (since causal flow does not depend on edge weights, only the semantics):

Lemma 4.8 (Causal flow path cover [de 08]). Let $(f, \leq)$ be a causal flow on an open graph (G, I, O) . Then there is a path cover $\mathcal{P}_f$ of (G, I, O) where $x \rightarrow y$ is an arc in some path of $\mathcal{P}_f$ if and only if $y = f(x)$.

A causal flow can always be viewed as a sequence of single gate teleportations with intermediate CZ operations. When we perform measurements in the corresponding pattern, each input is teleported onto a subsequent vertex in the graph, and thus can be seen to “flow” across the graph state. A *path cover* of the corresponding open graph formalises this intuition. Each input corresponds to the starting point of a path that traverses the graph from the inputs to the outputs, identifying the vertices of (G, I, O) that will be “traversed” by each input through subsequent teleportations.

Lemma 4.8 allows us to interpret the causal flow MBQC procedure as a sequence of single qudit gate teleportations, with additional entangling operations between teleportations. In fact, the path cover $\mathcal{P}_f$ allows us to distinguish between two types of edges in G :

- edges $(j, k) \in \mathcal{P}_f$ correspond to gate teleportations where one end is the input and the other the output, which we shall call *teleportation edges*;
- edges $(j, k) \notin \mathcal{P}_f$ correspond to controlled- Z gates in the final circuit; and are dubbed *mediating edges*.

Star pattern transformation (STP) [BK09] is a method based on this intuition for turning a measurement pattern on an open graph with causal flow into a quantum

circuit with equivalent semantics. In fact, the only real difficulty at this point is figuring out whether it is possible to totally order the resulting teleportations and mediating CZ s in order to obtain a circuit. Luckily, all we need to worry about is ordering the mediating edges such that they occur before any teleportation of a vertex they are connected to. This is possible since such an ordering exists if and only if there is a causal flow [MHM15] (although this result is stated in [MHM15] only for qubits, it is easily adapted to the case of qudits since once again the causal flow condition can be applied unchanged in that setting, as described in section 2.2.4).

The SPT of a given causal flow can be obtained by the following algorithm:

Assume (G, I, O) is an open graph with causal flow $(f, \prec)$ and corresponding path cover P_f , and let $\mathbf{M} : O^c \rightarrow \mathcal{M}(0, 1)$ be a choice of measurements.

Step 1: Interpret each path in P_f as a wire (qudit) in a quantum circuit, and index the wire by the collection of vertices intersected by the path.

Step 2: For each edge $(j, k) \notin \mathcal{P}_f$, insert a $CZ(G_{jk})$ gate between the edges indexed by j and k .

Step 3: For each edge $(j, k) \in \mathcal{P}_f$, insert a $J(G_{jk}, \alpha)$ gate after all the CZ gates for vertices $i \in \mathcal{P}_f$ such that $i \leq j$ but before all such gates for $k \leq i$, where α is the phase obtained from lemma 4.3 and corresponding to the measurement $\mathbf{M}(j)$.

Step 4: For each path in P_f that does not intersect the inputs, initialise the corresponding wire in the circuit with the auxiliary state $|0 : X\rangle$.

We have that:

Proposition 4.9 (Causal flow circuit). *Suppose the open $\mathbb{Z}_d$ -graph (G, I, O) has a causal flow $(f, \prec)$, then for any choice $\mathbf{M}$ of measurements,*

$$\begin{aligned} \llbracket G, I, O \rrbracket_{\mathbf{M}} : \mathcal{H}^{\otimes I} &\longrightarrow \mathcal{H}^{\otimes O} \\ |\psi\rangle &\longmapsto U_{SPT}(\mathbf{M})(|\psi\rangle \bigotimes_{\substack{j \in O \\ P_j \cap I = \emptyset}} |0 : X\rangle), \end{aligned} \quad (4.32)$$

where U_{SPT} is the unitary corresponding to the circuit obtained by star pattern transformation of f (with phases depending on the choice of measurements $\mathbf{M}$).

Proof. We present a slightly different algorithm that extracts the same circuit as the SPT. Firstly, pull the CZ gates acting only between the outputs into the circuit part of the diagram.

If O^c is empty, the graph part of the diagram consists only in the outputs. Replace all of the inputs (now contained in the outputs) with inputs to the circuit, and the non-inputs with state initialisation in the state $|0 : X\rangle$.

Otherwise, note that there is always at least one element $u \in O^c$ which is maximal for $\prec$ (by the properties of partial orders). By definition of causal flow, u then verifies the hypotheses of proposition 4.4 for the neighbour $f(v) \in O$. We can therefore use the proposition to extract u to a $J(G_{uo}, \alpha)$ gate. It is straightforward to verify that the restriction of f and $\prec$ to $O^c \setminus \{u\}$ gives a causal flow for $(G[\{f(u)\}^c, \{f(u)\}^c], I \setminus \{f(u)\}, (O \cup \{u\}) \setminus \{f(u)\})$ (the graph obtained by removing $f(u)$ and passing u into the outputs), so we can repeat the procedure starting from the first step.

Since we always either extract a vertex of the graph (which are finite) or terminate, this recursion must terminate. $\square$

The upshot of this, is that if (G, I, O) is an open graph with $\mathbb{Z}_d$ -flow, and there is a subset K of the penultimate layer Λ_1 such that there is a causal flow for K , then we can extract the vertices from K :

Proposition 4.10. *Suppose (G, I, O) is an open graph with simple $\mathbb{Z}_d$ -flow, and furthermore that there is a subset $K \subseteq \Lambda_1$ such that there is a causal flow $f : K \rightarrow O$. Then, for any choice of measurements $\mathbf{M} : O^c \rightarrow \mathcal{M}(0, 1)$,*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = U_{SPT}(\mathbf{M}|_K) \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{K^c}}, \quad (4.33)$$

where $G' = G[f(K)^c, f(K)^c]$, $I' = I \setminus f(K)$, $O' = (O \cup K) \setminus f(K)$, and U_{SPT} is the unitary obtained by applying proposition 4.9 to the subgraph between K and $f(K)$.

Proof. As noted in chapter 3, the semantics of a open graph with $\mathbb{Z}_d$ -flow does not depend on the exact choice of $\mathbb{Z}_d$ -flow. Thus, since the vertices in Λ_1 can be measured in any order, we can delay K to the end, and replace the part of the simple $\mathbb{Z}_d$ -flow that describes the corrections for K with f . Furthermore, the definition of causal flow implies that $f(K)$ can be connected *only* with K , so we can view (G, I, O) as the composition of (G', I', O') with the subgraph G'' of G containing only K and $f(K)$. Then,

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \llbracket G'', K, f(K) \rrbracket_{\mathbf{M}|_U} \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{K^c}} \quad (4.34)$$

$$= U_{SPT}(\mathbf{M}|_K) \circ \llbracket G', I', O' \rrbracket_{\mathbf{M}|_{K^c}}, \quad (4.35)$$

for any choice of measurement $\mathbf{M} \rightarrow \mathcal{M}(0, 1)$. $\square$

4.3 Triangularising $\mathbb{Z}_d$ -flow

The next challenge is to generalise this technique to the case of any simple $\mathbb{Z}_d$ -flow. We follow the ideas of [MHM15], associating open graphs with simple $\mathbb{Z}_d$ -flow to equivalent open graphs with (partial) causal flow which allows circuit extraction,

albeit using quite different proof methods. We can then apply proposition 4.10 to extract the causal flow.

More precisely, we show that the simple $\mathbb{Z}_d$ -flow from Λ_1 into Λ_0 can always be reduced to a causal flow, at the cost of some additional gates acting on the outputs. These gates can be extracted immediately to the circuit part of the diagram. Finally, by repeating this procedure for each layer, we extract a circuit for the total MBQC procedure, as a sequence of star pattern transformation circuits and intermediate arrays of CX gates.

4.3.1 From simple $\mathbb{Z}_d$ -flow to causal flow

In order to extract causal flows from simple $\mathbb{Z}_d$ -flows, we need a matricial characterisation of causal flow:

Lemma 4.11 (Matrix form of causal flow). *Let (G, I, O) be an open graph with simple $\mathbb{Z}_d$ -flow for a layer decomposition Λ , and $L \subseteq O^c$. Then there is a subset $C \subseteq P(L)^c$ with $|L| = |C|$ and a causal flow $L \rightarrow C$ if and only if the “correction matrix” of L can be written as*

$$A_L := G[P(L), (P(L) \cup I)^c] = M \cdot \begin{pmatrix} X & 0 \\ Y & T \end{pmatrix} \cdot N \quad (4.36)$$

where M and N are permutation matrices, T is a lower triangular $|V| \times |C|$ matrix with non-zero diagonal and X, Y are arbitrary real matrices. In other words, we can turn A_L into the partial triangular form of equation (4.36) only by reordering rows and columns, which in turn corresponds to relabelling the vertices of the graph G .

Proof. ($\Leftarrow$) If A_L takes the form described, then the diagonal elements of T determine a single correction vertex in C for each vertex in L , as well as a measurement order such that there is no back-action: the order of the columns in T (since all elements above the diagonal are now 0). Thus, there is a causal flow $L \rightarrow C$.

($\Rightarrow$) If there is a causal flow $L \rightarrow C$, then there is a measurement order $<$ on L such that when measuring vertex $i \in L$, there is a single unmeasured vertex $j \in I^c$ to correct onto, and this correction has no back-action on previously measured vertices. But this implies that if we reorder the columns of j according to $<$, column i has only zeros above row j (otherwise there is a back-action), and a non-zero entry in row j (otherwise it is not possible to correct onto j). Repeating this process for each vertex in L gives $|L|$ such columns, let C be the corresponding correction vertices.

Now, $<$ induces an order $<_C$ on C by the causal flow matching. Extend $<$ by

letting all previously measured vertices in $P(L)$ be less than L , and $<_C$ by letting all unmeasured vertices in $P(L)^c$ be less than C . Then, ordering the columns and rows of A_L according to $<$ and $<_C$, respectively, results in a matrix of the form described. $\square$

This characterisation of causal flow is the key difference between our proof method and that of Miyazaki, Hajdušek, and Murao [MHM15]—where they use arguments based on local complementation to find a causal flow from a g-flow, we solve the comparatively easier problem of proving it is always possible to map an open graph with simple $\mathbb{Z}_d$ -flow to one where the correction matrix takes this form.

The approach now is, having broken the measurement pattern down into layers, we show that the graph over each pair of layers can be seen as having flow, by transforming the correction matrix such that it takes the above triangular form. Reordering rows and columns of the correction matrix simply corresponds to relabelling of the vertices, however, we will also require linear addition of columns. This matrix or graphical operation, it turns out, is physically equivalent to applying CX gates, which are exactly the additional operations in the equivalence mentioned previously.

This emerges from the following stabiliser condition for controlled operators. For any $j \in V$ and $S \subseteq V \setminus \{j\}$, put

$$\text{CZ}_{j,S}(w) := \prod_{k \in S} \text{CZ}_{j,k}(w), \quad (4.37)$$

then,

Lemma 4.12 (Controlled stabilisers). *Let (G, I, O) be an open $\mathbb{Z}_d$ -graph, $j \in G$ and $k \in I^c$. Then, for any input state $\phi \in \mathcal{H}^{\otimes |I|}$*

$$\text{CX}_{j,k}(s) \text{CZ}_{j,N(k)}(s) |G(\phi)\rangle = |G(\phi)\rangle. \quad (4.38)$$

Proof. We have $\text{CX}_{j,k}(s) \text{CZ}_{j,N(k)}(s)G = G \text{CX}_{j,k}(s)$, and

$$\text{CX}_{j,k}(s)(|\psi\rangle_j \otimes |0 : X\rangle_k) = \text{CX}_{j,k}(s)(\sum \psi_n |n\rangle_j \otimes |0 : X\rangle_k) \quad (4.39)$$

$$= \sum_{n \in \mathbb{Z}_d} \psi_n |n\rangle_j \otimes X(sn) |0 : X\rangle_k \quad (4.40)$$

$$= \sum_{n \in \mathbb{Z}_d} \psi_n |n\rangle_j \otimes |0 : X\rangle_k \quad (4.41)$$

$$= |\psi\rangle_j \otimes |0 : X\rangle_k, \quad (4.42)$$

which proves the claim. $\square$

Corollary 4.13. *Let (G, I, O) be an open $\mathbb{Z}_d$ -graph, $j \in G$ and $k \in I^c$. Then, for any input state $\phi \in \mathcal{H}^{\otimes |I|}$*

$$\text{CX}_{j,k}(-s) |G(\phi)\rangle = \text{CZ}_{j,N(k)}(s) |G(\phi)\rangle. \quad (4.43)$$

In this way, the action of specific CZ operations - which are what are used to create or remove edges in the graph - are equivalent to the application of a CX operation. This allows us to achieve our goal of identifying a causal flow from the penultimate layer to the outputs:

Proposition 4.14 (Triangularisation). *If (G, I, O) is an open graph with simple $\mathbb{Z}_d$ -flow (C, Λ) , then (G, I, O) is equivalent to an open graph with a causal flow $\Lambda_1 \rightarrow O$, up to weighted CX gates acting in O and reordering the vertices in Λ_1 .*

Proof. We can reorder the columns of G_Λ^1 by relabeling the unmeasured vertices, and we can reorder the rows of G_Λ^1 by choosing a different measurement order for vertices in Λ_1 .

Further let $j, k \in O$, then by corollary 4.13 applying the gate $\text{CX}_{j,k}(-s)$ on the graph state induces new edges in the graph state. The result on the correction matrix is the transformation

$$C_j \mapsto C_j + sC_k, \quad (4.44)$$

where C_j is the j -th column of A_L .

By the definition of simple $\mathbb{Z}_d$ -flow, for each $v \in L$ we have that

$$G_\Lambda^1 c_v(1_v) = 1_v, \quad (4.45)$$

so that $c_v(1_v)$ gives a sum of columns G_Λ^1 which contains a single 1 in the row corresponding to v . Repeating this for each $v \in \Lambda_1$, we obtain $|\Lambda_1|$ such columns, each with the 1 on a different row, so that by reordering rows and columns we can write G_Λ^1 as

$$G_\Lambda^1 \sim \begin{pmatrix} X & 0 \\ Y & I_{|\Lambda_1|} \end{pmatrix} \quad (4.46)$$

where $I_{|\Lambda_1|}$ is the $|\Lambda_1| \times |\Lambda_1|$ identity matrix. Then, G_Λ^1 takes the form described in lemma 4.11, and this partial triangularisation procedure corresponds to extracting additional CX gates from the graph as described above. Then, the open graph (G, I, O) is approximately equivalent to a graph with causal flow $\Lambda_1 \rightarrow O$, up to CX gates acting in O . $\square$

The fact that the additional controlled gates act only on the outputs is crucial: it will allow us to immediately pull them out into the circuit part of the diagram.

As a result, they are taken care of in the extraction procedure and do not need to be taken into account of in the following steps.

4.3.2 The extraction algorithm

We now can give a description of the circuit extraction algorithm for simple $\mathbb{Z}_d$ -flows. An example of the algorithm applied to a specific open graph is given in section 4.4.

Assume the input to the algorithm takes the form of a graph-circuit diagram D and a simple $\mathbb{Z}_d$ -flow (C, Λ) for the open graph part (G, I, O) .

Step 1: If the graph part of the diagram contains no non-outputs, then each output is connected to an output wire and at most one input wire. Delete the output vertices, connect the inputs to the corresponding output wires, and initialise any $u \in I^c \cap O$ in the auxiliary state $|0 : X\rangle$. Then, return the resulting quantum circuit. Otherwise, go on to step 2.

Step 2: Calculate a triangularisation for the flow $\Lambda_1 \rightarrow O$, and pull the corresponding CX gates into the circuit part (corollary 4.13). This is always possible by proposition 4.14, and can be done by a Gaussian elimination.

Step 3: Use proposition 4.10 to extract the quantum circuit corresponding to the resulting causal flow $\Lambda_1 \rightarrow O$. The result is a graph-circuit diagram D' whose semantics match D for any choice of measurement. The graph part of D' is $(G[f(\Lambda_1)^c, f(\Lambda_1)^c], I \setminus f(\Lambda_1), (O \cup \Lambda_1) \setminus f(\Lambda_1))$, and by lemma 3.16, it has a simple $\mathbb{Z}_d$ -flow. Return to step 1.

Theorem 4.15 (Simple $\mathbb{Z}_d$ -flow circuit). *Let (G, I, O) be an open $\mathbb{Z}_d$ -graph with simple $\mathbb{Z}_d$ -flow (C, Λ) , then for any choice $\mathbf{M} : O^c \rightarrow \mathcal{M}(0, 1)$ of measurements,*

$$\begin{aligned} \llbracket G, I, O \rrbracket_{\mathbf{M}} : \mathcal{H}^{\otimes I} &\longrightarrow \mathcal{H}^{\otimes O} \\ |\psi\rangle &\longmapsto \prod_{L \in \Lambda} T^L U_{SPT}^L(\mathbf{M}|_L)(|\psi\rangle \bigotimes_{\substack{j \in O \\ P_j \cap I = \emptyset}} |0 : X\rangle). \end{aligned} \quad (4.47)$$

where the product is ordered according to the order on layers, U_{SPT}^L is the parametrised circuit extracted for layer L using the causal flow from corollary 4.13, and T^L contains the CX gates obtained from the triangularisation of the $\mathbb{Z}_d$ -flow (lemma 4.14).

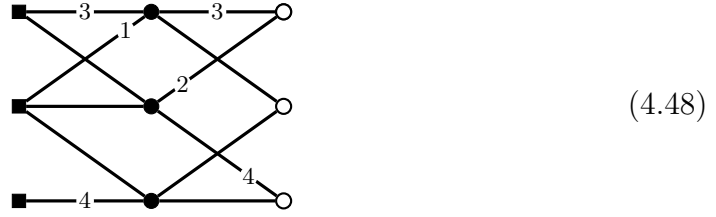
Proof. It is clear the algorithm terminates since at every recursive step we extract a layer into the circuit part of the diagram, and there are a finite number of layers.

The correctness of the algorithm follows from the fact that each step is correct, and this is proved in the statement of the algorithm by referring to the corresponding lemmas and propositions. $\square$

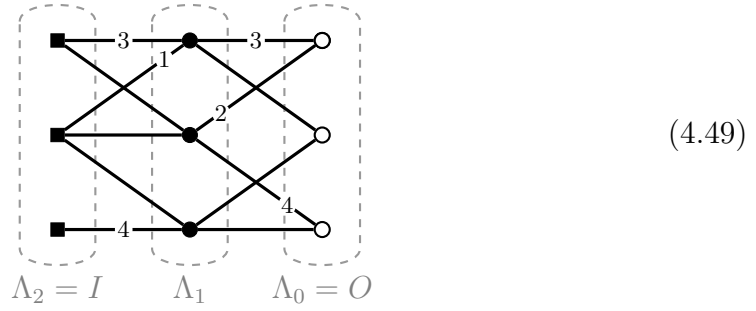
Since each step of the algorithm runs in time polynomial (step 1 is $O(|V|)$, step 2 can be done in time $O(|V|^3)$ by Gaussian elimination, and step 3 is $O(|V|)$) and the algorithm loops at most $|V|$ times, the total runtime of the algorithm is polynomial.

4.4 A worked out example

This section contains a complete worked out example of a circuit extraction, where the algorithm is applied step by step on the open graph



It has a simple $\mathbb{Z}_5$ -flow given by the layer decomposition



and correction matrix

$$\underbrace{\begin{pmatrix} & 3 & 1 & 0 \\ & 1 & 1 & 0 \\ & 0 & 1 & 4 \\ 3 & 1 & 0 & & 3 & 2 & 0 \\ 1 & 1 & 1 & & 1 & 0 & 1 \\ 0 & 0 & 4 & & 0 & 4 & 1 \\ & 3 & 1 & 0 \\ & 2 & 0 & 4 \\ & 0 & 1 & 1 \end{pmatrix}}_G \underbrace{\begin{pmatrix} 0 \\ 0 & 0 \\ 0 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 2 & 4 & 0 & 0 & 0 \\ 2 & 4 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 2 & 0 \\ 0 & 0 & 0 & 4 & 4 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 2 & 3 & 0 & 0 & 0 \end{pmatrix}}_C = \begin{pmatrix} 1 \\ 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (4.50)$$

where the empty matrix elements are taken to be 0. Note that the definition of $\mathbb{Z}_d$ -flow enforces that $\lambda(u) = (0, 1)$ for all $u \in O^c$, thus we indeed have a simple $\mathbb{Z}_5$ -flow by lemma 4.6.

Since the circuit is extracted from the back of the open graph, in the first step of the algorithm, we start with layer Λ_1 . Firstly, use Gaussian elimination to triangularise the sub-adjacency matrix $G[\Lambda_0^c, \Lambda_0]$, which must be possible by proposition 4.14:

$$G[\Lambda_0^c, \Lambda_0] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 4 & 1 \end{pmatrix} \xrightarrow{\begin{matrix} C_2 \leftarrow C_2 + C_1 \\ C_3 \leftarrow C_3 + 4C_2 \end{matrix}} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 4 & 2 \end{pmatrix} \quad (4.51)$$

Using corollary 4.13 to extract this triangularisation into the corresponding CX

operations in the circuit part of the diagram yields the equality:

$$(4.52)$$

By lemma 4.11, there is a causal flow $\Lambda_1 \rightarrow \Lambda_0$, so we can use SPT to obtain

$$(4.53)$$

where we have identified the new layer decomposition for the reduced graph. The unitaries J_4, J_5, J_6 are the J gates from the corresponding teleportation and are passed the angle for the measurement and the weight of the edge along which the teleportation occurs as arguments (see lemma 4.3). Repeating the triangularisation procedure for layer Λ_2 leads to:

$$G_{(1)}[\Lambda_0^c, \Lambda_0'] = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 4 \end{pmatrix} \xrightarrow{C_2 \leftarrow C_2 + 3C_1} \begin{pmatrix} 3 & 0 & 0 \\ 1 & 4 & 0 \\ 0 & 1 & 4 \end{pmatrix} \quad (4.54)$$

so that, applying lemma 4.11 a second time,

$$(4.55)$$

Using another SPT, the final extracted circuit for the whole MBQC is

$$(4.56)$$

where we have labelled the unitaries in the decomposition of theorem 4.15. Once again, the unitaries J_1, J_2, J_3 are the J gates from the corresponding teleportation and are passed the angle for the measurement and the weight of the edge along which the teleportation occurs as arguments.

Conclusion and outlook

We have provided a quantum circuit extraction for any open graph with simple $\mathbb{Z}_d$ -flow (i.e. when only the measurement space $\mathcal{M}(0, 1)$ is allowed), by relating it to a sequence of causal flows with intermediate CX gates. In the following chapter, we show how to use some of these methods to extract quantum circuits from extended $\mathbb{Z}_d$ -flows.

As mentioned in the introduction, many of the results presented here will also be re-used in chapter 6, which is concerned with MBQC in the continuous variable settings. There, we shall mostly be concerned with issues of convergence when the auxiliary state used to generate the open graph state is only an approximation to the ideal. Doing so will require us to reframe and extend many of the results from this chapter.

QUANTUM CIRCUIT EXTRACTION FOR EXTENDED $\mathbb{Z}_d$ -FLOWS

In the final chapter on qudits, we construct an algorithm for extracting reversible quantum circuits from robustly deterministic measurement patterns when *all* measurement spaces are allowed. Our algorithm is inspired in many ways by the one presented in [Bac+21] for the qubit case, but has its differences, and all proofs have to be redone to fit the setting of qudits. This algorithm also builds on the algorithm presented in chapter 4, since we once again proceed by using $\mathbb{Z}_d$ -flow-preserving transformations of the open graph to relate the measurements to gate teleportations.

The full extraction problem presents additional complications when compared to the simplified subcase which we solved in chapter 4, for a couple of reasons. On the one hand, up until this point we have only shown how to extract unitary gates from measurements in $\mathcal{M}(0, 1)$, by relating them to the gate teleportation protocol. Even a very simple labelled open graph such as

$$\begin{array}{c} \bullet \\ (1,0) \end{array} \text{---} \square \quad , \quad (5.1)$$

has a (non-simple) $\mathbb{Z}_d$ -flow, but it is not obvious how this should relate to the gate teleportation protocol¹.

This chapter is based on our upcoming article, [BP21].

¹In fact, this graph corresponds to a gadget for a Z -rotation gate, i.e. $R_Z(\alpha)$. It can be extracted as such, but this does not help us find a general extraction method.

On the other hand, the existence of extended $\mathbb{Z}_d$ -flow on an open graph imposes fewer restrictions on its connectivity than simple $\mathbb{Z}_d$ -flow, and this makes the task of identifying vertices to be extracted at any step in the algorithm a more subtle affair. A particularly pathological example is the complete graph on n vertices, with a single output o , no inputs, and such that every non-output is labelled by $(1, -1)$. In the case $n = 4$, this corresponds to



This open graph $(G^n, \emptyset, \{o\})$ has a $\mathbb{Z}_d$ -flow (C^n, Λ^n) given by

$$\underbrace{\begin{pmatrix} J_n - 1_n & J_{n \times 1} \\ J_{1 \times n} & 0 \end{pmatrix}}_{G^n} \underbrace{\begin{pmatrix} 1_n & 0_{n \times 1} \\ -J_{1 \times n} & 0 \end{pmatrix}}_{C_n} = \begin{pmatrix} -1_n & 0_{n \times 1} \\ J_{1 \times n} & 0 \end{pmatrix}, \quad (5.3)$$

where $J_{n \times m}$ is the $m \times n$ all-ones matrix, and

$$\Lambda^n = \{\{o\}^c, \{o\}\} \quad \text{such that} \quad \{o\}^c < \{o\}. \quad (5.4)$$

It therefore has a single output, while simultaneously having an arbitrary number of non-output vertices in the penultimate layer. If we want to extract such a graph using similar methods to the previous chapter, we are going to have to split up the penultimate layer since we can extract at most one teleportation edge at a time through the single output.

Fortunately, the solution to both of these difficulties lies in a single idea: using local-Clifford operations, we can simultaneously act on both the connectivity and the labels of the open graph. The nature of this action is explored in section 5.1 in terms of *local complementations* and *local scalings* of the open graph which collectively generate the local Clifford group [BB07b]. Crucially, it preserves the structure of measurement spaces and the semantics of the measurement pattern.

Using these operations, we can isolate a subset Λ_1^Z of the penultimate layer Λ_1 of any $\mathbb{Z}_d$ -flow (C, Λ) by changing all of its labels to $(0, 1)$. In doing so, we simplify the topology of the subgraph between Λ_1^Z and O enough that we can apply (a version of) the triangularisation technique of the previous chapter. Of course, the local Clifford operations affect multiple vertices of the graph, and in a way that depends on its connectivity. Since they also change the connectivity itself, some care is needed in correctly isolating Λ_1^Z , and this is the content of section 5.2. This allows us, in section 5.3, to present the extraction algorithm itself, along with some simplifications. Finally, in section 5.4, we present some explicitly worked out examples of applying the algorithm to some specific labelled open graphs.

5.1 Manipulating $\mathbb{Z}_d$ -flows with local Cliffords

Recall from chapter 2 that the Clifford group G on a qudit is the subgroup of $U(\mathcal{H})$ which preserves the Pauli group. We define the *local Clifford* group on a register V of qudits to be the group of operators $\{\otimes_{k \in V} P_k \mid (\forall k \in V) : P_k \in G\}$. Furthermore, we say that two graph states are *local Clifford equivalent* if there is a local Clifford operator that maps one to the other. We introduce two types of local Clifford operations, which we call local complementation and local scaling. It was show in [BB07b; BB07a] that any local-Clifford equivalence of graph states can be can be generated by just these two kinds of local Cliffords.

In this section, we show that both of these operations preverve the existence of $\mathbb{Z}_d$ -flow as well as the semantics of any corresponding measurement pattern. The key to the semantics part of this statement is the following simple result:

Lemma 5.1. *Let $(a, b) \in \mathbb{Z}_d^2$ be non-zero, and $M \in \mathcal{M}(a, b)$. If $U \in U(\mathcal{H})$ is any unitary such that $UX^aZ^bU^* \simeq X^cZ^d$, then $UMU^* \in \mathcal{M}(c, d)$.*

Proof. We have for some $\alpha \in [0, 2\pi)$:

$$X^cZ^dUMU^* = e^{i\alpha}UX^aZ^bU^*UMU^* = e^{i\alpha}UX^aZ^bMU^* \quad (5.5)$$

$$= e^{i\alpha}\omega UMX^aZ^bU^* = \omega UMU^*X^cZ^d, \quad (5.6)$$

as required. $\square$

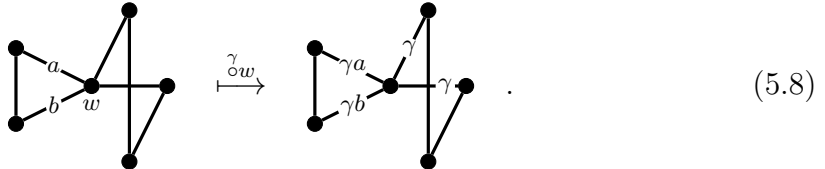
In other word, if a unitary transformation U maps the Pauli correction X^aZ^b to another Pauli correction X^cZ^d , then the image of the corresponding measurement space under the same unitary is $UM(a, b)U^* = \mathcal{M}(c, d)$.

5.1.1 Local scaling

Definition 5.2. *For any $\gamma \in \mathbb{Z}_d^*$, the γ -scaling about a vertex w in a graph G is given by:*

$$(G \circlearrowleft w)_{uv} := \begin{cases} \gamma G_{uv} & \text{if } u = w \text{ or } v = w; \\ G_{uv} & \text{otherwise.} \end{cases} \quad (5.7)$$

In other words, we apply a multiplicative scaling to all of the edges in the neighbourhood of w . For example:



Let $D_\gamma^w \in \mathbb{Z}_d^{V \times V}$ be the diagonal matrix given by

$$(D_\gamma^w)_{uv} = \begin{cases} 1 & \text{if } u = v \neq w; \\ \gamma & \text{if } u = v = w; \\ 0 & \text{otherwise.} \end{cases} \quad (5.9)$$

Lemma 5.3. $G \overset{\gamma}{\circ} w = D_\gamma^w G D_\gamma^w$.

Proof. This is clear since multiplying by D_γ^w on the left rescales the w -th row, and multiplying on the right rescales the w -th column. The only possible issue is at G_{ww} , but since we don't allow self-edges, $\gamma^2 G_{ww} = 0 = \gamma G_{ww}$. $\square$

First of all, we find a unitary representation of local scaling, which will be used to apply lemma 5.1:

Proposition 5.4. Let (G, I, O) be an open $\mathbb{Z}_d$ -graph. For any $|\phi\rangle \in \mathcal{H}^{\otimes I}$, $\gamma \in \mathbb{Z}_d^*$ and $w \in I^c$,

$$|G \overset{\gamma}{\circ} w(\phi)\rangle = M_w(\gamma^{-1}) |G(\phi)\rangle, \quad (5.10)$$

where $M(\gamma) |k\rangle := |\gamma \cdot k\rangle$, and this map is local-Clifford.

If $w \in I$, then

$$|G \overset{\gamma}{\circ} w(\phi)\rangle = M_w(\gamma^{-1}) |G(\phi')\rangle, \quad (5.11)$$

where $|\phi'\rangle = M_w(\gamma) |\phi\rangle$.

Proof. We have

$$M_1(\gamma^{-1}) \cdot E_{1,2} \cdot M_1(\gamma) |m\rangle |n\rangle = \omega^{\gamma mn} |m\rangle |n\rangle = E_{1,2}^\gamma |n\rangle |m\rangle, \quad (5.12)$$

and $M(\gamma) |0 : X\rangle = |0 : X\rangle$. Therefore, if $w \in I^c$, by commuting M through the E gates in equation 2.18 we obtain:

$$M_w(\gamma^{-1}) |G\rangle = M_w(\gamma^{-1}) \left(\prod_{\substack{u,v \in V \\ u < v}} E_{u,v}^{G_{uv}} \right) \left(|\psi\rangle \bigotimes_{u \in I^c} |0 : X\rangle \right) \quad (5.13)$$

$$= \left(\prod_{v \in N(w)} E_{u,v}^{\gamma G_{wv}} \right) \left(\prod_{\substack{u,v \in V \setminus \{w\} \\ u < v}} E_{u,v}^{G_{uv}} \right) M_w(\gamma^{-1}) \left(|\psi\rangle \bigotimes_{u \in I^c} |0 : X\rangle \right) \quad (5.14)$$

$$= \left(\prod_{\substack{u,v \in V \\ u < v}} E_{u,v}^{(G \circ w)_{uv}} \right) \left(|\psi\rangle \bigotimes_{u \in I^c} |0 : X\rangle \right) = |G \circ w\rangle, \quad (5.15)$$

as desired. In the case where $w \in I$, we do the same commutation through the E gates, but cannot do the simplification of the $M_w(\gamma^{-1})$ gate on the stabiliser state. Instead, the gate remains, acting on the corresponding input.

Then, for any $k \in \mathbb{Z}_d$ and non-zero $(a, b) \in \mathbb{Z}_d^2$, we have

$$M(\lambda)^* X^a Z^b M(\lambda) |k\rangle = M(\lambda)^* X^a Z^b |\lambda k\rangle \quad (5.16)$$

$$= M(\lambda)^* \omega^{b\lambda k} |\lambda k + a\rangle \quad (5.17)$$

$$= \omega^{b\lambda k} |k + \lambda^{-1}a\rangle \quad (5.18)$$

$$= X^{\lambda^{-1}a} Z^{\lambda b} |k\rangle \quad (5.19)$$

so $M(\lambda)^* X^a Z^b M(\lambda) = X^{\lambda^{-1}a} Z^{\lambda b}$ and $M(\lambda)$ is local-Clifford. $\square$

We can now use this unitary presentation to show that local scaling preserves both the existence of $\mathbb{Z}_d$ -flow, and the corresponding semantics of the MBQC. To do so, we construct a new open graph, with a new labelling and $\mathbb{Z}_d$ -flow which are obtained by considering the action of the corresponding unitary.

Proposition 5.5. *Suppose the labelled open graph (G, I, O, λ) has a $\mathbb{Z}_d$ -flow given by (C, Λ) . Then for any $w \in V$ and $\gamma \in \mathbb{Z}_d^*$, $(G \circ w, I, O, \lambda^{\circ w})$ has a $\mathbb{Z}_d$ -flow given by $(D_{\gamma^{-1}}^w C, \Lambda)$, and with labels*

$$\lambda^{\circ w}(u) := \begin{cases} \left(\gamma^{-1} C_{ww}, \gamma(GC)_{ww} \right) & \text{if } u = w; \\ \left(C_{uu}, (GC)_{uu} \right) & \text{otherwise;} \end{cases} \quad (5.20)$$

(where we originally had $\lambda(u) = (C_{uu}, (GC)_{uu})$).

If $w \in O^c$, for any $\mathbf{M} \in \mathcal{M}(\lambda)$, put

$$\mathbf{M}^{\circ w}(u) := \begin{cases} M(\gamma) \mathbf{M}(u) M(\gamma^{-1}) & \text{if } u = w; \\ \mathbf{M}(u) & \text{otherwise;} \end{cases} \quad (5.21)$$

then $\mathbf{M}^{\circ w} \in \mathcal{M}(\lambda^{\circ w})$ and

$$\llbracket G \circ w, I, O \rrbracket_{\mathbf{M}^{\circ w}} = \llbracket G, I, O \rrbracket_{\mathbf{M}}. \quad (5.22)$$

If $w \in O$, we have

$$M_w(\gamma^{-1}) \circ \llbracket G \circ w, I, O \rrbracket_{\mathbf{M}} = \llbracket G, I, O \rrbracket_{\mathbf{M}}, \quad (5.23)$$

and if $w \in I$,

$$\llbracket G \overset{\gamma}{\circ} w, I, O \rrbracket_{\mathbf{M}} \circ M_w(\gamma^{-1}) = \llbracket G, I, O \rrbracket_{\mathbf{M}}. \quad (5.24)$$

Proof. Left multiplication by a diagonal matrix only rescales rows, so it is clear that $D_{\gamma^{-1}}^w C$ and $(G \overset{\gamma}{\circ} w)C = D_{\gamma}^w G D_{\gamma}^w D_{\gamma^{-1}}^w C = D_{\gamma}^w G C$ are lower triangular. It is clear that local scaling preserves layers since it only rescales rows and columns thus preserves conditions (ii) and (iii) of the definition of $\mathbb{Z}_d$ -flow.

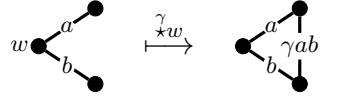
The semantics part follows from the fact that if the scaling acts on measured vertices, then it is absorbed into the choice of measurement plane at w , otherwise we pull it out of the pattern as a unitary acting on the outputs. $\square$

5.1.2 Local complementation

For any $\gamma \in \mathbb{Z}_d^*$, the γ -weighted local $\mathbb{Z}_d$ -complementation or γ -complementation about a vertex w in a graph $G \in \mathbb{Z}_d^{V \times V}$ is defined as:

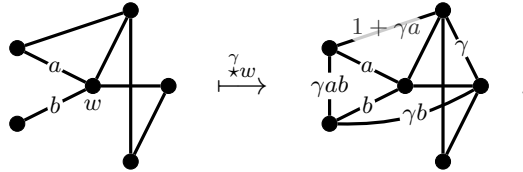
$$(G \overset{\gamma}{\star} w)_{uv} := \begin{cases} G_{uv} + \gamma G_{uw} G_{wv} & \text{if } u \neq v; \\ G_{uv} & \text{otherwise.} \end{cases} \quad (5.25)$$

This operation is somewhat harder than local scaling to get a good intuition for. It essentially operates on “cones” in G with summit w . The simplest example is the following:



$$\quad (5.26)$$

In a more complicated graph, local complementation about w performs this simple operation for every such “cone” with summit w . For example,



$$\quad (5.27)$$

We can give a more linear-algebraic form of local complementation as follows:

Proposition 5.6. For a vector $v \in \mathbb{Z}_d^n$, let D_v be the corresponding diagonal $n \times n$ matrix. If $G \in \mathbb{Z}_d^{V \times V}$, $w \in V$ and $\gamma \in \mathbb{Z}_d^*$, then

$$G \overset{\gamma}{\star} w = G + \gamma G 1_{\{w\}} 1_{\{w\}}^T G - \gamma D_{G_{ew}}^2. \quad (5.28)$$

Proof. The proof follows by directly calculating elements: if $u, v \in V$ and $u \neq v$,

$$(G + \gamma G 1_{\{w\}} 1_{\{w\}}^T G - \gamma D_{Ge_w}^2)_{uv} = G_{uv} + \gamma G_{uw} G_{wv} - \gamma D_{uv}^2 \quad (5.29)$$

$$= G_{uv} + \gamma G_{uw} G_{wv}. \quad (5.30)$$

Otherwise,

$$(G + \gamma G 1_{\{w\}} 1_{\{w\}}^T G - \gamma D_{Ge_w}^2)_{uu} = G_{uu} + \gamma G_{uw} G_{wu} - \gamma D_{uu}^2 \quad (5.31)$$

$$= G_{uu} + \gamma G_{uw} G_{wu} - \gamma (G 1_{\{w\}})^2 \quad (5.32)$$

$$= G_{uu} + \gamma G_{uw} G_{wu} - \gamma G_{uw}^2 \quad (5.33)$$

$$= G_{uu}, \quad (5.34)$$

as claimed. $\square$

Recall that the phase gate on $\mathcal{L}^2(\mathbb{Z}_d)$ is defined as

$$P |x\rangle := \omega^{\frac{x(x-1)}{2}} |x\rangle, \quad (5.35)$$

and put $\tilde{P} := F^{-1} P F$. In particular, we have

$$P X P^{-1} = X Z, \quad P Z P^{-1} = Z \quad (5.36)$$

$$\tilde{P} X \tilde{P}^{-1} = X, \quad \text{and} \quad \tilde{P} Z \tilde{P}^{-1} = Z X^{-1} = \omega^{-1} X^{-1} Z, \quad (5.37)$$

so the phase gates are Clifford operations. This allows us to express local complementation as a unitary acting on $\mathcal{H}^{\otimes V}$:

Proposition 5.7. *Let (G, I, O) be an open $\mathbb{Z}_d$ -graph, $\gamma \in \mathbb{Z}_d$ and $w \in I^c$. Then for any $|\phi\rangle \in \mathcal{H}^{\otimes I}$,*

$$|G \star w(\phi)\rangle = \tilde{P}_w^\gamma \prod_{v \in V} P_v^{-\gamma G_{wv}^2} |G(\phi)\rangle, \quad (5.38)$$

and this map is local-Clifford.

Proof. We first compute the action of $L := \tilde{P}_w^\gamma \prod_{v \in V} P_v^{-\gamma G_{wv}^2}$ on the open graph stabilisers when the input state is assumed to be a stabiliser state. Recall that these take the form

$$X_{1_{\{u\}}} Z_{G 1_{\{u\}}} |G(\phi)\rangle = |G(\phi)\rangle \quad \text{if } u \notin I, \quad (5.39)$$

$$\omega^{-n} X_{1_{\{u\}}} Z_{G 1_{\{u\}}} |G(n : X)\rangle = |G(\phi)\rangle \quad \text{if } u \in I, \quad (5.40)$$

$$\omega^{-n} Z_u |G(n : Z)\rangle = |G(\phi)\rangle \quad \text{if } u \in I. \quad (5.41)$$

Since we have assumed $w \notin I$, we have $u \neq w$ and $LZ_uL^\dagger = Z_u$. Firstly, note that

$$LX_{1_{\{w\}}}Z_{G1_{\{w\}}}L^\dagger = X_{1_{\{w\}}}Z_{G1_{\{w\}}} \quad (5.42)$$

and for $u \in V$ such that $u \neq w$:

$$LX_{1_{\{u\}}}Z_{G1_{\{u\}}}L^\dagger = \omega^{-\gamma G_{uw}}\omega^{-\gamma \frac{G_{uw}(G_{uw}-1)}{2}}X_uZ_u^{-\gamma G_{wu}^2}X_w^{-\gamma G_{uw}}Z_{G1_{\{u\}}} \quad (5.43)$$

$$= \omega^{-\gamma \frac{G_{uw}(G_{uw}+1)}{2}}X_uX_w^{-\gamma G_{uw}}Z_u^{-\gamma G_{wu}^2}Z_{G1_{\{u\}}} \quad (5.44)$$

$$= \omega^{-\gamma \frac{G_{uw}(G_{uw}+1)}{2}}\omega^{\gamma G_{wu}^2}X_w^{-\gamma G_{uw}}Z_u^{-\gamma G_{wu}^2}X_uZ_{G1_{\{u\}}} \quad (5.45)$$

$$= \omega^{\gamma \frac{G_{uw}(G_{uw}-1)}{2}}X_w^{-\gamma G_{uw}}Z_u^{-\gamma G_{wu}^2}X_uZ_{G1_{\{u\}}} \quad (5.46)$$

$$= \omega^{\gamma \frac{G_{uw}(G_{uw}-1)}{2}}X_w^{-\gamma G_{uw}}Z_u^{-\gamma G_{wu}^2}X_uZ_{G1_{\{u\}}} \quad (5.47)$$

$$= \omega^{\gamma \frac{G_{uw}(G_{uw}-1)}{2}}X_w^{-\gamma G_{uw}}\prod_{v \in V}Z_v^{-\gamma G_{wv}G_{wu}}\prod_{v \in V \setminus \{u\}}Z_v^{-\gamma G_{wv}G_{wu}}X_uZ_{G1_{\{u\}}} \quad (5.48)$$

$$= (X_{1_{\{w\}}}Z_{G1_{\{w\}}})^{-\gamma G_{uw}}\prod_{v \in V \setminus \{u\}}Z_v^{-\gamma G_{wv}G_{wu}}X_uZ_{G1_{\{u\}}}. \quad (5.49)$$

Then, applying $LX_{1_{\{w\}}}Z_{G1_{\{w\}}}L^\dagger$ on the left, we have:

$$\prod_{v \in V \setminus \{u\}}Z_v^{-\gamma G_{wv}G_{wu}}X_uZ_{G1_{\{u\}}} = X_{1_{\{u\}}}Z_{(G \star w)1_{\{u\}}}, \quad (5.50)$$

so the image of the stabiliser group of $|G(\phi)\rangle$ under L is the stabiliser group of $|G \star w(\phi)\rangle$ whenever the input ϕ is a stabiliser state. Let $|G(\vec{m})\rangle$ be the graph state obtained from the input state $\bigotimes_{i \in I} |m_i\rangle$, and $|G(\vec{0} : X)\rangle$ be the graph state obtained from the input state $\bigotimes_{i \in I} |0 : X\rangle$. Then it ensues that there are phases $\alpha_{\vec{m}}, \beta \in [0, 2\pi)$ such that

$$L|G(\vec{m} : Z)\rangle = e^{i\alpha_{\vec{m}}}|G \star w(\vec{m})\rangle \quad (5.51)$$

$$L|G(\vec{0} : X)\rangle = e^{i\beta}|G \star w(\vec{0} : X)\rangle, \quad (5.52)$$

by the stabiliser relations above.

Letting $|\psi\rangle \in \mathcal{H}^{\otimes I}$ be an arbitrary input state, we have

$$|0 : X\rangle = \frac{1}{\sqrt{d}} \sum_{\vec{m} \in \mathbb{Z}_d^I} |\vec{m}\rangle, \quad (5.53)$$

so that

$$|G(\vec{0} : X)\rangle = \frac{1}{\sqrt{d^{|I|}}} \sum_{\vec{m} \in \mathbb{Z}_d^I} |G(\vec{m})\rangle. \quad (5.54)$$

In turn,

$$L|G(\vec{0} : X)\rangle = \frac{1}{\sqrt{d^{|I|}}} \sum_{\vec{m} \in \mathbb{Z}_d^I} e^{i\alpha_{\vec{m}}} |G \star^\gamma w(\vec{m})\rangle \quad (5.55)$$

and

$$L|G(\vec{0} : X)\rangle = e^{i\beta} |G \star^\gamma w(\vec{0} : X)\rangle \quad (5.56)$$

$$= e^{i\beta} \frac{1}{\sqrt{d^{|I|}}} \sum_{\vec{m} \in \mathbb{Z}_d^I} |G \star^\gamma w(\vec{m})\rangle \quad (5.57)$$

Since the states $|G \star^\gamma w(\vec{m})\rangle$ are orthogonal, we must therefore have $e^{i\alpha_{\vec{m}}} = e^{i\beta}$ for all $\vec{m} \in \mathbb{Z}_d^{|I|}$. Letting $|\psi\rangle \in \mathcal{H}^{\otimes I}$ be an arbitrary input state, we then have

$$L|G(\psi)\rangle = \frac{1}{\sqrt{d^{|I|}}} \sum_{\vec{m} \in \mathbb{Z}_d^I} c_{\vec{m}} L|G(\vec{m})\rangle \quad (5.58)$$

$$= \frac{1}{\sqrt{d^{|I|}}} \sum_{\vec{m} \in \mathbb{Z}_d^I} c_{\vec{m}} e^{i\beta} |G \star^\gamma w(\vec{m})\rangle \quad (5.59)$$

$$\simeq |G \star^\gamma w(\psi)\rangle, \quad (5.60)$$

as claimed. $\square$

We now use this unitary presentation to show that local complementation preserves the existence of $\mathbb{Z}_d$ -flow for a given open graph, as well as the semantics of the corresponding measurement pattern up to local Cliffords acting on the outputs:

Proposition 5.8. *Suppose the open graph (G, I, O, λ) has a $\mathbb{Z}_d$ -flow given by (C, Λ) . Then, for any $w \in O^c$ and $\gamma \in \mathbb{Z}_d$, $(G \star^\gamma w, I, O, \lambda^{\star w})$ with new labels*

$$\lambda^{\star w}(u) := \begin{cases} \left(C_{ww} - \gamma(GC)_{ww}, (GC)_{ww} \right) & \text{if } u = w; \\ \left(C_{uu}, (GC)_{uu} - \gamma G_{uw}^2 (GC)_{uu} \right) & \text{otherwise;} \end{cases} \quad (5.61)$$

(where we originally had $\lambda(u) = (C_{uu}, (GC)_{uu})$) has a $\mathbb{Z}_d$ -flow $(C^{\star w}, \Lambda)$ defined as

$$C_{uv}^{\star w} := \begin{cases} C_{wv} - \gamma(GC)_{wv} & \text{if } u = w; \\ C_{uv} & \text{otherwise.} \end{cases} \quad (5.62)$$

Let P_O be the (possibly trivial) restriction of the product in equation (5.38) to outputs, and P_j its component acting on vertex $j \in O^c$. Then for any $\mathbf{M} \in \mathcal{M}(\lambda)$, we have

$$P_O \circ \llbracket G \star w, I, O \rrbracket_{\mathbf{M}^{\star w}} = \llbracket G, I, O \rrbracket_{\mathbf{M}}, \quad (5.63)$$

where for any $j \in O^c$, $\mathbf{M}^{\star w}(j) := P_j \mathbf{M}(j) P_j^*$ and is such that $\mathbf{M}^{\star w} \in \mathcal{M}(\lambda^{\star w})$.

Proof. $C^{\star w}$ maintains conditions (ii) and (iii) of the definition of $\mathbb{Z}_d$ -flow since from equation (5.62) we see that it amounts to a sum of columns of C and GC .

Furthermore, if $u \in I$, $C'_{uv} = C_{uv} = 0$, and if $v \in O$, $C_{uv} = 0$ which implies $(GC)_{uv} = \sum_{a \in V} G_{ua} C_{av} = 0$ so that $C'_{uv} = 0$.

We also have

$$\left((G \star w) C' \right)_{uv} = \sum_{a \in V} (G_{ua} + \gamma(Ge_w e_w^T G - D_{Ge_w}^2)_{ua}) C_{av} \quad (5.64)$$

$$- \gamma(G_{uw} + \gamma(Ge_w e_w^T G - D_{Ge_w}^2)_{uw}) (GC)_{wv} \quad (5.65)$$

$$= (GC)_{uv} + \gamma \sum_{a \neq u} G_{wu} G_{wa} C_{av} - \gamma G_{uw} (GC)_{wv} \quad (5.66)$$

$$= (GC)_{uv} - \gamma G_{uw}^2 C_{uv}, \quad (5.67)$$

From this equation we see that $(G \star w) C^{\star w}$ corresponds to a weighted element-wise sum of C and GC , hence also preserves condition (ii) and (iii) of the definition of $\mathbb{Z}_d$ -flow.

Moreover,

$$C'_{uu} = \begin{cases} C_{ww} - \gamma(GC)_{ww} & \text{if } u = w; \\ C_{uu} & \text{otherwise.} \end{cases} \quad (5.68)$$

and

$$\left((G \star w) C' \right)_{uu} = \begin{cases} (GC)_{ww} & \text{if } u = w; \\ (GC)_{uu} - \gamma G_{uw}^2 C_{uu} & \text{otherwise.} \end{cases} \quad (5.69)$$

from which it is clear that we always have C'_{uu} or $((G \star w) C')_{uu}$ different from zero, since the same is true of C_{uu} and $(GC)_{uu}$ by hypothesis.

Finally, we note that equations (5.68) and (5.69) correspond precisely to the image of the corrections $X^{C_u} Z^{(GC)_{uu}}$ under the action of the local complementa-

tion as described in proposition 5.7 and using the identities (5.36)-(5.37). In other words, the local complementation is absorbed into the choice of measurement spaces and unitaries within those new spaces, yielding the new labelling $\lambda^{\star w}(j)$ and choice of measurements $\mathbf{M}^{\star w}(j)$. Applying lemma 5.1 to the definition of $\mathbf{M}^{\star w}$ shows that $\mathbf{M}^{\star w}(j) \in \mathcal{M}(\lambda^{\star w}(j))$ as claimed. However, this is only possible on vertices that are measured, non-outputs, so that the remaining part of equation (5.38) acting on outputs must be tracked explicitly in P_O . $\square$

Locally complementing about an input

For our extraction algorithm, we will also sometimes need to locally complement the open graph about an input. This is forbidden since the unitary representation of local complementation depends on the fact that $\tilde{P}|0 : X\rangle = |0 : X\rangle$. We have to resort to a “trick”, taken from [Bac+21], proposition 4.4: we replace the input vertex by an auxiliary vertex onto which the input state is then teleported. The labelling of the new vertex matches the original labelling of the input (or it is an output if the original input was). For example, in the case of the Z -rotation gadget graph,

$$\text{we replace } \begin{array}{c} \bullet \\ (1,0) \end{array} \text{---} \square \quad \text{with} \quad \begin{array}{c} \text{---} \boxed{F^{-1}} \text{---} \blacksquare \\ (0,1) \\ \diagdown \\ \circ \\ \diagup \\ \bullet \\ (1,0) \end{array}, \quad (5.70)$$

where the new input must be measured in $X \in \mathcal{M}(0,1)$. The additional inverse Fourier gate on the input circuit comes from the fact that the gate teleportation adds a Fourier gate acting on the input, which we need to get rid of: by proposition 4.4, we have

$$\llbracket \text{---} \boxed{F^{-1}} \text{---} \blacksquare \text{---} \circ \rrbracket_X = \text{---} \boxed{F^{-1}} \text{---} \boxed{J(0,0)} \text{---} = \text{---} . \quad (5.71)$$

We can then apply the local complementation about the vertex that has replaced the input. Of course, we need to make sure that the existence of $\mathbb{Z}_d$ -flow and the semantics of the MBQC are preserved by this substitution. Formally, we have:

Proposition 5.9 (Complementing about an input). *Let (G, I, O, λ) be a labelled open $\mathbb{Z}_d$ -graph on the vertex set V with $\mathbb{Z}_d$ -flow, and $w \in I$. Also let (G', I', O, λ')*

be the labelled open graph on the vertex set $V \sqcup \{x\}$ where $I' = (I \sqcup \{x\}) \setminus \{w\}$,

$$G'_{uv} = \begin{cases} 1 & \text{if } u = x, v = w; \\ 1 & \text{if } u = w, v = x; \\ 0 & \text{if } u = x, v \neq w; \\ 0 & \text{if } u \neq w, v = x; \\ G_{uv} & \text{otherwise;} \end{cases} \quad (5.72)$$

and

$$\lambda'(u) = \begin{cases} (0, 1) & \text{if } u = x; \\ \lambda^{\gamma w}(u) & \text{otherwise.} \end{cases} \quad (5.73)$$

Then, (G', I', O, λ') has $\mathbb{Z}_d$ -flow.

Furthermore, for any $\mathbf{M} \in \mathcal{M}(\lambda)$, define $\mathbf{M}' : V' \setminus O \rightarrow U(\mathcal{H})$ as

$$\mathbf{M}'(u) := \begin{cases} X & \text{if } u = x; \\ \mathbf{M}^{\gamma w}(u) & \text{otherwise;} \end{cases} \quad (5.74)$$

then $\mathbf{M}' \in \mathcal{M}(\lambda')$ and

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \llbracket G' \star w, I', O' \rrbracket_{\mathbf{M}'} \circ F_x^{-1}. \quad (5.75)$$

Proof. (G', I', O, λ') can be seen to be the composition of (G, I, O, λ) with the teleportation graph

$$\blacksquare \text{---} \circ, \quad (5.76)$$

along the pair of maps

$$\begin{array}{c} \{\circ\} \longleftarrow \{*\} \longrightarrow I \\ \circ \longleftarrow * \longrightarrow w \end{array}.$$

Then by proposition 4.2, we have

$$\llbracket G', I', O' \rrbracket_{\mathbf{N}} \circ F_x^{-1} = \llbracket G, I, O, \lambda \rrbracket_{\mathbf{M}} \circ \llbracket \blacksquare \text{---} \circ \rrbracket_X \circ F_x^{-1} = \llbracket G, I, O, \lambda \rrbracket_{\mathbf{M}} \quad (5.77)$$

where in the second equality we have used equation (5.71). The equality for the local complementation then follows from proposition 5.8. $\square$

5.2 Quantum circuit extraction subprocesses

In this section, we construct useful subprocesses for the full circuit extraction algorithm, relying extensively on the results of the previous section. Explicitly, we prove the following statements:

1. Edges between output vertices can be pulled into the output circuit part of the diagram as CZ gates.
2. There is a sequence of local Clifford operations which simplifies the graph such that the only measurement labels are $(0, 1)$ or $(1, 0)$. Defining a simplified type of open graph, which we called *reduced* open graphs, we show that these methods can be used to reduce any open graph.
3. We show how to extract any number of vertices in the penultimate layer which are labelled with $(0, 1)$. The collection of such vertices is the set Λ_1^Z mentioned in the introduction.
4. If Λ is the maximally delayed layer decomposition for (G, I, O, λ) , and (G, I, O, λ) is reduced and non-empty, then there are always vertices in the penultimate layer labelled with $(0, 1)$.
5. Isolated vertices in the graph can be discarded without affecting the $\mathbb{Z}_d$ -flow or the semantics of the measurement pattern.

5.2.1 Extracting edges between outputs

In order to make the extraction procedure possible, we first want to simplify the labelled open graph part of the hybrid diagram as much as possible. Firstly, we show that one can simply pull any edges between outputs into the circuit part of the diagram, without changing the $\mathbb{Z}_d$ -flow nor the semantics of the diagram:

Proposition 5.10. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) . Define a new labelled open graph (G', I, O, λ) on the same vertex set by*

$$G'_{uv} := \begin{cases} 0 & \text{if } u, v \in O; \\ G_{uv} & \text{otherwise.} \end{cases} \quad (5.78)$$

Then (G', I, O, λ) has $\mathbb{Z}_d$ -flow (C, Λ) and for any $\mathbf{M} \in \mathcal{M}(\lambda)$,

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \prod_{\substack{(u,v) \in O \\ u \neq v}} E_{u,v}^{G_{uv}} \circ \llbracket G', I, O \rrbracket_{\mathbf{M}}. \quad (5.79)$$

Proof. If $u \neq O$, then $(G'C)_{uv} = \sum_{w \in V} G'_{uw} C_{wu} = \sum_{w \in V} G_{uw} C_{wu} = (GC)_{uv}$. Therefore, $G'C$ only differs from GC in the submatrix $G'C[O, O^c]$, so $G'C$ still all of the conditions for $\mathbb{Z}_d$ -flow (definition 6.5).

The semantics part follows straightforwardly from examining those obtained in theorem 3.2:

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \sqrt{d \times |O^c|} \bigotimes_{u \in O^c} \langle 0 : \mathbf{M}(u) | E_G N_{I^c} \quad (5.80)$$

$$= \sqrt{d \times |O^c|} \bigotimes_{u \in O^c} \langle 0 : \mathbf{M}(u) | \prod_{\substack{(u,v) \in O \\ u \neq v}} E_{u,v}^{G_{uv}} E_{G'} N_{I^c} \quad (5.81)$$

$$= \prod_{\substack{(u,v) \in O \\ u \neq v}} E_{u,v}^{G_{uv}} \sqrt{d \times |O^c|} \bigotimes_{u \in O^c} \langle 0 : \mathbf{M}(u) | E_{G'} N_{I^c} \quad (5.82)$$

$$= \prod_{\substack{(u,v) \in O \\ u \neq v}} E_{u,v}^{G_{uv}} \circ \llbracket G', I, O \rrbracket_{\mathbf{M}}, \quad (5.83)$$

as claimed. $\square$

5.2.2 Removing intermediate measurement spaces

It turns out that it is possible to perform a series of local Clifford transformations on a labelled open graph (G, I, O, λ) which deals with many of the complications evoked in the introduction of the chapter. We are going to map any open graph with $\mathbb{Z}_d$ -flow to the following form, up to local Clifford operations acting on the outputs:

Definition 5.11. *A labelled open $\mathbb{Z}_d$ -graph (G, I, O, λ) is reduced if*

- *there are no edges between outputs, i.e. $G[O, O] = 0$;*
- *the only labels that appear in the graph are $(0, 1)$ or $(1, 0)$, i.e. $\lambda(O^c) \subseteq \{(0, 1), (1, 0)\}$;*
- *there are no adjacent vertices in (G, I, O, λ) which are both labelled $(1, 0)$, i.e. $\lambda(u) = (0, 1) = \lambda(v)$ implies $G_{uv} = 0$;*
- *there are no vertices in (G, I, O, λ) which are labelled $(1, 0)$ and also connected to an output, i.e. $\lambda(u) = (0, 1)$ and $v \in O$ implies $G_{uv} = 0$.*

Then, every labelled open $\mathbb{Z}_d$ -graph with $\mathbb{Z}_d$ -flow is locally equivalent to a reduced labelled open $\mathbb{Z}_d$ -graph which must have $\mathbb{Z}_d$ -flow. Since local Cliffords preserve the semantics, as described in section 5.1:

Proposition 5.12. *If (G, I, O, λ) is a labelled open $\mathbb{Z}_d$ -graph on the vertex set V with $\mathbb{Z}_d$ -flow then there is a reduced open $\mathbb{Z}_d$ -graph (G', I, O, λ') on a vertex set $V' \supseteq V$, such that for any $\mathbf{M} \in \mathcal{M}(\lambda)$, there are $\mathbf{M}' \in \mathcal{M}(\lambda')$, a local Clifford $P : \mathcal{H}^{\otimes O} \rightarrow \mathcal{H}^{\otimes O}$, an array A of CZ gates and an array B of (inverse) Fourier gates and M gates such that*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = P \circ A \circ \llbracket G', I, O \rrbracket_{\mathbf{M}'} \circ B. \quad (5.84)$$

In other words, if D is a hybrid diagram, we can transform it to a diagram D' whose graph part is reduced, by pulling P into the circuit part. Once again, we build up to this statement in multiple smaller steps.

Lemma 5.13. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) . Then it is locally equivalent to an open graph (G', I, O, λ') such that $\lambda'(O^c) \subseteq \{(x, 0), (0, x) \mid x \in \mathbb{Z}_d\}$.*

Proof. Note that local complementation at some vertex $w \in I^c$ only changes the X -coordinate of the measurement space at w and the Z -coordinate of the measurement spaces of the neighbours of w . Pick a random vertex $v \in V$ such that $\lambda(v)_1 \neq 0 \neq \lambda(v)_2$, and apply the local complementation at v with weight $\gamma := \lambda(v)_1 \cdot \lambda(v)_2^{-1}$. The resulting open graph has $\lambda'(v) = (0, \lambda(v)_2)$. Since, as noted above, local complementation does not change the X -coordinate of any other vertex than w , we can repeat this procedure for any vertex in V without reintroducing a non-zero X -coordinate at w . The only vertices for which this is not possible are:

- inputs $i \in I$, since the local complementation rule does not hold at inputs, but these must have $\lambda(i) = (0, \lambda(i)_2)$ by the definition of $\mathbb{Z}_d$ -flow;
- vertices $u \in V$ such that $\lambda(u)_2 = 0$ since then local complementation at u has no effect on the measurement space of u , but then we already have $\lambda(u) = (\lambda(u)_1, 0)$.

Then, at each iteration of this procedure we eliminate a vertex that doesn't verify the condition, and the iteration terminates when the whole graph is labelled according to the statement of the lemma. $\square$

Lemma 5.14. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) . Then it is locally equivalent to open graph (G', I, O, λ') such that $\lambda'(O^c) \subseteq \{(1, 0), (0, 1)\}$.*

Proof. By the preceding lemma, (G, I, O, λ) is locally equivalent to an open graph such that for any $v \in O^c$, $\lambda'(v)$ is either $(\lambda(v)_1, 0)$ or $(0, \lambda(v)_2)$. Note that local scaling at v only changes the measurement space of v and no other vertex in the graph. Then, if we are in the first case, apply a local scaling at v with weight $\lambda(v)_1$, which maps the measurement space of v to $(1, 0)$. In the second case, apply a local scaling with weight $\lambda(v)_2^{-1}$, which maps the measurement space to $(0, 1)$. $\square$

Lemma 5.15. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) , and assume there are vertices $u, v \in V$ such that $G_{uv} \neq 0$ and $\lambda(u) = (x, 0)$ and either $\lambda(v) = (y, 0)$ or $v \in O \setminus I$. Then (G, I, O, λ) is locally equivalent to an open graph (G', I, O, λ') with $\lambda'(u) = (0, 1)$ and $\lambda'(v) = (0, 1)$ if $v \notin O$.*

Proof. Let (u, v) be such a pair of adjacent X -vertices. Then, perform the following sequence of local complementations:

$$\begin{array}{ccccccc} \lambda(u) = (x, 0) & \xrightarrow{\alpha_v} & (x, 1) & \xrightarrow{\beta_u} & (0, 1) & \xrightarrow{\gamma_u} & (0, 1) \\ \lambda(v) = (y, 0) & \xrightarrow{\alpha_v} & (y, 0) & \xrightarrow{\beta_u} & (y, q) & \xrightarrow{\gamma_u} & (0, q), \end{array} \quad (5.85)$$

where $\alpha = -G_{uv}^{-2}y^{-1}$, $\beta = x$ which implies $q = -xyG_{uv}^2$, and $\gamma = yq^{-1} = -x^{-1}G_{uv}^{-2}$.

Finally, use local scaling as in lemma 5.14 to maps both labels to $(0, 1)$.

In the case where $v \in O$, it suffices to perform the first two local complementations, and push the corresponding action on v into the extracted circuit. $\square$

Finally, we need the version of the previous lemma for which the output turns out to also be an input. In this case, we need to use the rule for locally complementation about an input. In particular, we need to add an extra vertex to the graph to make this possible.

Lemma 5.16. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) , and assume there are vertices $u \in V$ and $v \in O \cap I$ such that $G_{uv} \neq 0$ and $\lambda(u) = (x, 0)$. Then there is a reduced open graph (G', I', O, λ') on a vertex set $V \sqcup \{x\}$ with $\lambda'(u) = (0, 1)$, and such that the open graph (G, I, O) embeds into (G', I', O, λ') by the inclusion map of V into $V \sqcup \{x\}$, up to local equivalence.*

Proof. Same as lemma 5.15, except we use the rule for local complementation about an input, proposition 5.9. As a result we have to add a vertex to the graph following that proposition, and pull an inverse Fourier gate into the input circuit. $\square$

Proof of proposition 5.12. Alternate between

1. applying lemmas 5.13 and 5.14 to simplify (G, I, O, λ) to an open graph labelled entirely in $(1, 0), (0, 1)$, pulling local Clifford into the outputs whenever local complementation is used (proposition 5.8) and pulling multipliers into the input circuit whenever local scaling is applied at an input (proposition 5.5);
2. applying lemmas 5.15 to each pair of adjacent $(1, 0)$ -vertices in G (pulling local Cliffords into the output circuit) and 5.16 to any $(1, 0)$ -vertex adjacent to an input (pulling inverse Fourier into the input circuit, proposition 5.9).

Since at each loop we reduce the number of $(1, 0)$ -vertices this must eventually terminate, either because there are no $(1, 0)$ -vertices left or because the connectivity of the graph no longer allows the lemmas to be applied. Finally, use

proposition 5.10 to pull any edges between outputs into the circuit part of the diagram as the array A . The graph part of the resulting diagram is reduced. $\square$

5.2.3 Diagonalising extended $\mathbb{Z}_d$ -flow

We have now reached the core of the algorithm. We show here how to extract vertices in the penultimate layer which are measured in $\mathcal{M}(0, 1)$. The idea used here is very similar to that of triangularisation in the case of simple $\mathbb{Z}_d$ -flow (section 4.3), except here we diagonalise instead.

Proposition 5.17. *Let (G, I, O, λ) be a reduced open graph with $\mathbb{Z}_d$ -flow (C, Λ) , and put $\Lambda_1^Z = \lambda^{-1}(\{(0, 1)\}) \cap \Lambda_1$. Then (G, I, O, λ) is Clifford equivalent to a reduced open graph (G', I, O, λ) such that*

1. *there is a subset $U \subseteq O$ and a perfect matching $\Lambda_1^Z \rightarrow U$ in G' ;*
2. *U is connected only to Λ_1^Z .*

Furthermore, this equivalence is given only by an array of CX gates acting in the outputs of (G, I, O, λ) .

Proof. First let $\Lambda_1^X = \Lambda_1 \setminus \Lambda_1^Z$, which is such that $\lambda(\Lambda_1^X) = \{(0, 1)\}$, and consider the matrix

$$(GC)[V, \Lambda_1^Z] = \begin{pmatrix} (GC)[\Lambda_N, \Lambda_1^Z] \\ \vdots \\ (GC)[\Lambda_2, \Lambda_1^Z] \\ (GC)[\Lambda_1^X, \Lambda_1^Z] \\ (GC)[\Lambda_0, \Lambda_1^Z] \end{pmatrix} = \begin{pmatrix} (GC)[\Lambda_N, \Lambda_1^Z] \\ \vdots \\ (GC)[\Lambda_2, \Lambda_1^Z] \\ (GC)[\Lambda_1^X, \Lambda_1^Z] \\ (GC)[\Lambda_1^Z, \Lambda_1^Z] \\ (GC)[\Lambda_0, \Lambda_1^Z] \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1_{\Lambda_1^Z} \\ A \end{pmatrix}. \quad (5.86)$$

We have that

$$(GC)[\Lambda_k, \Lambda_1^Z] = \sum_j G[\Lambda_k, \Lambda_j] C[\Lambda_j, \Lambda_1^Z], \quad (5.87)$$

$$= G[\Lambda_k, \Lambda_1] C[\Lambda_1, \Lambda_1^Z] + G[\Lambda_k, \Lambda_0] C[\Lambda_0, \Lambda_1^Z], \quad (5.88)$$

$$= G[\Lambda_k, \Lambda_0] C[\Lambda_0, \Lambda_1^Z]. \quad (5.89)$$

Using the first equation, we then have

$$\begin{pmatrix} G[\Lambda_N, \Lambda_0] \\ \vdots \\ G[\Lambda_2, \Lambda_0] \\ G[\Lambda_1^X, \Lambda_0] \\ G[\Lambda_1^Z, \Lambda_0] \\ G[\Lambda_0, \Lambda_0] \end{pmatrix} C[\Lambda_0, \Lambda_1^Z] = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1_{\Lambda_1^Z} \\ A \end{pmatrix}. \quad (5.90)$$

Finally, $A = G[\Lambda_0, \Lambda_0]C[\Lambda_0, \Lambda_1^Z] = 0$ since (G, I, O, λ) is reduced, so that $C[\Lambda_0, \Lambda_1^Z]$ describes a set of column operations on $G[V, \Lambda_0]$ that finds a perfect matching for Λ_1^Z in O . Following section 4.3, these column operations correspond to CX gates acting in the outputs O of (G', I, O) . $\square$

Corollary 5.18. *Under the same hypotheses, for any $\mathbf{M} \in \mathcal{M}(\lambda)$,*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = T \circ \llbracket G', I, O \rrbracket_{\mathbf{M}}, \quad (5.91)$$

where T collects the array of CX gates acting on the outputs.

By pulling the array T of CX gates into the circuit part of the diagram D , we find a perfect matching for the vertices in Λ_1^Z with vertices $U \subseteq O$ which are disconnected from the rest of the graph. In other words, each $u \in \Lambda_1^Z$ now verifies the conditions for proposition 4.4. It follows that

Corollary 5.19. *Under the same hypotheses, for any $\mathbf{M} \in \mathcal{M}(\lambda)$, there is a unique collection choice of $\alpha_u \in [0, 2\pi)$ for each $u \in \Lambda_1^Z$ such that*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = T \circ \prod_{u \in \Lambda_1^Z} J(G_{u\gamma(u)}, \alpha_u)_u \circ \llbracket G[U^c, U^c], I \setminus U, (O \cup \Lambda_1^Z) \setminus U \rrbracket_{\mathbf{M}|_{U^c}}, \quad (5.92)$$

where T collects the array of CX gates acting on the outputs, $\gamma : \Lambda_1^Z \rightarrow U$ is the bijection corresponding to the perfect matching found in the proposition.

Proof. By the discussion above, (G', I, O, λ) is the composition of $(G[U^c, U^c], I \setminus U, (O \cup \Lambda_1^Z) \setminus U, \lambda|_{U^c})$ and the open graph consisting in a collection of parallel gate teleportation graphs (lemma 4.3) along the pair of maps

$$(O \setminus U) \cup \Lambda_1^Z \xleftarrow{\iota} \Lambda_1^Z \xrightarrow{\gamma} U, \quad (5.93)$$

where ι denotes inclusion. The equality on interpretations then follows from corollary 5.18 and (multiple applications of) proposition 4.4. $\square$

5.2.4 Correctness of the extraction algorithm

The final key to the algorithm is a proof that if D is a diagram whose graph part is a reduced open graph with $\mathbb{Z}_d$ -flow, either

1. the graph part is essentially empty and the extraction is complete, or;
2. $\Lambda_1^Z \neq \emptyset$ and we can use the procedures constructed in section 5.2.3 to extract more vertices from the graph part of the diagram into the circuit part.

The algorithm can therefore never reach a “fail” state where it cannot continue. More specifically, if the graph is non-empty, either there is a vertex connected to the outputs and labelled with $(0, 1)$ that can be extracted, or the remaining graph is totally disconnected and can be discarded without changing the semantics of the diagram.

Proposition 5.20. *If (G, I, O, λ) is a reduced open graph and has a maximally delayed $\mathbb{Z}_d$ -flow (C, Λ) , then either $\text{rank } G[\Lambda_1, \Lambda_0] \geq 1$, or all of the non-output vertices are isolated.*

Before proving this however, we need a couple of intermediary lemmas:

Lemma 5.21. *Let (G, I, O, λ) be a open graph with $\mathbb{Z}_d$ -flow (C, Λ) , and assume there is $v \in \Lambda_1$ such that $\lambda(v)_2 \neq 0$. Then, $\text{rank } G[\Lambda_1, \Lambda_0] \geq 1$.*

Proof. We work by contradiction. Assume that $\text{rank } G[\Lambda_1, \Lambda_0] = 0$, then $G[\Lambda_1, \Lambda_0] = 0$. We have that

$$(GC)[\Lambda_1, \Lambda_1] = \sum_k G[\Lambda_1, \Lambda_k] C[\Lambda_k, \Lambda_1] \quad (5.94)$$

$$= G[\Lambda_1, \Lambda_1] C[\Lambda_1, \Lambda_1] + G[\Lambda_1, \Lambda_0] C[\Lambda_0, \Lambda_1], \quad (5.95)$$

from which it follows that $(GC)[\Lambda_1, \Lambda_1] = G[\Lambda_1, \Lambda_1] C[\Lambda_1, \Lambda_1]$. However, $C[\Lambda_1, \Lambda_1]$ is diagonal, thus only rescales columns, but the diagonal elements of $G[\Lambda_1, \Lambda_1]$ are zero since we don't allow loops. This implies that the diagonal elements of $(GC)[\Lambda_1, \Lambda_1]$ are also zero, but we have $\lambda(u) = (GC)_{uu} = (GC)[\Lambda_1, \Lambda_1]_{uu}$ for each $u \in \Lambda_1$, therefore $\lambda(u) = 0$ for all $u \in \Lambda_1$, which is a contradiction. $\square$

Lemma 5.22. *If (G, I, O, λ) is a labelled open graph with $\mathbb{Z}_d$ -flow such that the outputs are disconnected from the rest of the graph, then all of the non-output vertices are isolated.*

Proof. Since (G, I, O, λ) has an $\mathbb{Z}_d$ -flow, it has a maximally delayed $\mathbb{Z}_d$ -flow

(C, Λ) . If the outputs are disconnected from the rest of the graph, we have that

$$(GC)[\Lambda_1, \Lambda_1] = G[\Lambda_1, \Lambda_1]C[\Lambda_1, \Lambda_1] + G[\Lambda_1, \Lambda_0]C[\Lambda_0, \Lambda_1] = G[\Lambda_1, \Lambda_1]C[\Lambda_1, \Lambda_1], \quad (5.96)$$

so that for any $u, v \in \Lambda_1$, $(GC)_{uv} = \sum_{x \in \Lambda_1} G_{ux}C_{xv} = G_{uv}C_{vv}$ since $C[\Lambda_1, \Lambda_1]$ is diagonal. But this implies $GC[\Lambda_1, \Lambda_1] = 0 = G[\Lambda_1, \Lambda_1]$ since $G_{uu} = 0$ and $(GC)_{uv} = 0$ if $u \neq v$. We must therefore also have $C[\Lambda_1, \Lambda_1] = 1_{|\Lambda_1| \times |\Lambda_1|}$. Furthermore, for $k > 1$,

$$(GC)[\Lambda_k, \Lambda_1] = \sum_j G[\Lambda_k, \Lambda_j]C[\Lambda_j, \Lambda_1] = G[\Lambda_k, \Lambda_1]C[\Lambda_1, \Lambda_1] = G[\Lambda_k, \Lambda_1] = 0. \quad (5.97)$$

Then, the vertices in Λ_1 are isolated. A simple induction using lemma 3.16 shows that all the non-output vertices must be isolated. $\square$

Proof of proposition 5.20. By lemma 5.22, we know that if the outputs are disconnected from the rest of the graph, all of the non-output vertices are isolated. By lemma 5.21, we know that $\text{rank } G[\Lambda_1, \Lambda_0] \geq 1$ if even a single vertex in Λ_1 is labelled by $(0, 1)$. Assume this is not the case, and also that the outputs are not disconnected from the rest of the graph.

It follows that all vertices in Λ_1 are labelled by $(1, 0)$, and are not isolated vertices (since those are all in Λ_0 as a conclusion of maximal delay). Pick some $u \in \Lambda_2$, then there is some $v \in \Lambda_1$ such that $C_{vu} \neq 0$ and $G_{uv} \neq 0$ since otherwise the $\mathbb{Z}_d$ -flow is not maximally delayed. It follows that u must be labelled in $(0, 1)$. Furthermore, $(GC)_{uv} = G_{uv}C_{vv} + \sum_{x \in O} G_{ux}C_{xv} = G_{uv} + \sum_{x \in O} G_{ux}C_{xv} = 0$ since $u \prec v$.

Put $\vec{c} \in \mathbb{Z}_d^V$ such that $\vec{c} := C_{\bullet u} - \sum_{v \in \Lambda_1} C_{uv}C_{\bullet v}$. Then,

$$(G\vec{c})_x = \sum_{n \in V} G_{xn}c_n = \sum_{n \in V} G_{xn}C_{nu} - \sum_{n \in V} \sum_{v \in \Lambda_1} C_{uv}G_{xn}C_{nv}. \quad (5.98)$$

$$= (GC)_{xu} - \sum_{n \in \Lambda_1} \sum_{v \in \Lambda_1} C_{uv}G_{xn}C_{nv} - \sum_{n \in O} \sum_{v \in \Lambda_1} C_{uv}G_{xn}C_{nv}. \quad (5.99)$$

$$= (GC)_{xu} - \sum_{v \in \Lambda_1} C_{uv}G_{xv} - \sum_{n \in O} \sum_{v \in \Lambda_1} C_{uv}G_{xn}C_{nv}. \quad (5.100)$$

It follows that

$$(G\vec{c})_u = 1 - \sum_{v \in \Lambda_1} C_{uv}G_{uv} - \sum_{n \in O} \sum_{v \in \Lambda_1} C_{uv}G_{un}C_{nv} \quad (5.101)$$

$$= 1 - \sum_{v \in \Lambda_1} C_{uv}(G_{uv} + \sum_{n \in O} G_{un}C_{nv}) = 1, \quad (5.102)$$

since as stated previously $G_{uv} + \sum_{n \in O} G_{un} C_{nv} = 0$.

If $x \in \Lambda_1$,

$$(G\vec{c})_x = (GC)_{xu} - \sum_{v \in \Lambda_1} C_{uv} G_{xv} - \sum_{n \in O} \sum_{v \in \Lambda_1} C_{uv} G_{xn} C_{nv} \quad (5.103)$$

$$= (GC)_{xu} = \sum_{v \in V} G_{xn} C_{nu} \quad (5.104)$$

$$= \sum_{v \in \Lambda_1} G_{xn} C_{nu} + \sum_{v \in O} G_{xn} C_{nu} = 0, \quad (5.105)$$

since x is connected to no other vertex in either Λ_1 or O .

If $x \notin O \cup \Lambda_1 \cup \{v\}$,

$$(G\vec{c})_x = (GC)_{xu} - \sum_{v \in \Lambda_1} C_{uv} G_{xv} - \sum_{n \in O} \sum_{v \in \Lambda_1} C_{uv} G_{xn} C_{nv} \quad (5.106)$$

$$= (GC)_{xu} - \sum_{v \in \Lambda_1} C_{uv} (G_{xv} + \sum_{n \in O} G_{xn} C_{nv}) \quad (5.107)$$

$$= (GC)_{xu} = 0. \quad (5.108)$$

Finally, we have $c_x = C_{xu} - \sum_{v \in V_1} C_{uv} C_{xv} = C_{xu} - C_{ux} = 0$ if $x \in \Lambda_1$, and $c_u = C_{uu} = 0$. Then, by lemma 3.15, $u \in \Lambda_1$ which is a contradiction. $\square$

Corollary 5.23. *If (G, I, O, λ) is a labelled open graph with $\mathbb{Z}_d$ -flow and $U \subseteq O^c$ is a subset of vertices which is path-disconnected from O , then the vertices in U are isolated.*

Corollary 5.24. *If (G, I, O, λ) is a reduced open graph and has a maximally delayed $\mathbb{Z}_d$ -flow (C, Λ) , then either there is some $u \in \Lambda_1$ such that $\lambda(u) = (0, 1)$ and u is connected to O , or $G = 0$.*

Proof. By the previous lemma there are two possibilities. If the outputs are disconnected from the graph, then all non-outputs are isolated, and since in a reduced open graph, outputs are isolated, the graph is totally disconnected so that $G = 0$.

Otherwise, there is at least one edge between Λ_1 and the outputs. Then, the endpoint of this edge cannot be labelled with $(1, 0)$ because otherwise it would not be lonely, so it must be labelled with $(0, 1)$. $\square$

By corollary 3.19, if (G, I, O, λ) has a $\mathbb{Z}_d$ -flow, it also has a maximally delayed $\mathbb{Z}_d$ -flow. This allows us to use the results of this section for any open graph with $\mathbb{Z}_d$ -flow.

5.2.5 Discarding subgraphs disconnected from the outputs

Since we always extract vertices in the open graph by pulling them through outputs into the output circuit part of a hybrid diagram, we need a way to treat subgraphs of the open graph which are not path connected to the outputs. Luckily, this is easy: just discard those vertices. Here we show that this operation preserves both $\mathbb{Z}_d$ -flow and the semantics (up to a global phase).

Proposition 5.25. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) , and $v \in V$ an isolated vertex. Then, the labelled open graph $(G[\{v\}^c, \{v\}^c], I, O, \lambda|_{\{v\}^c})$ has $\mathbb{Z}_d$ -flow $(C[\{v\}^c, \{v\}^c], \Lambda')$, where $\Lambda' = \{L \setminus \{v\} \mid L \in \Lambda\}$ with the induced order. Furthermore, for any $\mathbf{M} \in \mathcal{M}(\lambda)$,*

$$\llbracket G[\{v\}^c, \{v\}^c], I, O \rrbracket_{\mathbf{M}|_{\{v\}^c}} \simeq \llbracket G, I, O \rrbracket_{\mathbf{M}}. \quad (5.109)$$

Proof. For any $j, k \in V \setminus \{v\}$,

$$(G[\{v\}^c, \{v\}^c]C[\{v\}^c, \{v\}^c])_{jk} = \sum_{u \in \{v\}^c} G_{ju} C_{uk} \quad (5.110)$$

$$= \sum_{u \in V} G_{ju} C_{uk} \quad (5.111)$$

$$= (GC)_{jk}, \quad (5.112)$$

since $G_{vk} = 0$, so discarding v clearly preserves the $\mathbb{Z}_d$ -flow.

The semantics part follows from

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} = \sqrt{d \times |O^c|} \bigotimes_{u \in O^c} \langle 0 : \mathbf{M}(u) | E_G N_{I^c} \quad (5.113)$$

$$= \langle 0 : \mathbf{M}(v) | 0 : X \rangle \sqrt{d \times |O^c|} \bigotimes_{u \in O^c \setminus \{v\}} \langle 0 : \mathbf{M}(u) | E_G N_{I^c \setminus \{v\}} \quad (5.114)$$

$$= e^{i\alpha} \sqrt{d \times (|O^c| - 1)} \bigotimes_{u \in O^c \setminus \{v\}} \langle 0 : \mathbf{M}(u) | E_G N_{I^c \setminus \{v\}} \quad (5.115)$$

$$\simeq \llbracket G[\{v\}^c, \{v\}^c], I, O \rrbracket_{\mathbf{M}|_{\{v\}^c}}, \quad (5.116)$$

where we have used the fact that $\langle 0 : \mathbf{M}(v) | 0 : X \rangle = \frac{e^{i\alpha}}{\sqrt{d}}$ for some $\alpha \in [0, 2\pi)$, otherwise the pattern is not uniformly deterministic. $\square$

Corollary 5.26. *Let (G, I, O, λ) be a labelled open graph with $\mathbb{Z}_d$ -flow (C, Λ) and $K \subseteq O^c$ a subset of vertices which is path-disconnected from O . Then, the labelled open graph $(G[K^c, K^c], I, O, \lambda|_{K^c})$ has $\mathbb{Z}_d$ -flow $(C[K^c, K^c], \Lambda')$, where $\Lambda' = \{L \setminus K \mid L \in \Lambda\}$ with the induced order. Furthermore, for any $\mathbf{M} \in \mathcal{M}(\lambda)$,*

$$\llbracket G[K^c, K^c], I, O \rrbracket_{\mathbf{M}|_{K^c}} \simeq \llbracket G, I, O \rrbracket_{\mathbf{M}}. \quad (5.117)$$

Proof. By corollary 5.23, the vertices in K must be isolated in G . Then, the corollary follows from a simple induction using proposition 5.25. $\square$

5.3 The extraction algorithm

We are now ready to describe the algorithm for extracting a reversible quantum circuit from any open graph with $\mathbb{Z}_d$ -flow.

Let D be a diagram whose graph part (G, I, O, λ) has $\mathbb{Z}_d$ -flow.

Step 0: Find the maximal subgraph of G which is connected to O and discard the rest of the graph (an operation which preserves the semantics up to a global phase, by corollary 5.26).

Step 1: If the graph part of the diagram contains no non-outputs, then each output is connected to an output wire and at most one input wire. Delete the output vertices, connect the inputs to the corresponding output wires, and initialise any $u \in I^c \cap O$ in the auxiliary state $|0 : X\rangle$. Then, return the resulting quantum circuit. If the graph part of the diagram contains any non-outputs, go on to step 2.

Step 2: Firstly, reduce the open graph using proposition 5.12, pulling the resulting local-Clifford operation P into the input circuit part of the diagram, the Fourier and multipliers on inputs into the input circuit part of the diagram, and update the choice of measurements $\mathbf{M}$ following propositions 5.5, 5.8 and 5.9. Then use the algorithm of section 3.3 to find a maximally delayed $\mathbb{Z}_d$ -flow (C, Λ) for the resulting open graph (G', I, O, λ') .

Step 3: Find Λ_1^Z , and use proposition 5.17 to diagonalise the submatrix $G[\Lambda_1^Z, O]$ by pulling the corresponding array T of CX gates into the circuit part of the diagram (corollary 5.18).

Step 4: Extract Λ_1^Z using proposition 5.19, and pull the resulting unitary into the circuit part of the diagram. Return to step 1.

Every step takes a number of elementary operations which is polynomial in the size of the graph $|V|$, therefore the total algorithm runs in time polynomial in $|V|$.

Theorem 5.27. *Let (G, I, O, λ) be an open graph with $\mathbb{Z}_d$ -flow. Then, for any $\mathbf{M} \in \mathcal{M}(\lambda)$,*

$$\llbracket G, I, O \rrbracket_{\mathbf{M}} |\psi\rangle \simeq \prod_{k=1}^N \left(P^{(k)} A^{(k)} T^{(k)} U^{(k)} (\mathbf{M}^{(k)}) B^{(k)} \right) (|\psi\rangle \otimes_{j \in I \cap O^{(N)}} |0 : X\rangle), \quad (5.118)$$

where $P^{(k)}$ and $A^{(k)}$ are the unitaries pulled into the output circuit part of the diagram in the k -th loop of the algorithm at steps 2, $T^{(k)}$ at step 3, and $U^{(k)}$ at step 4. $B^{(k)}$ is the array of inverse Fourier gates pulled into the input circuit part of

the diagram if any local complementation around inputs need to be applied when reducing the open graph. N corresponds to the number of loops the algorithm makes before terminating. The angles in the unitary circuit $U^{(k)}$ depend on the choice of measurements $\mathbf{M}^{(k)}$ for the vertices in Λ_1^Z at loop k .

Proof. The only point at which the algorithm can fail is at step 3 if Λ_1^Z is empty. Since after step 2 the graph part of the diagram is reduced, by corollary 5.24 there are only 2 possibilities. If Λ_Z^1 is empty then $G = 0$, so that the graph part would have been discarded in step 0 and the algorithm would have terminated at step 1. Otherwise, Λ_Z^1 is non-empty and the algorithm proceeds.

Let n be the number of vertices in the graph and m the number of vertices labelled with $(1, 0)$. In any given loop, at step 2 we reduce the number m if it is non-zero, and increase the number n by at most m (once for every time we might need to apply proposition 5.9 about an input). Eventually, we reach a state $(0, n')$, where n' might be greater than at the first iteration. However, at this point, there are no vertices labelled $(1, 0)$ so we no longer need to apply any local complementations, and the number n' of vertices only reduces in further iterations. It follows that on any given loop we reduce (m, n) in the alphabetical order, so the algorithm must terminate since we eventually reach state $(0, 0)$ in step 1 after removing all of the outputs. N is therefore finite. $\square$

5.4 Some worked out examples

We conclude this chapter with a few examples of the circuit extraction algorithm applied to some examples. We start with the phase-gate graph and the total graph which were presented as particularly pathological examples in the introduction.

5.4.1 The Z -rotation gadget

Recall that the Z -rotation gadget graph is given by

$$\begin{array}{c} \bullet \\ (1, 0) \end{array} \text{---} \square \quad . \quad (5.119)$$

This graph is not reduced, so the first step of the algorithm is to apply proposition 5.12 to obtain a reduced open graph. In this case, we have an X -vertex which is connected to an output. To eliminate this vertex, we need to locally complement about the output. This is also an input, so we need to extend the graph as per

proposition 5.9:

$$\left[\begin{array}{c} \bullet \\ (1,0) \end{array} \square \right]_M \stackrel{\text{PROP 5.9}}{=} \left[\begin{array}{c} \square F^{-1} (0,1) \\ (1,0) \bullet \end{array} \right]_{M'} \quad (5.120)$$

$$\stackrel{-1 \star 3}{=} \left[\begin{array}{c} \square F^{-1} (0,1) \\ (1,1) \bullet \end{array} \begin{array}{c} \square \\ \tilde{P}^{-1} \end{array} \right]_{M''} \quad (5.121)$$

$$\stackrel{1 \star 2}{=} \left[\begin{array}{c} \square F^{-1} (0,1) \\ (0,1) \bullet \end{array} \begin{array}{c} \square \\ \tilde{P}^{-1} \end{array} \right]_{M'''} \quad (5.122)$$

At this point we recognise the sequential gate teleportation graph of section 4.1, so that for any choice of measurement $M \in \mathcal{M}(1,0)$,

$$\left[\begin{array}{c} \bullet \\ (1,0) \end{array} \square \right]_M = \square F^{-1} \square J(-1,0) \square J(0,\alpha) \square P^{-1} \square \tilde{P}^{-1} \square \quad (5.123)$$

From this example, it is clear that the extraction algorithm sometimes outputs circuits that are very much not optimal. Rewriting the leftmost J gate to its components, we get

$$\begin{aligned} & \square F^{-1} \square J(-1,0) \square J(0,\alpha) \square P^{-1} \square \tilde{P}^{-1} \square \\ &= \square F^{-1} \square R_Z(0) \square F \square M(-1) \square J(0,\alpha) \square P^{-1} \square \tilde{P}^{-1} \square \\ &= \square M(-1) \square J(0,\alpha) \square P^{-1} \square \tilde{P}^{-1} \square \end{aligned} \quad (5.124)$$

But even this is still not optimal. Because we know this open graph to correspond to a Z -rotation gadget, there is some $\alpha' \in [0, 2\pi)^{d-1}$ such that

$$\left[\begin{array}{c} \bullet \\ (1,0) \end{array} \square \right]_M = \square R_Z(\alpha') \square \quad (5.125)$$

We leave fixing these issues for future work.

5.4.2 The total graph

Next, we consider the case of the total graph on 4 vertices that was given in the introduction:

$$\begin{array}{c}
 (1, -1) \\
 \bullet \\
 (1, -1) \bullet \quad \bullet \\
 \bullet \\
 (1, -1)
 \end{array}
 \quad . \quad (5.126)$$

As was explained, while it has $\mathbb{Z}_d$ -flow, this open graph is particularly pathological from the point of view of the algorithm of the previous chapter. While we can extract at most one gate at a time through the output (since they must be totally ordered in the resulting circuit on one wire), every non-output is connected to the sole output. There is therefore no clear ordering for extraction.

As before, this graph is not reduced. The graph is connected, and we don't terminate at step 1 so the first real step of the algorithm is to transform it to an equivalent reduced open graph. This can be done (non-uniquely) by locally complementing about any of the non-outputs with weight 1. We get the equality of diagrams, for any $\mathbf{M} \in \mathcal{M}(\lambda)$:

$$\left[\begin{array}{c} (1, -1) \\ \bullet \\ (1, -1) \bullet \quad \bullet \\ \bullet \\ (1, -1) \end{array} \right]_{\mathbf{M}} = \left[\begin{array}{c} (0, 1) \\ \bullet \\ -1 \quad -1 \\ \bullet \quad \bullet \\ (1, 0) \quad (1, 0) \end{array} \right]_{\mathbf{M}'} \quad , \quad (5.127)$$

and we can extract the first vertex:

$$\left[\begin{array}{c} (1, -1) \\ \bullet \\ (1, -1) \bullet \quad \bullet \\ \bullet \\ (1, -1) \end{array} \right]_{\mathbf{M}} = \left[\begin{array}{c} (1, 0) \\ \bullet \\ -1 \quad -1 \\ \bullet \quad \bullet \\ (1, 0) \end{array} \right]_{\mathbf{M}'|_{2,3}} \quad , \quad (5.128)$$

where the angle α_1 depends on the measurement $\mathbf{M}'(1)$ which is obtained as $M(-1)\tilde{P}^{-1}\mathbf{M}(1)\tilde{P}M(-1)$.

Then, the graph part is once again not reduced. At step 2 of the algorithm, we therefore reduce the graph part: denoting o the output and once again ordering

the non-outputs 2, 3 from top to bottom,

$$\left[\begin{array}{c} (1,0) \\ \bullet \\ -1 \\ \bullet \\ (1,0) \end{array} \right] \xrightarrow{-1} J(-1, \alpha_1) \xrightarrow{P^{-1}} \left[\right]_{M'|_{2,3}} \quad (5.129)$$

$$\stackrel{-1}{\star o} \left[\begin{array}{c} (1,1) \\ \bullet \\ -1 \\ \bullet \\ (1,1) \end{array} \right] \xrightarrow{-1} \tilde{P}^{-1} \xrightarrow{J(-1, \alpha_1)} \xrightarrow{P^{-1}} \left[\right]_{(M')^{-1} o} \quad , \quad (5.130)$$

$$\stackrel{1}{\star 2} \left[\begin{array}{c} (0,1) \\ \bullet \\ -1 \\ \bullet \\ (1,1) \end{array} \right] \xrightarrow{-1} \xrightarrow{P^{-1}} \tilde{P}^{-1} \xrightarrow{J(-1, \alpha_1)} \xrightarrow{P^{-1}} \left[\right]_{((M')^{-1} o)^{1} 1} \quad , \quad (5.131)$$

$$\stackrel{1}{\star 3} \left[\begin{array}{c} (0,1) \\ \bullet \\ -1 \\ \bullet \\ (0,1) \end{array} \right] \xrightarrow{-1} \xrightarrow{P^{-1}} \tilde{P}^{-1} \xrightarrow{J(-1, \alpha_1)} \xrightarrow{P^{-1}} \left[\right]_{M''} \quad , \quad (5.132)$$

Then, we once again recognise the sequential teleportation graph, which we can extract in one step:

$$\left[\begin{array}{c} (1,-1) \\ \bullet \\ (1,-1) \\ \bullet \\ (1,-1) \end{array} \right]_{\mathbf{M}} = |0 : X\rangle \xrightarrow{J(-1, \alpha_3)} \xrightarrow{J(-1, \alpha_2)} \xrightarrow{P^{-1}} \tilde{P}^{-1} \xrightarrow{J(-1, \alpha_1)} \xrightarrow{P^{-1}} . \quad (5.133)$$

Conclusion and outlook

We have presented an algorithm for extracting unitary quantum circuits from any open $\mathbb{Z}_d$ -graph with $\mathbb{Z}_d$ -flow. This extends the results of chapter 4 to allow for all measurement spaces.

As we saw in section 5.4.1, the circuits found by the algorithm can be very sub-optimal. We leave improving this aspect to future work. Recent work has shown how to extract circuits from open $\mathbb{Z}_2$ -graphs with extended Pauli $\mathbb{Z}_2$ -flow, and with a simpler method [Sim21]. Possibly this technique can be extended to cover the case of arbitrary prime dimension as well.

Finally, the original work on which this chapter draws a lot of inspiration, [Bac+21], was concerned with extracting circuits from ZX-diagrams with graph-like properties [Dun+20]. The ZX-calculus [van20] has been extended to the case of qudits (of arbitrary dimension) [Wan21], and it would be interesting to see how much of our work can be adapted to that setting.

CONVERGENCE IN CONTINUOUS VARIABLE MEASUREMENT-BASED QUANTUM COMPUTATION

The final research chapter of this thesis is concerned with the following question: how much of the preceding work on qudits can be extended beyond the finite-dimensional setting? We offer only a partial answer, for two reasons. Firstly, we shall only consider the case of MBQC in the model of continuous variable quantum computation proposed by Lloyd and Braunstein [LB99]. Secondly, the results in this section were actually obtained mostly before the qudit case was considered [Boo+21]. While it is clear, given the results of chapter 3, how to construct measurement spaces for CV-MBQC, we only allow measurements in a single space, as in chapter 4. The details of the full construction have yet to be formally derived.

The main complication here is that the gate teleportation protocol does not carry over from the finite-dimensional case. Rather, the best one can expect is an approximation to the gate teleportation, where the auxiliary state is replaced by a *squeezed state*. Then, the main concerns are questions of convergence when the approximation is sent to its ideal limit: is the gate teleportation appropriately recovered? And how does this approximation hold up when one tries to run more complicated MBQC protocols than a simple gate teleportation? As a result, this

This chapter is based on our article, [BM21], and the work was presented at the 18th International Conference on Quantum Physics and Logic.

chapter has a substantially more analytic flavour than the previous ones.

Section 6.1 presents the standard model of continuous-variable quantum computation as well as the Wigner transform for CV states. The Wigner function often proves useful for making calculations in the CV setting which we will use extensively in proofs. Then, in section 6.2, we explicit the CV gate teleportation protocol, and prove that, in the ideal limit, it converges (in the strong sense) to the expected unitary. Section 6.3 introduces CV-MBQC and $\mathbb{R}$ -flow, which is the straightforward generalisation of simple $\mathbb{Z}_d$ -flow to continuous variables. Finally, section 6.4 treats the question of convergence for MBQCs with simple $\mathbb{R}$ -flow, by adapting the circuit extraction algorithm of chapter 4.

6.1 Preliminaries

Before diving into the heart of the matter, we need to introduce the computational model and some useful tools. In CV quantum computation, the basic building block is the *qumode*¹, a complex, countably infinite-dimensional, separable Hilbert space $\mathcal{H} = \mathcal{L}^2(\mathbb{R})$ which takes the place of the qudit. As described in chapter 1, $\mathcal{H}$ is a space of square-integrable complex-valued functions: an element $\phi \in \mathcal{H}$ is represented by a function $\mathbb{R} \rightarrow \mathbb{C}$ such that

$$\int_{x \in \mathbb{R}} |\phi(x)|^2 < \infty, \quad (6.1)$$

and where the Hilbert inner product is

$$\langle \psi, \phi \rangle := \int_{x \in \mathbb{R}} \overline{\psi(x)} \phi(x), \quad (6.2)$$

with corresponding norm $\|\psi\| := \sqrt{\langle \psi, \psi \rangle}$.

Each qumode is equipped with a pair of unbounded linear position and momentum operators Q and P , which are defined on the dense subspace $\mathcal{S}(\mathbb{R}) \subseteq \mathcal{H}$ of *Schwartz functions* [Sch50; Lig58], along with any real polynomial thereof, by:

$$\text{for any } \phi \in \mathcal{S}(\mathbb{R}), \quad Q\phi(x) := x\phi(x) \quad \text{and} \quad P\phi(x) := -i \frac{d\phi(x)}{dx}. \quad (6.3)$$

$\mathcal{S}(\mathbb{R})$ forms a common, dense domain for any polynomial of Q and P such that they are all self-adjoint (see section 1.1.2). From these, the functional calculus (theorem 1.16) is used to define the corresponding translation operators (continuously extended to all $\mathcal{H}$):

$$\text{for any } s \in \mathbb{R}, \quad X(s) := \exp(-isP) \quad \text{and} \quad Z(s) := \exp(isQ). \quad (6.4)$$

¹This terminology comes from quantum optics, where we can identify each quantisation mode of the quantum electromagnetic field with a space $\mathcal{L}^2(\mathbb{R})$ [FT20].

Then, $X(s)f(x) = f(x - s)$, $X^*(s) = X(-s)$ and $Z^*(s) = Z(-s)$ so that

$$X(-s)QX(s) = Q + sI; \quad (6.5)$$

$$Z(-s)PZ(s) = P + sI. \quad (6.6)$$

Hopefully, it is clear that these operators are an analogue of the Pauli group in CV. In fact, all four of these operators are defined by the exponential Weyl commutation relations (up to unitary equivalence, by the Stone-von Neumann theorem, see [Hal13], chapter 14):

$$\text{for any } s, t \in \mathbb{R}, \quad X(s)Z(t) = e^{-ist}Z(t)X(s), \quad (6.7)$$

which generalise the canonical commutation relations, and further related by the Fourier transform operator $F = \exp\left(i\frac{\pi}{4}(Q^2 + P^2)\right)$:

$$F^*QF = P \quad \text{and} \quad F^*PF = -Q. \quad (6.8)$$

The multiplier, defined in equation 2.4, also generalises to this setting, although it is conventionally called the *squeeze operator*: for any real number $\eta > 0$, called the *squeezing factor*,

$$S(\eta) := \exp\left(-i \ln(\eta)(QP + PQ)\right). \quad (6.9)$$

Then $S(\eta)\psi(x) = \sqrt{\eta^{-1}}\psi(\eta^{-1}x)$ so that:

$$S(\eta)^*QS(\eta) = \eta Q, \quad S(\eta)^*PS(\eta) = \eta^{-1}P \quad (6.10)$$

$$S(\eta)^*Z(s)S(\eta) = Z(\eta s), \quad S(\eta)^*X(s)S(\eta) = X(\eta^{-1}s). \quad (6.11)$$

Following Lloyd and Braunstein [LB99; Bv05], the state of a register V of qumodes can be used to encode information and perform computations just as one would with a register of qudits. We use the gates from the set of unitaries

$$\left\{F, \exp(isQ_j), \exp(isQ_j^2), \exp(isQ_j^3), \exp(isQ_jQ_k) \mid s \in \mathbb{R}, j, k \in V\right\}, \quad (6.12)$$

also defined using the functional calculus. As described in section 1.1.4, the indices j, k indicate on which subsystems in the total tensor product $\mathcal{H}^{\otimes N}$ the operators act. For brevity and by analogy with the qudit case, we write:

$$CZ_{j,k}(s) := \exp(isQ_jQ_k), \quad (6.13)$$

$$CX_{j,k}(s) := \exp(-isQ_jP_k) = F_k CZ_{j,k}(s) F_k^*, \quad (6.14)$$

$$U(\alpha, \beta, \gamma) := \exp(i\alpha Q) \exp(i\beta Q^2) \exp(i\gamma Q^3). \quad (6.15)$$

In the circuit representation, the parameters of these controlled unitaries are once again represented as edge weights:

$$CZ(w) = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \bullet \text{---} \\ w \end{array} \quad \text{and} \quad CX(w) = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \oplus \text{---} \\ w \end{array} . \quad (6.16)$$

This model of computation is strong enough to encode qubit quantum computation [GKP01], and is universal in the sense that any “physical” unitary can be approximated by combinations of applications of (6.13) - (6.15) [LB99].

The Wigner function

Before diving into MBQC, we present one last tool. The Wigner function is a phase-space quasi-probability distribution which uniquely represents the state of a quantum system with Hilbert space $\mathcal{L}^2(\mathbb{R})$. We briefly review the Wigner formulation [CG69; de 06; de 17; de 18]. In fact, we do not need the full phase space picture: it is sufficient for our purposes to understand how to represent states. While it has many interesting properties from the standpoint of quantum theory, we chose not to present them as we essentially use the Wigner function as a functional representation of density operators to be used for calculations.

In the phase space formalism, to each density operator $\rho \in \mathfrak{D}(\mathcal{H}^{\otimes N})$ (where $N \in \mathbb{N}$) such that $\rho = \sum_j c_j P_{\psi_j}$ (see proposition 1.20), we associate a *real-valued* square-integrable function W_ρ in a Hilbert space $\mathcal{L}^2(\mathbb{R}^N \times \mathbb{R}^N, \mathbb{R})$, called the *Wigner function* of ρ :

$$W_\rho(x, y) := \frac{1}{(2\pi)^N} \sum_j c_j \int_{\mathbb{R}^N} \int_{\mathbb{R}^N} \overline{\psi_j(q - \frac{1}{2}y)} \psi_j(q + \frac{1}{2}y) e^{2ip \cdot y} dq dp . \quad (6.17)$$

It is clear that this association is $\mathbb{R}$ -linear, $W_{\rho+\lambda\sigma} = W_\rho + \lambda W_\sigma$. The norm is given by

$$\|W_\rho\| := \sqrt{\int_{\mathbb{R}^N} \int_{\mathbb{R}^N} W_\rho(x, y)^2 dq dp}, \quad (6.18)$$

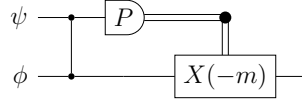
which agrees with the Hilbert-Schmidt norm on $\mathfrak{D}(\mathcal{H})$, $\|W_\rho\|^2 = \text{tr}(\rho^2)$.

6.2 The gate teleportation protocol

Just as for qudits, the core of continuous-variable MBQC is gate teleportation. However, the qudit gate teleportation protocol does not carry over identically to continuous variables. This comes down mainly to the following fact: the key property of the auxiliary state used in the qudit case is that it is a fixed point for the X operator: $X|0 : X\rangle = |0 : X\rangle$. In CV, neither the momentum operator P

nor the translation operation $X(s)$ admit any eigenvectors. For no $s \in \mathbb{R} \setminus \{0\}$ does there exist a non-zero $\phi \in \mathcal{H}$ for which $X(s)\phi = \phi$ holds. Such a vector would be an s -periodic function, and therefore could never satisfy equation (6.1).

We therefore need to find a replacement for this auxiliary state. But even this is ill-fated: there is in fact no state $\phi \in \mathcal{H}$ at all such that for all $\psi \in \mathcal{H}$, the circuit



outputs the state $F\psi$. As a result, the best we can hope for is an approximation to the “ideal” auxiliary state. The gate teleportation circuit is then only an approximation to the gate teleportation, which should converge to the desired unitary in the ideal limit of the approximation.

Such an approximation is given by the following net² of Gaussian states. Let g_1 be an $\mathcal{L}^2$ -normalised Gaussian distribution on $\mathbb{R}$ given by

$$g_1(x) := \frac{1}{\sqrt[4]{2\pi}} e^{-\frac{x^2}{2}}, \quad (6.19)$$

and put $g_\eta = S(\eta)g_1$. In other words,

$$g_\eta(x) = \frac{1}{\sqrt[4]{2\pi\eta^2}} e^{-\frac{x^2}{2\eta^2}}. \quad (6.20)$$

Such a state is called a *squeezed state*, in part because of its Wigner function which appears spatially squeezed along the momentum axis:

Proposition 6.1. *The Wigner function of g_η is given by $Wg_\eta(x, y) = G_\eta(x)G_{1/\eta}(y)$, where*

$$G_\eta(x) := \frac{1}{\sqrt{\pi\eta^2}} e^{-\frac{x^2}{\eta^2}} = g_\eta(x)^2. \quad (6.21)$$

Proof.

$$Wg_\eta(x, y) = \int_{q \in \mathbb{R}} e^{-iqy} g_\eta(x + \frac{q}{2}) g_\eta(x - \frac{q}{2}) \quad (6.22)$$

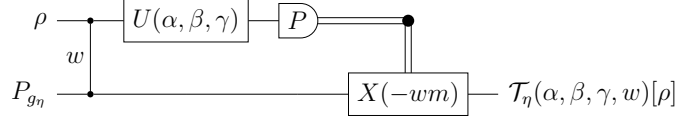
$$= \frac{1}{\sqrt{\pi\eta^2}} \int_{q \in \mathbb{R}} e^{-iqy} e^{-\frac{(x+\frac{q}{2})^2}{2\eta^2}} e^{-\frac{(x-\frac{q}{2})^2}{2\eta^2}} \quad (6.23)$$

$$= \frac{1}{\sqrt{\pi\eta^2}} e^{-\frac{x^2}{\eta^2}} \int_{q \in \mathbb{R}} e^{-iqy} e^{-\frac{q^2}{4\eta^2}} \quad (6.24)$$

²A net is a sort of generalised sequence, where the index set $\mathbb{N}$ is replaced by a directed set. Here we only need to consider the positive real numbers $\mathbb{R}_+^*$ with their usual order.

$$\begin{aligned}
 &= \frac{1}{\sqrt{\pi\eta^2}} e^{-\frac{x^2}{\eta^2}} \cdot \sqrt{\pi\eta^2} e^{-\eta^2 y^2} \\
 &= G_\eta(x) G_{\frac{1}{\eta}}(y). \quad \square
 \end{aligned} \tag{6.25}$$

The desired approximation to the gate teleportation protocol can then be obtained by the following quantum circuit, parameterised by a squeezing factor η :



where P_{g_η} is the pure density operator associated to g_η and $\mathcal{T}_\eta(\alpha, \beta, \gamma, w)$ is the quantum channel described by the circuit. An analytic form for the output state of this quantum circuit, ignoring the CZ weight and unitary $U(\alpha, \beta, \gamma)$, was obtained by Gu et al. [Gu+09], in terms of the Wigner function of ρ as

$$W_{\mathcal{T}_\eta(\alpha, \beta, \gamma, w)[\rho]}(x, y) = \int_{q \in \mathbb{R}} G_\eta(x - q) W_\rho(q, y), \tag{6.26}$$

i.e. convolution with respect to the first variable. They never explicitly consider the convergence question as $\eta \rightarrow \infty$, called the *infinite squeezing limit*. While it is clear that the net $(g_\eta)_{\eta \geq 1}$ can have no limit in $\mathcal{H}$ as $\eta \rightarrow +\infty$, somewhat surprisingly, for any $\rho \in \mathfrak{D}(\mathcal{H})$, $\mathcal{T}_\eta(\alpha, \beta, \gamma, w)[\rho]$ does converge to a state in $\mathfrak{D}(\mathcal{H})$.

Proposition 6.2 (Gate teleportation convergence). *For any $\alpha, \beta, \gamma, w \in \mathbb{R}$ and any $\rho \in \mathfrak{D}(\mathcal{H})$,*

$$\lim_{\eta \rightarrow +\infty} \mathcal{T}_\eta(\alpha, \beta, \gamma, w)[\rho] = \Gamma_{S(w)FU(\alpha, \beta, \gamma)}[\rho], \tag{6.27}$$

where Γ_U is the unitary channel given by conjugation by U .

In other words, the quantum channel $\mathcal{T}_\eta(\alpha, \beta, \gamma, w)$ converges to $\Gamma_{S(w)FU(\alpha, \beta, \gamma)}$ in the *strong topology* on the set $\mathfrak{C}_{\leq 1}(\mathcal{H})$ of quantum operations. In general the usual topology on the set of quantum operations is inappropriate for considering the approximation of arbitrary quantum operations in infinite-dimensional Hilbert spaces [SH08; Wil18; PLB18]. The net $(\mathcal{T}_\eta(\alpha, \beta, \gamma, w))_{\eta \geq 1}$ can be viewed as a pointwise approximation to the unitary channel $\Gamma_{S(w)FU(\alpha, \beta, \gamma)}$.

The question of convergence in the infinite squeezing limit has been considered for some slightly different but related protocols, such as the convergence of the quantum state teleportation protocol of [Wil18; SW20].³ Their result does not immediately apply in our case, but we use some of their ideas as well as some standard results of functional analysis in formulating our proof:

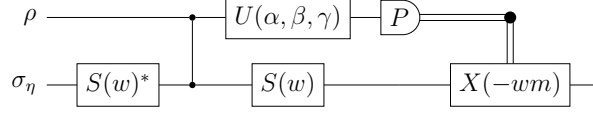
³The quantum state teleportation should not be confused with the gate teleportation we use here. The state teleportation involves three qumodes: an initial qumode is teleported using an auxiliary two qumode state and entangling two-qumode measurement. In contrast, the gate teleportation only uses two qumodes.

Proof. We first note that we can ignore the parameter w for the $CZ(w)$ gate: we know that

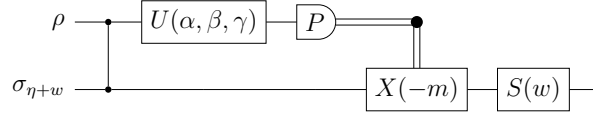
$$CZ(w) = \exp(iwQ_1Q_2) = \exp(iQ_1wQ_2) = \exp(iQ_1S_2(w)Q_2S_2(w)^*) \quad (6.28)$$

$$= S_2(w) \exp(iQ_1Q_2) S_2(w)^* = S_2(w) CZ(1) S_2(w)^*. \quad (6.29)$$

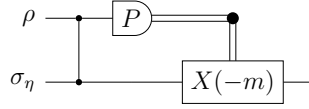
Thus, the teleportation circuit is equivalent to



and, commuting the correction with the squeezing operator, to



The additional squeezing w in the auxiliary state will be absorbed into the limit, and the final $S(w)$ gate can be added at the end since it comes after the teleportation (it is unitary thus continuous and preserves limits). Since the “change of basis” unitary $U(\alpha, \beta, \gamma)$ commutes with the CZ gate, it can be absorbed into the input state which is arbitrary by hypothesis. We have therefore reduced the problem to proving convergence of the simpler circuit:



for an arbitrary input $\rho \in \mathfrak{D}(\mathcal{H})$. From [Gu+09] we know that the output of this circuit is

$$W_{\mathcal{T}_\eta[\rho]}(x, y) = \int_{q \in \mathbb{R}} G_\eta(x - q) W_\rho(q, y) = W_{F\rho F^*} *_1 g_{\frac{1}{\eta}}(x, y), \quad (6.30)$$

where $*_1$ indicates convolution with respect to the first variable. We need to bound the trace distance $\|\mathcal{T}_\eta[\rho] - F\rho F^*\|$. By [AU00; HQ12] we know that for any $\rho, \sigma \in D(\mathcal{H})$,

$$\|\rho - \sigma\| \leq \sqrt{1 - F(\rho, \sigma)}, \quad (6.31)$$

where F is the Uhlmann fidelity [Uhl76] which can be calculated for pure states as

$$F(\rho, \sigma) = \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} W_\rho(q, p) W_\sigma(q, p). \quad (6.32)$$

Assume ρ is a pure state, and furthermore that it is the density operator of $\psi \in \mathcal{L}^1(\mathbb{R}) \cap \mathcal{L}^2(\mathbb{R})$, i.e. the projector P_ψ onto the one-dimensional subspace generated by ψ . Then we have

$$1 - F(\mathcal{T}_\eta[\rho], F\rho F^*) = 1 - \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} W_{\mathcal{T}_\eta[\rho]}(q, p) W_\rho(p, -q) \quad (6.33)$$

$$= \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} \left(W_\rho(p, -q)^2 - W_{\mathcal{T}_\eta[\rho]}(q, p) W_\rho(p, -q) \right) \quad (6.34)$$

$$= \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} W_\rho(p, -q) \left(W_\rho(p, -q) - W_{\mathcal{T}_\eta[\rho]}(q, p) \right). \quad (6.35)$$

since

$$\int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} W_\rho(p, -q)^2 = \text{tr}((F\rho F^*)^2) = \text{tr}(\rho^2) = 1. \quad (6.36)$$

ψ being $\mathcal{L}^1$ implies that its Wigner transform W_ρ is also $\mathcal{L}^1$ ([de 06], proposition 6.43), so

$$1 - F(\mathcal{T}_\eta[\rho], F\rho F^*) = |1 - F(\mathcal{T}_\eta[\rho], F\rho F^*)| \quad (6.37)$$

$$= \left| \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} W_\rho(p, -q) \left(W_\rho(p, -q) - W_{\mathcal{T}_\eta[\rho]}(q, p) \right) \right| \quad (6.38)$$

$$\leq \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} \left| W_\rho(p, -q) \left(W_\rho(p, -q) - W_{\mathcal{T}_\eta[\rho]}(q, p) \right) \right| \quad (6.39)$$

$$= \frac{1}{\pi} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} |W_\rho(p, -q)| \cdot |W_\rho(p, -q) - W_{\mathcal{T}_\eta[\rho]}(q, p)| \quad (6.40)$$

$$\leq \frac{1}{\pi^2} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} |W_\rho(p, -q) - W_{\mathcal{T}_\eta[\rho]}(q, p)| \quad (6.41)$$

$$= \frac{1}{\pi^2} \int_{q \in \mathbb{R}} \int_{p \in \mathbb{R}} \left| W_\rho(p, -q) - W_\rho *_1 g_{\frac{1}{\eta}}(p, -q) \right|, \quad (6.42)$$

where we have used the inequality $|W_\rho(p, -q)| \leq \frac{1}{(2\pi)^N} \leq \frac{1}{\pi}$ for pure states ([de 06], section 6.4.3) to go from equation (6.40) to (6.41). As a result,

$$\|\mathcal{T}_\eta[\rho] - F\rho F^*\| \leq \frac{1}{\pi} \left\| W_{F\rho F^*} - W_{F\rho F^*} *_1 g_{\frac{1}{\eta}} \right\|_{\mathcal{L}^1}. \quad (6.43)$$

By definition, $G_\eta(x) = \eta^{-1}G_1(\eta^{-1}x)$ and $\int_{\mathbb{R}} G_\eta = 1$, so that by [WZ15], theorem 9.6, the net $(G_\eta)_{\eta \in \mathbb{R}_+^*}$ forms an approximation to identity. As a result,

$$\left\| W_{F\rho F^*} - W_{F\rho F^*} *_{\mathbb{1}} g_{\frac{1}{\eta}} \right\|_{\mathcal{L}^1} \rightarrow 0 \quad \text{as } \eta \rightarrow +\infty, \quad (6.44)$$

and it follows that

$$\lim_{\eta \rightarrow \infty} \mathcal{T}_\eta[\rho] = F\rho F^*, \quad (6.45)$$

for any such ρ . Since the trace-class norm agrees with the Hilbert space norm for pure states, and $\mathcal{L}^1(\mathbb{R}) \cap \mathcal{L}^2(\mathbb{R})$ is dense in $\mathcal{L}^2(\mathbb{R})$, equation 6.45 holds by continuity of $\mathcal{T}_\eta$ for any pure $\rho \in \mathfrak{D}(\mathcal{H})$. Finally, since the set of finite convex sums of pure $\rho \in \mathfrak{D}(\mathcal{H})$ is dense in $\mathfrak{D}(\mathcal{H})$ (which is Banach) the result can be extended to mixed states.

Reintroducing the edge-weight and measurement angles, we have

$$\lim_{\eta \rightarrow \infty} \mathcal{T}_\eta(\alpha, \beta, \gamma, w)[\rho] = S(w)FU(\alpha, \beta, \gamma)\rho U^*(\alpha, \beta, \gamma)F^*S^*(w), \quad (6.46)$$

as desired. $\square$

6.3 CV-MBQC and $\mathbb{R}$ -flow

We are now ready to move on to more general MBQCs. Our first stop is to extend the measurement calculus to continuous variables. Like in the qudit case, a (CV) measurement pattern will describe a computation in terms of a sequence of commands. The main difference is in the preparation command, which will have an squeezing-dependent interpretation, since it will formally correspond to initialising a finitely-squeezed auxiliary state.

Definition 6.3. *A CV measurement term on a register V of qumodes consists in a finite ordered sequence of V -indexed commands chosen from:*

- N_u : *initialisation of a qumode u in an auxiliary squeezed state;*
- $E_{u,v}^w$: *entangling operation on qumodes u and v for some $w \in \mathbb{R}$, with $u \neq v$;*
- $M_u(\vec{\theta})$: *measurement of qumode u with angles $\vec{\theta} \in \mathbb{R}^3$;*
- $X_u^{m_v}$ and $Z_u^{m_v}$: *Pauli corrections depending on the outcome $m_v \in \mathbb{R}$ of the measurement of vertex v .*

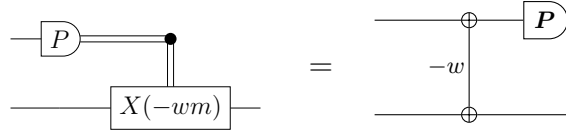
A measurement term is runnable if no commands act on a qumode $v \in V$ before it is initialised (except initialisations) or after it is measured; and no commands depend on the outcome of a measurement before it is made. A runnable measurement term is called a measurement pattern.

Since, formally, the commands above verify essentially the same equations as in the qudit case (equations (2.15)-(2.17)), we can once again rewrite any measurement pattern to the form:

$$\left(\prod_{v \in O^c}^{\prec} X_{\mathbf{x}(v)}^{m_v} Z_{\mathbf{z}(v)}^{m_v} M_v(\vec{\theta}_v) \right) \left(\prod_{u,v \in V} E_{u,v}^{G_{uv}} \right) \left(\prod_{v \in I^c} N_v \right), \quad (6.47)$$

where I, O are subsets of V , $\mathbf{x}, \mathbf{z}$ are functions $O^c \rightarrow \mathbb{R}^V$, m_v is the outcome of the measurement M_v , G is the adjacency matrix of an $\mathbb{R}$ -graph on the vertex set V , and the measurements follow the order $\prec$ induced by the order in which they appear in the measurement pattern. The functions $\mathbf{x}, \mathbf{z}$ implicitly describe a weaker measurement order: the transitive closure of the relation $\{(u, v) \mid \mathbf{x}(v)_u \neq 0 \text{ or } \mathbf{z}(v)_u \neq 0\}$ gives a strict partial order $\prec_{\mathbf{x}, \mathbf{z}}$ on O^c . The measurement order $\prec$ must agree with $\prec_{\mathbf{x}, \mathbf{z}}$, and in fact any measurement order that agrees with $\prec_{\mathbf{x}, \mathbf{z}}$ gives a valid standard form.

We define semantics for CV measurement patterns in a similar way to the qudit case. However, there is one complication: the branch maps no longer give a Kraus decomposition for the total MBQC, as discussed in section 1.3.1. Indeed, each “branch map” would correspond to an outcome $m \in \mathbb{R}^{O^c}$, which formally occurs with probability 0 since we are performing momentum measurements whose outcome probability measures have density with respect to the Lebesgue measure. In order to describe semantics for a pattern, we use a “trick”, reasoning about the induced quantum channel in terms of Stinespring dilations (theorem 1.29) rather than Kraus decompositions. We essentially identify the circuits



$$(6.48)$$

where in both circuits the measurement outcome is discarded. The two-sided control gate in the RHS represents the unitary operation $\exp(-wP_1P_2)$. Both circuits can be seen to output the same Wigner function for inputs W_ρ and W_σ :

$$W_{\text{out}}(x, y) = \int_{\mathbb{R}} \int_{\mathbb{R}} W_\rho(\tau, m) W(x + wm, y) d\tau dm. \quad (6.49)$$

The RHS of equation 6.48 can be represented in terms of density matrices using the partial trace as

$$\rho_{\text{out}} = \text{tr}_1(\exp(-iwP_1P_2)\rho_{\text{in}}\exp(iwP_1P_2)) = \text{tr}_1(\Gamma_{\exp(-iwP_1P_2)}[\rho_{\text{in}}]) \quad (6.50)$$

Extending this construction to the entire measurement pattern, we get, for an input $\rho \in \mathfrak{D}(\mathcal{H}^{\otimes I})$, squeezing factor $\eta \in \mathbb{R}_+^*$ and choice of measurements

$\theta : O^c \rightarrow \mathbb{R}^3$:

$$\begin{aligned} & \llbracket G, I, O, \mathbf{x}, \mathbf{z} \rrbracket_\theta^\eta [\rho] \\ &= \left(\prod_{v \in O^c} \text{tr}_v \circ \Gamma_{\exp(-iP_v \mathbf{x}(v) \cdot \vec{P})} \circ \Gamma_{\exp(iP_v \mathbf{z}(v) \cdot \vec{Q})} \circ \Gamma_{U_v(\theta(v))} \right) \circ \Gamma_{E_G} \left(\rho \bigotimes_{v \in I^c} P_{g_\eta} \right), \end{aligned} \quad (6.51)$$

where

$$E_G = \prod_{u,v \in V} CZ_{u,v}^{G_{uv}}, \quad (6.52)$$

$$\mathbf{x}(v) \cdot \vec{P} = \sum_{k \in V} \mathbf{x}(v)_k P_k, \quad (6.53)$$

$$\mathbf{z}(v) \cdot \vec{Q} = \sum_{k \in V} \mathbf{z}(v)_k Q_k. \quad (6.54)$$

Finally, the outcome determinism question no longer really makes sense in the CV case: the state obtained for a given outcome $m \in \mathbb{R}^{O^c}$ isn't well defined. If we want to make sense of this question at all, we have to describe a partition of the outcome space into measurement space, which essentially amounts to binning the outcomes. Even then, the situation is hopeless: one always has a non-zero (but very low, as η increases) probability of obtaining some very large measurement outcome for which the output state is garbage. As a consequence we cannot drop the corrections in the LHS of equation 6.51 as we did in equation 2.22 for robustly deterministic qudit MBQCs. It turns out that the question of convergence is much more appropriate in the CV case, since if the channel converges to a unitary, then the output state does not depend on the measurement outcomes anyways.

It is hopefully clear at this point that many of the results we obtained for $\mathbb{Z}_d$ -flow will carry over to continuous variables, but where the field $\mathbb{R}$ replaces $\mathbb{Z}_d$. We will of course use the name $\mathbb{R}$ -flow (although in the article version [BM21], simple $\mathbb{R}$ -flow was called CV-flow), and repeat some definitions here for the sake of completeness:

Definition 6.4. *An open $\mathbb{R}$ -graph is a triple (G, I, O) where G is an $\mathbb{R}$ -graph over V , and $I, O \subseteq V$ are distinguished sets of vertices which identify inputs and outputs in an MBQC.*

A labelled open $\mathbb{R}$ -graph is a tuple (G, I, O, λ) where (G, I, O) is an open $\mathbb{R}$ -graph and $\lambda : O^c \rightarrow \mathbb{R}^2 \setminus \{(0, 0)\}$ assigns a measurement space to each measured vertex.

For an open graph (G, I, O) , an arbitrary input state $\phi \in \mathcal{H}^{\otimes I}$, and a squeezing

factor $\eta \geq 1$ we define a *CV open graph state* as

$$G_\eta(\phi) = \left(\prod_{\substack{u,v \in V \\ u < v}} CZ_{u,v}^{G_{u,v}} \right) \left(\phi \bigotimes_{u \in I^c} g_\eta \right). \quad (6.55)$$

As in the qudit case, when $I = \emptyset$ we obtain finitely squeezed graph states [Men+06; Gu+09; Zha10; Zha08; ZB06]. This graph-theoretical representation is similar to that of [MFv11]

Definition 6.5. *The labelled open $\mathbb{R}$ -graph (G, I, O, λ) has an $\mathbb{R}$ -flow (C, Λ) if $C \in \mathbb{R}^{V \times V}$ and Λ is a totally ordered partition of V such that*

1. $\forall u \in O^c, \lambda(u) = (C_{uu}, (GC)_{uu})$;
2. $C[I, V] = 0$ and $C[V, O] = 0$;
3. for any $M, N \in \Lambda$,
 - $C[M, M]$ and $(GC)[M, M]$ are diagonal;
 - whenever $M < N$, $C[M, N] = (GC)[M, N] = 0$.

If $\lambda(u) = (0, 1)$ for all $u \in O^c$, we say that (C, Λ) is a *simple $\mathbb{R}$ -flow*, otherwise it is extended. We call Λ a *layer decomposition* of (G, I, O, λ) for C and the elements of Λ are *layers*.

As stated in the introduction, we will restrict our attention to the case of simple $\mathbb{R}$ -flows, since the necessary work on extending measurement spaces to $\mathcal{L}^2(\mathbb{R})$ has not yet been done. As in the qudit case, if (G, I, O) is an open graph with simple $\mathbb{R}$ -flow (C, Λ) , then we obtain a runnable MBQC $(G, I, O, \mathbf{x}_C, \mathbf{z}_C)$ by setting

$$\mathbf{x}_C(v) := C_{\bullet v} \quad \text{and} \quad \mathbf{z}_C(v) := ((GC)_{\bullet v} - 1_{\{v\}}), \quad (6.56)$$

where $M_{\bullet v}$ is the v -th column of a given matrix M .

Then, we obtain the same equivalent characterisation as in the qudit case:

Definition 6.6. *Let (G, I, O) be an open graph, Λ a layer decomposition of G , and define $P(k) := \cup_{j \geq k} \Lambda_k$ (the “past” of layer k). Then the correction matrix G_k^Λ is the matrix $G_k^\Lambda := G[P(k), (P(k) \cup I)^c]$.*

G_k^Λ is the subgraph of G which at each step of the MBQC (each layer) describes the back-action of possible corrections made on as-of-yet unmeasured vertices. Viewed this way, simple $\mathbb{R}$ -flow essentially amounts to a condition that assures that this back-action can always be controlled to correct the measurement outcome without induces new errors in previous layers:

Proposition 6.7. *An open $\mathbb{R}$ -graph (G, I, O) has simple $\mathbb{R}$ -flow (C, Λ) if and only if for each k the linear equation*

$$G_k^\Lambda \vec{c}_j = \begin{pmatrix} \vec{0}_{P(k) \setminus \Lambda_j} \\ \vec{m} \end{pmatrix} \quad \text{has solutions} \quad \vec{c}_k \in \mathbb{R}^{(P(k) \cup I)^c} \quad \text{for any} \quad \vec{m} \in \mathbb{R}^{\Lambda_k}, \quad (6.57)$$

where $\vec{0}_n$ is a (possibly empty) column vector of n zeros.

Proof. The proof is essentially identical to the qudit case (proposition 4.6), where we formally replace $\mathbb{Z}_d$ by $\mathbb{R}$. $\square$

6.4 CV-MBQCs with simple $\mathbb{R}$ -flow converge

We now address the induced quantum map and the question of convergence of the MBQC. In general, for an arbitrary graph state, even one with simple $\mathbb{R}$ -flow, the MBQC procedure is not convergent. It is possible for the output state to contain squeezing dependant components which diverge in the limit. The simplest example is given by the single-vertex open graph $\circ$ with no input and a single output.⁴ One can readily check that it trivially has simple $\mathbb{R}$ -flow but the output is a squeezed state. As a result, when if we try to take the infinite squeezing limit the state diverges in $\mathcal{H}$.

We address the infinite squeezing limit by constructing an explicit circuit to which the MBQC converges. To do so, we re-use many of the techniques of chapter 4—with a twist. In the qudit case, we were able to extract the circuit from the back since we treat each extracted teleportation independently and do not have to worry about the convergence of teleportations from earlier in the MBQC. Here, this method no longer suffices. We need to ensure that all the teleportations converge. In order for this to work, we show how to construct a path cover for any open graph with simple $\mathbb{R}$ -flow. This path cover essentially identifies a sequence of gate teleportations which each input undergoes, and each of these can be proven to converge by proposition 6.2. We restate many of the results from chapter 4 for clarity, whilst also noting that some results need new proofs as they only hold in an approximate sense (for example, lemma 6.12 on controlled stabilisers of the open graph).

As we shall see, the existence of a simple $\mathbb{R}$ -flow implies both that $|I| \leq |O|$ and $|O| \neq 0$, and we shall conclude that a sufficient condition for the protocol to be convergent is that the open graph has simple $\mathbb{R}$ -flow and as many input vertices as outputs, $|I| = |O|$. Furthermore, if the open graph has simple $\mathbb{R}$ -flow, then the MBQC converges only if $|I| = |O|$.

⁴This open graph is formally defined in the language of definition 6.3 on the vertex set $\{\circ\}$ as $(0, \emptyset, \{\circ\})$.

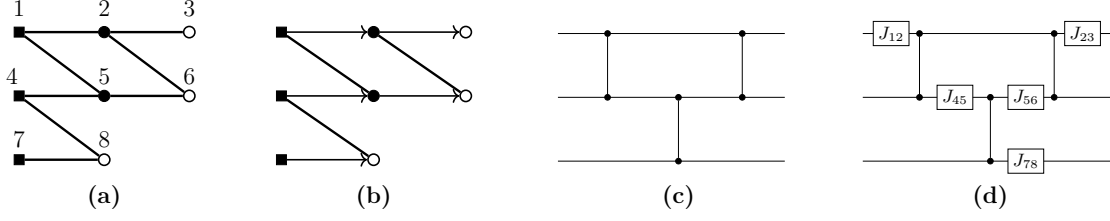


Figure 6.1: An example of circuit extraction of an MBQC for an open graph with causal flow, using star pattern transformation as described in section 6.4.1. Starting from an open graph with a causal flow **(a)**, we identify a path cover of the graph that agrees with the causal flow (thick edges directed $u \rightarrow f(u)$ for each $u \in O^c$) **(b)**, and each path as a wire in a quantum circuit **(c)**. The remaining edges of the graph implement CZ gates in the circuit. Finally, each causal flow edge implements a unitary of the form given by equation (4.9), and we obtain a circuit representation of the unitary implemented by the MBQC **(d)**.

Like for chapter 4, the actual circuit extraction scheme is inspired by [MHM15]. While the circuits extracted by our scheme as well as the broad structure of the proof are entirely analogous to that work, our proof method is quite different. The original graph-theoretical arguments using local complementation in [MHM15] do not hold for CV, so we reason instead with the adjacency matrix and correction matrices of the open graph. The main differences with the qudit case are the new proofs of lemmas 6.12, proposition 6.10 and theorem 6.18 which only hold in the infinite squeezing limit, and the construction of a path cover for any simple $\mathbb{R}$ -flow (lemma 6.9).

6.4.1 Star pattern transformation

As in chapter 4, in order to model the computation through the MBQC, the trick is to distinguish between “real” qumodes that undergo a unitary transformation through the MBQC (which act like the wires in a circuit undergoing gates), and auxiliary qumodes that are consumed in teleportations. In the case of causal flow, things work quite nicely as follows.

We use the following which also holds in CV (since the causal flow does not depend on edge weights, only the correction procedure):

Definition 6.8 ([de 08]). A **path cover** of an open graph (G, I, O) is a collection $\mathcal{P}$ of directed edges (or arcs) in G such that

- each vertex in G is contained in exactly one path in $\mathcal{P}$;
- each path in $\mathcal{P}$ is either disjoint from I or intersects I only at its initial point;

- each path in $\mathcal{P}$ intersects O only at its final point.

If the open $\mathbb{R}$ -graph (G, I, O) has a causal flow $(f, \prec)$ (definition 2.11) then we can obtain a runnable CV MBQC $(G, I, O, \mathbf{x}_f, \mathbf{z}_f)$ given by:

$$\mathbf{x}_f(u) = -G_{u,f(u)}^{-1} 1_{\{f(u)\}} \quad \text{and} \quad \mathbf{z}_f(u) = -G_{u,f(u)}^{-1} G 1_{N(f(u)) \setminus \{u\}}. \quad (6.58)$$

Lemma 6.9 (Causal flow path cover [de 08]). *Let $(f, \leq)$ be a causal flow on an open graph (G, I, O) . Then there is a path cover P_f of (G, I, O) where $x \rightarrow y$ is an arc in some path of P_f if and only if $y = f(x)$.*

Lemma 6.9 allows us to interpret the causal flow MBQC procedure as a sequence of single qumode gate teleportations, with additional entangling operations between teleportations. In fact, the path cover $\mathcal{P}_f$ allows us to distinguish between two types of edges in G :

- edges $(j, k) \in \mathcal{P}_f$ correspond to gate teleportations where one end is the input and the other the output;
- edges $(j, k) \notin \mathcal{P}_f$ correspond to $\text{CZ}(A_{j,k})$ gates in the final circuit.

While it was originally formulated for DV, an almost identical method to *Star pattern transformation* (STP) functions in CV, the only real difference being the nature of the unitary gates. Assume (G, I, O) is an open graph with causal flow $(f, \prec)$ and corresponding path cover P_f , and let

$$J(w, \alpha, \beta, \gamma) := S(w)FU(\alpha, \beta, \gamma), \quad (6.59)$$

and for any subset $S \subseteq G$,

$$\text{CZ}_{j,S}(s) := \prod_{k \in S} \text{CZ}_{j,k}(w), \quad \text{and} \quad \text{CX}_{j,S}(s) := \prod_{k \in S} \text{CX}_{j,k}(w). \quad (6.60)$$

To obtain a circuit for the causal flow MBQC,

1. Interpret each path in P_f as a wire (qumode) in a quantum circuit, and index the wire by the collection of vertices intersected by the path.
2. For each edge $(j, k) \notin \mathcal{P}_f$, insert a $\text{CZ}(A_{j,k})$ gate between the edges indexed by j and k .
3. For each edge $(j, k) \in \mathcal{P}_f$, insert a $J(A_{j,k}, \alpha, \beta, \gamma)$ gate after all the CZ gates for vertices $i \in \mathcal{P}_f$ such that $i \leq j$ but before all such gates for $k \leq i$.

An example is worked out in figure 6.1. In the ideal limit, the MBQC converges to the CV SPT map for any choice of measurements:

Proposition 6.10 (Causal flow circuit). *Suppose the open graph (G, I, O) has a causal flow and $|I| = |O|$. Then for any $\theta : O^c \rightarrow \mathbb{R}^3$ and any $\rho \in D(\mathcal{H}^{\otimes |I|})$,*

$$\lim_{\eta \rightarrow \infty} \llbracket G, I, O, \mathbf{x}_f, \mathbf{z}_f \rrbracket_{\theta}^{\eta} [\rho] = U_{SPT}(\theta) \rho U_{SPT}^*(\theta), \quad (6.61)$$

where U_{SPT} is the unitary corresponding to the circuit obtained by star pattern transformation of (G, I, O) for the choice of measurements θ . Furthermore, the condition $|I| = |O|$ is necessary.

Proof. As explained above, we can decompose $\llbracket G, I, O, \mathbf{x}_f, \mathbf{z}_f \rrbracket_{\theta}^{\eta}$ as a set of parallel paths with mediating edges. Each of these parallel paths corresponds to a sequence of single gate teleportations. All we need to worry about is ordering the mediating edges such that they appear before any teleportation of a vertex they are connected to. This is possible since such an ordering exists if and only if there is a causal flow [MHM15]. Then, by proposition 6.2 each teleportation converges, and since each gate teleportation channel is continuous it preserves limits. $\square$

6.4.2 Simple $\mathbb{R}$ -flow triangularisation

The next challenge is to do the same as above and extract a circuit, for simple $\mathbb{R}$ -flow. For simple $\mathbb{R}$ -flow however, it is not obvious how to go about this, for instance one does not directly have an obvious path cover. We follow the ideas of [MHM15], associating open graphs with simple $\mathbb{R}$ -flow to equivalent open graphs with causal flow which allows circuit extraction, albeit using quite different proof methods.

This section repeats many of the proofs of chapter 4. There are two main differences. Firstly, some results only hold in the infinite-squeezing limit, such as the existence of controlled-stabilisers (lemma 6.12), so those results need to be reproved. Secondly, we show that we can use the triangularisation procedure to find a causal flow from each layer into the next ($\Lambda_{n+1} \rightarrow \Lambda_n$), and use this sequence of causal flows to construct the path cover which we need for the convergence proof (section 6.4.2).

From $\mathbb{R}$ -flow to causal flow

In order to extract causal flows from $\mathbb{R}$ -flows, we need a matricial characterisation of causal flow. Essentially the same proposition holds as in the qudit case (proposition 4.11):

Lemma 6.11 (Matrix form of causal flow). *Let (G, I, O) be an open graph with simple $\mathbb{R}$ -flow for a layer decomposition Λ and $L \subseteq O^c$. Then there is a subset*

$C \subseteq P(L)^c$ with $|L| = |C|$ and a causal flow $L \rightarrow C$ if and only if the “correction matrix” of L can be written as

$$A_L := G[P(L), (P(L) \cup I)^c] = M \cdot \begin{pmatrix} X & 0 \\ Y & T \end{pmatrix} \cdot N \quad (6.62)$$

where M and N are permutation matrices, T is a lower triangular $|V| \times |C|$ matrix with non-zero diagonal and X, Y are arbitrary real matrices. In other words, we can turn $A_L^<$ into the partial triangular form of equation (4.36) only by reordering rows and columns, which in turn corresponds to relabelling the vertices of the graph G .

Proof. The proof is essentially the same as proposition 4.11. □

As in the qudit case, this characterisation of causal flow is the key difference between our proof method and that of Miyazaki, Hajdušek, and Murao [MHM15]—where they use arguments based on local complementation to find a causal from a g-flow, we solve the comparatively easier problem of proving it is always possible to map an open state with $\mathbb{R}$ -flow to one where the correction matrix takes this form. The approach now is, having broken the measurement pattern down into layers, we show that the graph over each pair of layers can be seen as having flow, by transforming the correction matrix such that it takes the above triangular form. Reordering rows and columns of the correction matrix simply corresponds to relabelling of the vertices, however, we will also require linear addition of columns. This matrix or graphical operation, it turns out, is physically equivalent to applying CX gates, which are exactly the additional operations in the equivalence we mentioned. This emerges from the following stabiliser condition for controlled operators, which is approximate for any finite squeezing and, as for the standard stabiliser conditions, only holds perfectly in the infinite squeezing limit:

Lemma 6.12 (Approximate controlled stabilizers). *Let (G, I, O) be an open graph, $j \in G$ and $k \in I^c$. Then, for any Schwartz input state $\phi \in \mathcal{H}^{\otimes |I|}$ and $s \in \mathbb{R}$,*

$$\lim_{\eta \rightarrow \infty} \left\| \text{CX}_{j,k}(s) \text{CZ}_{j,N(k)}(s) G_\eta(\phi) - G_\eta(\phi) \right\| = 0. \quad (6.63)$$

The Schwartz condition on the input state is a technical consideration without which I have been unable to find a proof of this statement, and which therefore carries through to the main convergence result, theorem 6.18. Note however, that any physical state is experimentally indistinguishable from a Schwartz state [BG89].

Proof. Let $\phi \in (\mathcal{S}(\mathbb{R}))_1$, $s \in \mathbb{R}$ and consider

$$\text{CX}_{1,2}(s)[\phi \otimes g_\eta](x, y) = \exp(isQ_1P_2)[\phi \otimes g_\eta](x, y) = \phi(q)g_\eta(y + sx). \quad (6.64)$$

Now, since ϕ is square-integrable of norm 1, for any $\epsilon > 0$ there is some bounded measurable subset $E \subseteq \mathbb{R}$ such that

$$\int_{x \in E^c} |\phi(x)|^2 < \epsilon, \quad (6.65)$$

and

$$\|CX_{1,2}(s)\phi \otimes g_\eta - \phi \otimes g_\eta\|^2 = \frac{1}{\sqrt{\pi\eta^2}} \int_{x \in \mathbb{R}} \int_{y \in \mathbb{R}} \left| \phi(x) e^{-\frac{(y+sx)^2}{2\eta^2}} - \phi(x) e^{-\frac{y^2}{2\eta^2}} \right|^2 \quad (6.66)$$

$$\leq \frac{1}{\sqrt{\pi\eta^2}} \int_{x \in \mathbb{R}} \int_{y \in \mathbb{R}} |\phi(x)|^2 \left| e^{-\frac{(y+sx)^2}{2\eta^2}} - e^{-\frac{y^2}{2\eta^2}} \right|^2 \quad (6.67)$$

$$\leq \frac{1}{\sqrt{\pi\eta^2}} \int_{x \in E} \int_{y \in \mathbb{R}} |\phi(x)|^2 \left| e^{-\frac{(y+sx)^2}{2\eta^2}} - e^{-\frac{y^2}{2\eta^2}} \right|^2 \quad (6.68)$$

$$+ \frac{1}{\sqrt{\pi\eta^2}} \int_{x \in E^c} \int_{y \in \mathbb{R}} |\phi(x)|^2 \left| e^{-\frac{(y+sx)^2}{2\eta^2}} - e^{-\frac{y^2}{2\eta^2}} \right|^2 \quad (6.69)$$

$$\leq \frac{1}{\sqrt{\pi\eta^2}} \int_{x \in E} |\phi(x)|^2 \int_{y \in \mathbb{R}} \left| e^{-\frac{(y+sx)^2}{2\eta^2}} - e^{-\frac{y^2}{2\eta^2}} \right|^2 + 2 \int_{x \in E^c} |\phi(x)|^2. \quad (6.70)$$

Furthermore, using for any $x, y \in \mathbb{R}$,

$$\left| e^{-\frac{(y+sx)^2}{2\eta^2}} - e^{-\frac{y^2}{2\eta^2}} \right| \leq |sx| \cdot \max_{t \in \mathbb{R}} \frac{d}{dt} \left(e^{-\frac{t^2}{2\eta^2}} \right) \leq \frac{A}{\eta} |sx| \quad (6.71)$$

where $A = \max_{t \in \mathbb{R}} \frac{d}{dt} \left(e^{-\frac{t^2}{2}} \right)$. Then,

$$\|CX_{1,2}(s)\phi \otimes g_\eta - \phi \otimes g_\eta\|^2 \leq \frac{A^2 s^2}{\eta^3 \sqrt{\pi}} \int_{x \in E} |x\phi(x)|^2 + 2\epsilon, \quad (6.72)$$

and since ϕ is Schwartz, $\int_{x \in E} |x\phi(x)|^2$ is bounded by some $B > 0$. Finally,

$$\|CX_{1,2}(s)\phi \otimes g_\eta - \phi \otimes g_\eta\|^2 \leq \frac{A^2 B s^2}{\eta^3 \sqrt{\pi}} + 2\epsilon, \quad (6.73)$$

whence picking $\eta > \sqrt[3]{\frac{\sqrt{\pi}}{A^2Bs^2}}$ we have $\|CX_{1,2}(s)\phi \otimes g_\eta - \phi \otimes g_\eta\|^2 < 3\epsilon$, and because $\epsilon < 0$ was arbitrary,

$$\lim_{\eta \rightarrow \infty} \|CX_{1,2}(s)\phi \otimes g_\eta - \phi \otimes g_\eta\|^2 = 0. \quad (6.74)$$

Every controlled stabiliser can be reduced to this case by commuting through E_G ,

$$CX_{j,k}(s) CZ_{j,N(k)}(s) E_G = E_G CX_{j,k}(s), \quad (6.75)$$

and noting that g_η is Schwartz so can be substituted for the arbitrary input ϕ if $j \notin I$, we are done. $\square$

In this way, the action of specific CZ operations - which are what are used to create or remove edges in the graph - are equivalent (in the infinite squeezing limit) to the application of a CX operation. This allows us to achieve the our goal:

Proposition 6.13 (Triangularisation). *If (G, I, O) is an open graph with $\mathbb{R}$ -flow, and L is the last layer in a corresponding layer decomposition, then (G, I, O) is approximately equivalent to an open graph with a causal flow $L \rightarrow O$, up to weighted CX gates acting in O and reordering the vertices in L .*

Proof. Let A_L be the correction matrix of L for a given $\mathbb{R}$ -flow order. Then, we can reorder the columns of A_L by relabeling the unmeasured vertices, and we can reorder the rows of A_L by choosing a different measurement order for vertices in L .

Further let $j, k \in O$, then by lemma 6.12 applying the gate $CX_{j,k}(-s)$ on the graph state induces new edges in the graph state *in the infinite squeezing limit*. The result on the correction matrix is the transformation

$$C_j \mapsto C_j + sC_k, \quad (6.76)$$

where C_j is the j -th column of A_L .

By the definition of $\mathbb{R}$ -flow, for each $v \in L$ we have that

$$A_L^< c_v(1_v) = 1_v, \quad (6.77)$$

so that $c_v(1_v)$ gives a sum of columns A which contains a single 1 in the row corresponding to v . Repeating this for each $v \in L$, we obtain $|L|$ such columns, each with the 1 on a different row, so that by reordering rows and columns we can write A_L as

$$A_L \sim \begin{pmatrix} X & 0 \\ Y & I_{|L|} \end{pmatrix} \quad (6.78)$$

where $I_{|L|}$ is the $|L| \times |L|$ identity matrix. Then, A_L takes the form described in lemma 6.11, and this partial triangularisation procedure corresponds to extracting additional CX gates from the graph as described above. Then, the open graph (G, I, O) is approximately equivalent to a graph with causal flow $L \rightarrow O$, up to CX gates acting in O . $\square$

The fact that the additional controlled gates act only on the outputs is crucial: it will allow us reduce the total physical map to a sequence of single-gate teleportation operations. Since the CX gates never appear in between a measurement and the corresponding CZ gate for the teleportation, nor do they act on the auxiliary squeezed states before they are consumed in the teleportation, the projective measurements can be brought forward and the squeezed inputs delayed to obtain a single gate teleportation circuit within the larger circuit representing the total physical map of the computation.

Path cover of $\mathbb{R}$ -flow

Now, using these two lemmas, we obtain a causal flow from the last layer Λ_1 of a decomposition into a subset of the outputs by adding CX gates. Most importantly, this subset is then only connected to Λ_1 so it can be removed from the open graph as far as determining flows on the remainder is concerned. As a result, we can reduce a graph to a sequence of causal flows by peeling off each layer one-by-one.

Lemma 6.14 (Graph reduction). *If (G, I, O) is an open graph with simple $\mathbb{R}$ -flow (C, Λ) then there is $C_1 \subseteq O$ such that there is a causal flow $\Lambda_1 \rightarrow C_1$ with $|\Lambda_1| = |C_1|$, up to a product T of weighted CX gates acting in O . Furthermore, let G' be the graph state obtained from the triangularisation procedure for layer Λ_1 , then $(G' \setminus C_1, I \setminus C_1, \Lambda_1 \cup (O \setminus C_1))$ has simple $\mathbb{R}$ -flow, for the layer decomposition $\{\Lambda_k\}_{k=2}^N$.*

Proof. The first part follows straightforwardly from lemmas 6.11 and 6.13. The second is immediate once one realises the following: by the third condition in the definition of causal flow, if there is a causal flow $C_1 \rightarrow L_1$, C_1 cannot be connected to any vertex in a layer $k > 1$. Since L_1 is measured last, so C_1 must be connected *only* to L_1 (and possibly O). As a result, we can remove C_1 from the graph for subsequent layers: since it is not connected to any previous layer $k > 1$, it never appears in any subsequent correction subgraphs. As a result, the truncated $\mathbb{R}$ -flow and layer decomposition remain valid for the reduced graph. $\square$

This “peeling” procedure also allows us to determine a path cover of (G, I, O) , by noting that each layer causal flow has a path cover, and the endpoints of each of these covers meet up. So, by a successive applications of this lemma, we obtain a the final ingredient to our proof, a $\mathbb{R}$ -flow analogue of lemma 6.9:

Lemma 6.15 ($\mathbb{R}$ -flow path cover). *Let (G, I, O) be an open graph with simple $\mathbb{R}$ -flow, then there is a path cover of (G, I, O) whose edges are causal flow edges of the triangularised graph (6.13). If $|I| = |O|$, every path is indexed by an input.*

Proof. Let $\{L_k\}$ be a layer decomposition of (G, I, O) , and consider each vertex $j \in O$ the endpoint of a path. Then, by lemma 6.14 there is $C_1 \subseteq O$ such that there is a causal flow and a bijection $L_1 \rightarrow C_1$; label each vertex in L_1 by its image under the causal flow matching. Then, remove C_1 from the graph as in lemma 6.14, and repeat the process. Since $\bigcup_{k=1}^N L_k \cup O = G$, we eventually label the whole graph. Furthermore, the resulting paths never cross: if they did, there would be two vertices in the same layer corrected onto the same vertex—but this is impossible, by the definition of causal flow. Thus the resulting set of paths is a path cover for (G, I, O) .

Finally, if $|I| = |O|$, every input is the beginning of some path, since we measure all $j \in I$ but can never correct onto I . Since there are exactly $|O| = |I|$ paths, every path must begin in I and end in O , and every path is indexed by an input. $\square$

As a corollary, we obtain bounds on the number of inputs and outputs of an open graph if it has a $\mathbb{R}$ -flow:

Corollary 6.16. *Let (G, I, O) be an open graph with simple $\mathbb{R}$ -flow, then $|I| \leq |O|$.*

Proof. By the proof to the lemma, every input is the beginning of a path that ends in O , and these paths never cross, such that even their endpoints in O cannot coincide. Then, the collection of paths describes an injection $I \rightarrow O$, since each path uniquely associates an endpoint in O to each input. $\square$

Corollary 6.17. *Let (G, I, O) be an non-empty open graph with simple $\mathbb{R}$ -flow, then $|O| \neq 0$.*

Proof. If $G \neq \emptyset$ and the open graph has simple $\mathbb{R}$ -flow, then there is a path cover of the open graph which contains at least one path. This path must end at an output vertex, thus $|O| \neq 0$. $\square$

Putting it all together

Theorem 6.18 (Simple $\mathbb{R}$ -flow circuit). *Assume (G, I, O) is an open graph with simple $\mathbb{R}$ -flow (C, Λ) and $|I| = |O|$ then for any $\theta : O^c \rightarrow \mathbb{R}^3$ and any Schwartz input state $\rho \in \mathcal{D}(\mathcal{H}^{\otimes I})$,*

$$\lim_{\eta \rightarrow \infty} \llbracket G, I, O, \mathbf{x}_C, \mathbf{z}_C \rrbracket_{\theta}^{\eta} [\rho] = \Gamma_{\prod_{k=1}^n T^{(k)} U_{SPT}^{(k)}(\theta|_{\Lambda_k})} [\rho], \quad (6.79)$$

where $U_{SPT}^{(k)}$ is the circuit extracted for the k -th layer using the causal flow from lemma 6.14, and $T^{(k)}$ contains the CX gates obtained from the triangularisation of the $\mathbb{R}$ -flow (lemma 6.13).

$T^{(k)}U_{SPT}^{(k)}(\theta|_{\Lambda_k})$ acts on the qumodes represented by wires indexed by L_k , and the total product acts on the qumodes represented by wires indexed by I .

As mentioned previously, we need to assume that the input state is Schwartz in order to be able to use lemma 6.12. If it is a pure state, this amounts to assuming that it is the density operator of a Schwartz function. In the mixed case, Schwartz density operators are defined in [KKW16], but they naturally correspond to density operators whose Wigner functions are Schwartz. For pure states, these two definitions match.

Proof. By lemma 6.15 we obtain a graph G' that is approximately equivalent to G up to CX gates. Let $E_G^{(k)}$ be the product of CZ gates in G' from layer Λ_k into its outputs and $T^{(k)}$ the CX gates obtained from the corresponding triangularisation procedure. By lemmas 6.13 and 6.15 for any $A > 0$ we have, for high enough squeezing, that

$$\left\| \Gamma_{E_G} [P_{g_\eta}^{\otimes |I^c|} \otimes \rho] - \Gamma_{\prod_{k=1}^n \left(T^{(k)} E_G^{(k)} \right)} [P_{g_\eta}^{\otimes |I^c|} \otimes \rho] \right\| < A. \quad (6.80)$$

Now, none of the edges in $T^{(k)} E_G^{(k)}$ for $k < n$ touch the vertices in Λ_{k+1} , so that we can bring the auxiliary squeezed states $|\eta\rangle_v$ for $v \in \Lambda_k$ forward until $E_G^{(k)}$. Since there is a causal flow $\Lambda_{k+1} \rightarrow \Lambda_k$,

$$\Gamma_{\prod_{k=1}^n \left(T^{(k)} E_G^{(k)} \right)} [P_{g_\eta}^{\otimes |I^c|} \otimes \rho] = \Gamma_{T^{(n)}} \circ \mathcal{O}^{(n)} \circ \dots \circ \Gamma_{T^{(1)}} \circ \mathcal{O}^{(1)} [\rho] \quad (6.81)$$

where $\mathcal{O}^{(k)}$ is the channel associated to the causal flow procedure $\Lambda_{k+1} \rightarrow \Lambda_k$. Then by proposition 6.10, we can perform an SPT for each $\mathcal{O}^{(k)}$, and

$$\lim_{\eta \rightarrow \infty} \llbracket G, I, O, \mathbf{x}_C, \mathbf{z}_C \rrbracket_\theta^\eta [\rho] = \prod_{k=1}^n T^{(k)} U_{SPT}^{(k)}(\vec{\alpha}, \vec{\beta}, \vec{\gamma}), \quad (6.82)$$

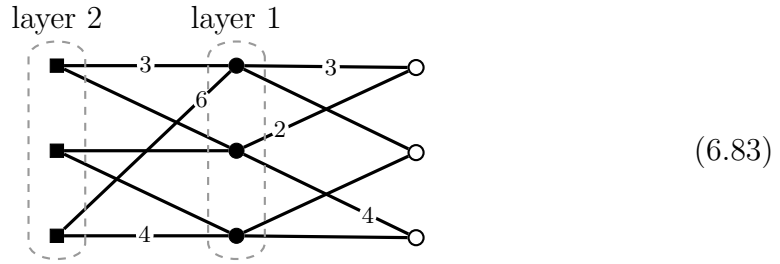
by continuity. $\square$

An example of the complete circuit extraction procedure for an open graph based on a $\mathbb{R}$ -flow in section 6.5.

6.5 A worked-out example

We conclude this chapter with an example of the extraction procedure corresponding to theorem 6.18. It is important to note that running the algorithm from chapter 4 produces the correct circuit for the ideal limit, if one, as always, replaces the field $\mathbb{Z}_d$ with $\mathbb{R}$. We include this example nonetheless, as we present the extraction in a slightly different way, which more closely matches the proof method for theorem 6.18. Hopefully, it will help to make that proof clearer.

Consider the open graph:



whose adjacency matrix is

$$G = \begin{pmatrix} & & & 3 & 1 & 0 \\ & & & 0 & 1 & 1 \\ & & & 6 & 0 & 4 \\ 3 & 0 & 6 & & & 3 & 1 & 0 \\ 1 & 1 & 0 & & & 2 & 0 & 4 \\ 0 & 1 & 4 & & & 0 & 1 & 1 \\ & & & 3 & 2 & 0 \\ & & & 1 & 0 & 1 \\ & & & 0 & 4 & 1 \end{pmatrix} \quad (6.84)$$

It has a simple $\mathbb{R}$ -flow for the given layer decomposition given by

$$C = \begin{pmatrix} 0 \\ 0 & 0 \\ 0 & 0 & 0 \\ \frac{2}{9} & -\frac{2}{9} & \frac{1}{18} & 0 \\ \frac{1}{3} & \frac{2}{3} & -\frac{1}{6} & 0 & 0 \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{6} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{2}{7} & \frac{1}{14} & -\frac{2}{7} & 0 \\ 0 & 0 & 0 & \frac{1}{7} & -\frac{3}{14} & \frac{6}{7} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{7} & \frac{3}{14} & \frac{1}{7} & 0 & 0 & 0 \end{pmatrix} \quad (6.85)$$

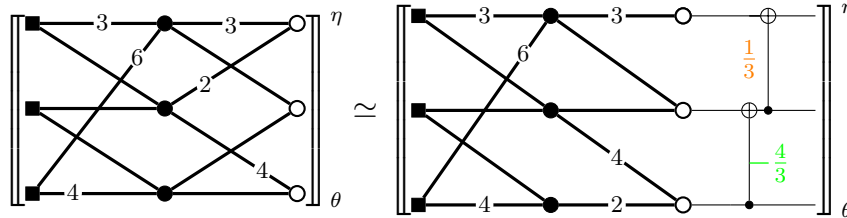
since

$$GC = \begin{pmatrix} 1 & & & & & & & & \\ 0 & 1 & & & & & & & \\ 0 & 0 & 1 & & & & & & \\ 0 & 0 & 0 & 1 & & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 0 & 0 & 0 & 0 & 1 & & & \\ \frac{4}{3} & \frac{2}{3} & -\frac{1}{6} & 0 & 0 & 0 & 0 & & \\ \frac{1}{9} & -\frac{1}{9} & \frac{2}{9} & 0 & 0 & 0 & 0 & 0 & \\ 1 & 3 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (6.86)$$

The empty elements are once again taken to be zero. The first step of the algorithm is to run the triangularisation procedure for the entire graph, layer by layer. From equation (6.85) and definition 6.6, the correction matrix for layer 1 can be triangularised by:

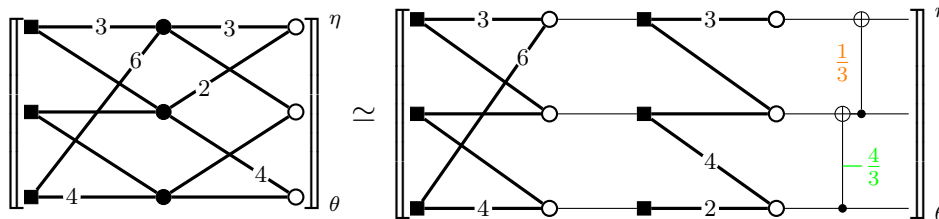
$$G[O^c, O] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 0 & 4 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{\begin{matrix} C_2 \leftarrow C_2 - \frac{1}{3}C_1 \\ C_3 \leftarrow C_3 + \frac{4}{3}C_2 \end{matrix}} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3 & 0 & 0 \\ 2 & -\frac{2}{3} & 0 \\ 0 & 1 & \frac{11}{3} \end{pmatrix} \quad (6.87)$$

By lemma 6.14, these column operations correspond to CX gates acting within the outputs, which we call pull into the circuit part of the circuit:



$$\approx \quad (6.88)$$

Then, we can view the remaining open graph as the composition of the subgraph between layer 1 and the outputs, and the remaining open graph. If we view the composition as a circuit between the outputs of the latter into the inputs of the former, we get the approximation:

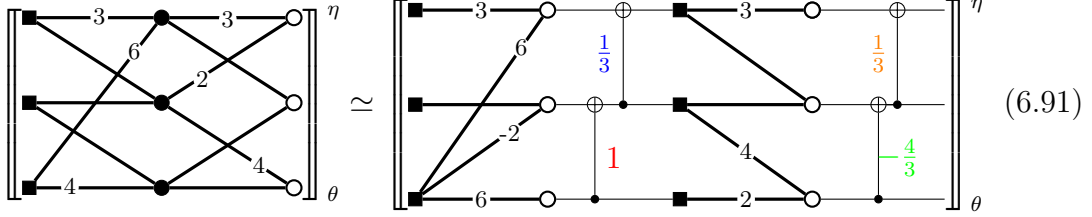


$$\approx \quad (6.89)$$

The remaining subgraph, which corresponds to layer 2, is triangularised by:

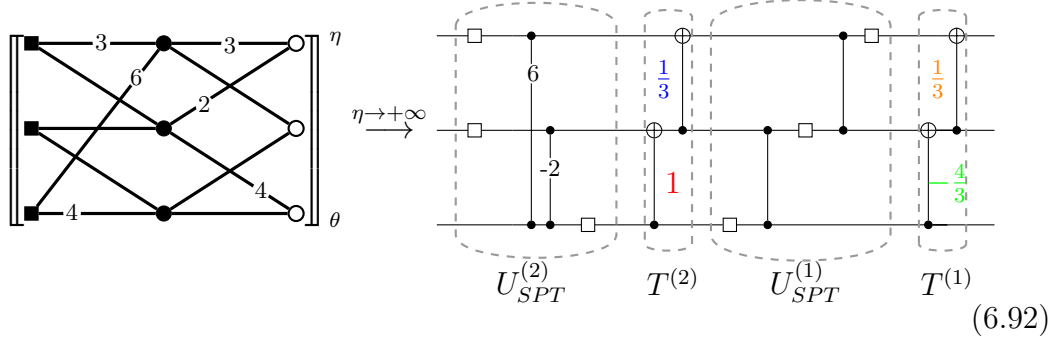
$$G[O'^c, O'] = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 1 & 1 \\ 6 & 0 & 4 \end{pmatrix} \xrightarrow{\begin{array}{l} C_2 \leftarrow C_2 - \frac{1}{3}C_1 \\ C_2 \leftarrow C_2 - C_2 \end{array}} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 6 & -2 & 6 \end{pmatrix} \quad (6.90)$$

Pulling the CX gates into the intermediate circuit,



$$(6.91)$$

The equality is the graphical form of equation 6.81, where each set of CX gates corresponds to a $T^{(k)}$ factor, and each of the open graphs has causal flow thus corresponds to a factor of the form $\mathcal{O}^{(k)}$. To obtain the circuit implemented in the infinite squeezing limit, we perform the SPT of each open graph, and obtain:



$$(6.92)$$

This circuit is in the form claimed in theorem 6.18.

Conclusion and outlook

We have extended the measurement calculus to continuous variables, and defined a flow condition, $\mathbb{R}$ -flow, which is appropriate in this setting. Then, we have shown that MBQCs with $\mathbb{R}$ -flow converge in the infinite squeezing limit.

There are a number of questions we leave for future work. On the practical side of things, we have only shown convergence without considering the actual rate of convergence as a function of squeezing and approximation error. Asking for such a rate is actually not a very well-posed question in general: even in the case of gate teleportation, for a fixed squeezing factor, there are states with arbitrarily

high approximation error. To make any progress, it is necessary to restrict the set of input states to a bounded subset of $\mathcal{H}$, and probably also exert some kind of stronger control on the unitary change-of-basis for the measurement. Any further work therefore must proceed on a case-by-case basis which strongly depends on the implementation under consideration.

On the more theoretical side, many of the questions which were either posed or resolved in the previous chapters are also still open in the CV case. Chief amongst them perhaps is the extension to arbitrary measurement spaces. It is clear how one should define the set of CV measurement spaces, combining definition 2.1 and equation 6.7, but the details still need to be figured out. Such a generalisation would also need to formulate an algorithm similar to chapter 5 in order to prove convergence of the MBQC in the squeezing limit. As for the qudit case, finding a formulation of Pauli $\mathbb{R}$ -flow is also a question which we have not considered.

Finally, it is unclear whether flow conditions would provide a useful tool in MBQC in infinite-dimensional Hilbert spaces beyond the CV model. Weyl-like commutation relations related to topological groups have been extensively studied in the mathematics literature, but as we saw, even in the qudit case, MBQC over groups which are not fields are problematic.

CONCLUSION, OUTLOOK AND UNRESOLVED PROBLEMS

In this thesis, we have extended the measurement calculus to odd prime dimensions and continuous variables. Introducing a class of related flow conditions, we have been able to completely characterise the robustly deterministic MBQC in odd prime dimensions, and constructed algorithms to find a matching reversible quantum circuit that implements the same operation. For continuous variables, we have adapted the circuit extraction algorithm and used it to prove convergence of a large class of MBQCs.

As with all theses, there were many questions that I considered with varying degrees of ambition and various degrees of success. Many of these have not yet been answered, and I list them here. Some of these are the subject of ongoing research, while others I do not know how to attack and merely state in the vain hope that someone else will find a satisfying solution.

Further extensions to $\mathbb{Z}_d$ -flow

Beyond prime fields We have already made the remark that much of our work extends naturally to the case of any finite field $\mathbb{F}$. In fact, the only section where I expect any meaningful complications to arise in this extension is section 3.2, where it is proved that every robustly deterministic $\mathbb{Z}_d$ -MBQC has $\mathbb{Z}_d$ -flow. I expect this proof can be adapted to the general case, but there is some work to be done. Building off this, it should be reasonably straightforward to see that all of our results cover the case of products of finite fields. In particular, this should imply that our results cover all dimensions, in a somewhat convoluted way, since it essentially amounts to viewing a qudit of dimension d as a register of smaller qudits of dimensions p_n where the p_n are the prime factorisation of d .

Generalising further, it seems natural to consider A -flow, where A is any finite abelian group. This amounts to allowing more general kinds of Pauli groups as corrections, which should be given by a representation of a semi-direct product $(A \times A) \rtimes \mathbb{T}$ in the style of Weil [Wei64].

It is well-known that any such group A factors as a finite product of cyclic groups of power-of-prime order. The work in this thesis, combined with the preceding remark about product flows, takes care of any of the factors of the form $\mathbb{Z}_p^n$. What remains are those of the form $\mathbb{Z}_{p^n}$. These groups are far trickier to tackle as there is no nice ring or field structure to use. Already in the case of $\mathbb{Z}_4$ the only non-trivial ring structure is arithmetic modulo 4, which our methods do not treat. This is already a problem at the level of measurement patterns, as equation (2.11) does not hold, and measurement spaces have a more complicated structure.

$\mathbb{Z}_d$ -flow within the qudit ZX calculus There is a natural connection between the ZX-calculus and MBQC, which so far has been exploited only for qubits. Measurement patterns have a very clean representation within the ZX-calculus [DP10], and inversely, oftentimes ZX-diagrams can be interpreted as measurement terms. This has led to the use of $\mathbb{Z}_2$ -flow to extract reversible quantum circuits from such ZX-diagrams [Bac+21], and this is to my knowledge the most general technique for doing so. It has been used extensively as the final step in circuit optimisation algorithms using the ZX-calculus as intermediate representation [Kv20; dBW20; Dun+20]. The connection has also been important for other applications of the ZX-calculus [Hor11; de +20].

The ZX-calculus has recently been generalised to qudits [Wan18; Wan18], and many of the same techniques we developed in this thesis should apply there.

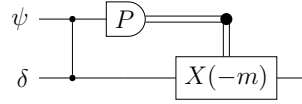
A reasonable CV quantum circuit model

Throughout the chapter on continuous variables, we treated CV quantum circuits as a natural representation for the unitaries appearing in a CV quantum computer. There remain conceptual gaps in interpreting the set of such CV quantum circuits as a computational model. First of all, it is unclear exactly what unitaries can be generated by the gate set of equations (6.13)-(6.15)—is it dense in the unitary group acting on $\mathcal{H}$ as in the qudit case, or not?

Furthermore, in order to obtain a realistic model, it is necessary not just to impose a uniformity condition like in the finite-dimensional case, but also an energy bound since otherwise the model is physically unrealistic. It is also necessary to have some kind of binning on the outcomes of measurements, if one wants to extract outcomes as a digital signal. Having imposed these restrictions, a number of further questions impose themselves. Does the energy bound come at a computational cost to the model? Is there a more natural gate set that allows one to reason without imposing an external energy bound? Finally, it is generally assumed that once such bounds are imposed, the model should be (weakly) efficiently simulable by a finite-dimensional quantum computer, but there are limited actual results in this direction.

A “good” distribution theory for CV quantum information

While it is maybe surprising to be able to prove a convergence result at all for MBQCs, I have to confess some frustration with the results of chapter 6. As described there, the problem of convergence comes from the non-existence of eigenvectors for the position operator. These are typically treated informally in the physics literature as Dirac delta “distributions” which are assumed to preserve all of the algebraic properties of their finite-dimensional counterparts. Such distributions can be formalised in terms of Schwartz generalised functions, and one can show that many properties *do* still hold in a weaker sense. However, this description of distributions is not subtle enough for the types of operations which are at the core of MBQC. Consider the gate teleportation circuit:



In the Schwartz theory, the state $CZ(\psi \otimes \delta)$ is described by a distribution. Evaluating the “branch” corresponding to an outcome $m \in \mathbb{R}$ should formally correspond to taking the inner product of a distribution δ_m with this state. But this inner product is not valid in the Schwartz theory, and so it doesn’t really give a satisfying semantics to the gate teleportation protocol, at least in the way that physicists tend to reason about it.

One work-around for this is to abandon the idea of branches altogether, as we have done in this thesis. The Schwartz theory has recently seen an operational generalisation [KKW16]. Using only the semantics of equation (6.51) in the Stinespring picture, it should be possible to use this theory to give a valid semantics for measurement pattern where the ideal auxiliary state corresponds to a “distributional” operator.

On the other hand, if one wants to make sense of the branch maps at all cost, the only solution seems to be to find a more appropriate distribution theory that allows such products of distributions. Various theories of generalised functions exist which allow this, but it is not obvious which one best applies. Furthermore, they are much less studied than the Schwartz theory, so many of the tools one might like to use simply have not been developed.

LIST OF SYMBOLS

- $\mathbb{N}$ - natural numbers, including 0
- $\mathbb{R}$ - real numbers
- $\mathbb{R}^*$ - non-zero real numbers
- $\mathbb{R}_+$ - non-negative real numbers
- $\mathbb{C}$ - complex numbers
- $\mathbb{T}$ - group of unit complex numbers
- $\mathbb{Z}_d$ - field of integers modulo d (d is always prime)
- $\mathbb{Z}_d^*$ - group of units of $\mathbb{Z}_d$
- $\mathbb{F}^{V \times V}$ - algebra of $V \times V$ matrices over a field $\mathbb{F}$
- $\mathcal{H}, \mathcal{I}, \mathcal{J}$ - Hilbert spaces
- $\mathcal{L}^2(X)$ - Hilbert space of square integrable functions on a measurable space X
- A^c - complement $X \setminus A$ of a set A within some ambient set X ; only used when the ambient set is clear, typically this means $X = V$ the set of vertices of an open $\mathbb{Z}_d$ -graph
- 1_A - column vector whose u -th element is 1 if $u \in A$, 0 otherwise
- $G[A, B]$ - when $G \in \mathbb{F}^{V \times V}$ and $A, B \subseteq V$, the submatrix of G obtained by keeping only the rows corresponding to elements of A and columns corresponding to elements of B

BIBLIOGRAPHY

- [Alb+18] Victor V. Albert et al.
“Performance and Structure of Single-Mode Bosonic Codes”.
In: *Physical Review A* 97.3 (Mar. 2018), p. 032346.
DOI: [10.1103/PhysRevA.97.032346](https://doi.org/10.1103/PhysRevA.97.032346).
- [AU00] Peter M. Alberti and Armin Uhlmann.
“On Bures Distance and *-Algebraic Transition Probability between Inner Derived Positive Linear Forms over W^* -Algebras”.
In: *Acta Applicandae Mathematica* 60.1 (Jan. 2000), pp. 1–37.
DOI: [10.1023/A:1006317508252](https://doi.org/10.1023/A:1006317508252).
- [AL04] Panos Aliferis and Debbie W. Leung.
“Computation by Measurements: A Unifying Picture”.
In: *Physical Review A* 70.6 (Dec. 2004), p. 062314.
DOI: [10.1103/PhysRevA.70.062314](https://doi.org/10.1103/PhysRevA.70.062314).
arXiv: [quant-ph/0404082](https://arxiv.org/abs/quant-ph/0404082).
- [Bac14] Miriam Backens.
“The ZX-calculus Is Complete for Stabilizer Quantum Mechanics”.
In: *New Journal of Physics* 16.9 (Sept. 2014), p. 093021.
DOI: [10.1088/1367-2630/16/9/093021](https://doi.org/10.1088/1367-2630/16/9/093021).
arXiv: [1307.7025](https://arxiv.org/abs/1307.7025).
- [Bac+21] Miriam Backens, Hector Miller-Bakewell, Giovanni de Felice, Leo Lobski, and John van de Wetering.
“There and Back Again: A Circuit Extraction Tale”.
In: *Quantum* 5 (Mar. 2021), p. 421.
DOI: [10.22331/q-2021-03-25-421](https://doi.org/10.22331/q-2021-03-25-421).
- [BB07a] Mohsen Bahramgiri and Salman Beigi.
“An Efficient Algorithm to Recognize Locally Equivalent Graphs in Non-Binary Case”.
In: *arXiv:cs/0702057* (July 2007).
arXiv: [cs/0702057](https://arxiv.org/abs/cs/0702057).
- [BB07b] Mohsen Bahramgiri and Salman Beigi.

- “Graph States Under the Action of Local Clifford Group in Non-Binary Case”.
In: *arXiv:quant-ph/0610267* (June 2007).
arXiv: [quant-ph/0610267](#).
- [BT00] H. Bechmann-Pasquinucci and W. Tittel.
“Quantum Cryptography Using Larger Alphabets”.
In: *Physical Review A* 61.6 (May 2000), p. 062308.
DOI: [10.1103/PhysRevA.61.062308](#).
- [Ben80] Paul Benioff.
“The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines”.
In: *Journal of Statistical Physics* 22.5 (May 1980), pp. 563–591.
DOI: [10.1007/BF01011339](#).
- [Ben82] Paul Benioff.
“Quantum Mechanical Hamiltonian Models of Turing Machines”.
In: *Journal of Statistical Physics* 29.3 (Nov. 1982), pp. 515–546.
DOI: [10.1007/BF01342185](#).
- [Ben+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters.
“Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels”.
In: *Physical Review Letters* 70.13 (Mar. 1993), pp. 1895–1899.
DOI: [10.1103/PhysRevLett.70.1895](#).
- [Ber+17] Juan Bermejo-Vega, Nicolas Delfosse, Dan E. Browne, Cihan Okay, and Robert Raussendorf.
“Contextuality as a Resource for Models of Quantum Computation on Qubits”.
In: *Physical Review Letters* 119.12 (Sept. 2017).
DOI: [10.1103/PhysRevLett.119.120505](#).
arXiv: [1610.08529](#).
- [BV93] Ethan Bernstein and Umesh Vazirani.
“Quantum Complexity Theory”.
In: *Proceedings of the 25th Annual ACM Symposium on Theory of Computing* (1993), p. 63.
- [BB94] André Berthiaume and Gilles Brassard.
“Oracle Quantum Computing”.
In: *Journal of Modern Optics* 41.12 (Dec. 1994), pp. 2521–2535.
DOI: [10.1080/09500349414552351](#).

- [BW08] Rainer Blatt and David Wineland.
“Entangled States of Trapped Atomic Ions”.
In: *Nature* 453.7198 (June 2008), pp. 1008–1015.
DOI: [10.1038/nature07125](https://doi.org/10.1038/nature07125).
- [BG89] Arno Bohm and Manuel Gadella.
Dirac Kets, Gamow Vectors and Gel’fand Triplets.
Vol. 348.
Lecture Notes in Physics.
1989.
- [Boh13] N. Bohr.
“I. On the Constitution of Atoms and Molecules”.
In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 26.151 (July 1913), pp. 1–25.
DOI: [10.1080/14786441308634955](https://doi.org/10.1080/14786441308634955).
- [Boo+21] Robert I. Booth, Aleks Kissinger, Damian Markham, Clément Meignant, and Simon Perdrix.
“Outcome Determinism in Measurement-Based Quantum Computation with Qudits”.
Submitted to *Quantum*, Sept. 2021.
arXiv: [2109.13810](https://arxiv.org/abs/2109.13810).
- [BM21] Robert I. Booth and Damian Markham.
“Flow Conditions for Continuous Variable Measurement-Based Quantum Computing”.
Submitted to *Quantum*, Apr. 2021.
arXiv: [2104.00572](https://arxiv.org/abs/2104.00572).
- [BP21] Robert I. Booth and Simon Perdrix.
“Extracting Reversible Circuits from Measurement-Based Quantum Computations with Higher-Dimensional Systems”.
In preparation, 2021.
- [Bou+97] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger.
“Experimental Quantum Teleportation”.
In: *Nature* 390.6660 (Dec. 1997), pp. 575–579.
DOI: [10.1038/37539](https://doi.org/10.1038/37539).
- [BK98] Samuel L Braunstein and H J Kimble.
“Teleportation of Continuous Quantum Variables”.
In: *Physical Review Letters* 80.4 (1998), p. 4.
DOI: [10.1103/PhysRevLett.80.869](https://doi.org/10.1103/PhysRevLett.80.869).

- [BP03] Samuel L. Braunstein and Arun K. Pati, eds.
Quantum Information with Continuous Variables.
Dordrecht: Springer Netherlands, 2003.
DOI: [10.1007/978-94-015-1258-9](https://doi.org/10.1007/978-94-015-1258-9).
- [Bv05] Samuel L. Braunstein and Peter van Loock.
“Quantum Information with Continuous Variables”.
In: *Reviews of Modern Physics* 77.2 (June 2005), pp. 513–577.
DOI: [10.1103/RevModPhys.77.513](https://doi.org/10.1103/RevModPhys.77.513).
arXiv: [quant-ph/0410100](https://arxiv.org/abs/quant-ph/0410100).
- [Bri+09] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest.
“Measurement-Based Quantum Computation”.
In: *Nature Physics* 5.1 (Jan. 2009), pp. 19–26.
DOI: [10.1038/nphys1157](https://doi.org/10.1038/nphys1157).
arXiv: [0910.1116](https://arxiv.org/abs/0910.1116).
- [BK09] Anne Broadbent and Elham Kashefi.
“Parallelizing Quantum Circuits”.
In: *Theoretical Computer Science* 410.26 (June 2009), pp. 2489–2510.
DOI: [10.1016/j.tcs.2008.12.046](https://doi.org/10.1016/j.tcs.2008.12.046).
- [Bro+07] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix.
“Generalized Flow and Determinism in Measurement-based Quantum Computation”.
In: *New Journal of Physics* 9.8 (Aug. 2007), pp. 250–250.
DOI: [10.1088/1367-2630/9/8/250](https://doi.org/10.1088/1367-2630/9/8/250).
arXiv: [quant-ph/0702212](https://arxiv.org/abs/quant-ph/0702212).
- [BB16] Dan Browne and Hans Briegel.
“One-Way Quantum Computation”.
In: *Quantum Information*.
John Wiley & Sons, Ltd, 2016.
Chap. 21, pp. 449–473.
DOI: [10.1002/9783527805785.ch21](https://doi.org/10.1002/9783527805785.ch21).
- [BKP09] Dan E. Browne, Elham Kashefi, and Simon Perdrix.
“Computational Depth Complexity of Measurement-Based Quantum Computation”.
In: *arXiv:0909.4673 [quant-ph]* (Sept. 2009).
arXiv: [0909.4673 \[quant-ph\]](https://arxiv.org/abs/0909.4673).
- [CG69] K. E. Cahill and R. J. Glauber.
“Density Operators and Quasiprobability Distributions”.

- In: *Physical Review* 177.5 (Jan. 1969), pp. 1882–1902.
DOI: [10.1103/PhysRev.177.1882](#).
- [Cer+02] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin.
“Security of Quantum Key Distribution Using d -Level Systems”.
In: *Physical Review Letters* 88.12 (Mar. 2002), p. 127902.
DOI: [10.1103/PhysRevLett.88.127902](#).
- [Chi93] A. Chi-Chih Yao.
“Quantum Circuit Complexity”.
In: *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*.
Palo Alto, CA, USA: IEEE, 1993,
Pp. 352–361.
DOI: [10.1109/SFCS.1993.366852](#).
- [Cla06] Sean Clark.
“Valence Bond Solid Formalism for D-Level One-Way Quantum Computation”.
In: *Journal of Physics A: Mathematical and General* 39.11 (Mar. 2006),
pp. 2701–2721.
DOI: [10.1088/0305-4470/39/11/010](#).
arXiv: [quant-ph/0512155](#).
- [CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo.
“How to Share a Quantum Secret”.
In: *Physical Review Letters* 83.3 (July 1999), pp. 648–651.
DOI: [10.1103/PhysRevLett.83.648](#).
arXiv: [quant-ph/9901025](#).
- [CD11] Bob Coecke and Ross Duncan.
“Interacting Quantum Observables: Categorical Algebra and Diagrammatics”.
In: *New Journal of Physics* 13.4 (Apr. 2011), p. 043016.
DOI: [10.1088/1367-2630/13/4/043016](#).
arXiv: [0906.4725](#).
- [CK17] Bob Coecke and Aleks Kissinger.
Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning.
Cambridge: Cambridge University Press, 2017.
DOI: [10.1017/9781316219317](#).

- [dGK11] Raphael Dias da Silva, Ernesto F. Galvao, and Elham Kashefi.
“Closed Timelike Curves in Measurement-Based Quantum Computation”.
In: *Physical Review A* 83.1 (Jan. 2011), p. 012316.
DOI: [10.1103/PhysRevA.83.012316](https://doi.org/10.1103/PhysRevA.83.012316).
arXiv: [1003.4971](https://arxiv.org/abs/1003.4971).
- [DK06] Vincent Danos and Elham Kashefi.
“Determinism in the One-Way Model”.
In: *Physical Review A* 74.5 (Nov. 2006), p. 052310.
DOI: [10.1103/PhysRevA.74.052310](https://doi.org/10.1103/PhysRevA.74.052310).
- [DKP07] Vincent Danos, Elham Kashefi, and Prakash Panangaden.
“The Measurement Calculus”.
In: *Journal of the ACM* 54.2 (Apr. 2007), 8–es.
DOI: [10.1145/1219092.1219096](https://doi.org/10.1145/1219092.1219096).
- [Dan+09] Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix.
“Extended Measurement Calculus”.
In: *Semantic Techniques in Quantum Computation*.
Ed. by Ian Mackie and Simon Gay.
Cambridge: Cambridge University Press, 2009,
Pp. 235–310.
DOI: [10.1017/CB09781139193313.008](https://doi.org/10.1017/CB09781139193313.008).
- [DG28] C. J. Davisson and L. H. Germer.
“Reflection of Electrons by a Crystal of Nickel”.
In: *Proceedings of the National Academy of Sciences* 14.4 (Apr. 1928),
pp. 317–322.
DOI: [10.1073/pnas.14.4.317](https://doi.org/10.1073/pnas.14.4.317).
- [de 08] Niel de Beaudrap.
“Finding Flows in the One-Way Measurement Model”.
In: *Physical Review A* 77.2 (Feb. 2008), p. 022328.
DOI: [10.1103/PhysRevA.77.022328](https://doi.org/10.1103/PhysRevA.77.022328).
arXiv: [quant-ph/0611284](https://arxiv.org/abs/quant-ph/0611284).
- [de 12] Niel de Beaudrap.
“A Linearized Stabilizer Formalism for Systems of Finite Dimension”.
In: *arXiv:1102.3354 [quant-ph]* (Sept. 2012).
arXiv: [1102.3354 \[quant-ph\]](https://arxiv.org/abs/1102.3354).
- [dBW20] Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang.
“Fast and Effective Techniques for T-count Reduction via Spider Nest Identities”.

- In: *arXiv:2004.05164 [quant-ph]* (Apr. 2020).
arXiv: [2004.05164 \[quant-ph\]](#).
- [de +20] Niel de Beaudrap, Ross Duncan, Dominic Horsman, and Simon Perdrix.
“Pauli Fusion: A Computational Model to Realise Quantum Transformations from ZX Terms”.
In: *Electronic Proceedings in Theoretical Computer Science* 318. Proceedings QPL 2019 (Apr. 2020), pp. 85–105.
DOI: [10.4204/EPTCS.318](#).
arXiv: [1904.12817](#).
- [de 17] Maurice de Gosson.
The Wigner Transform.
WORLD SCIENTIFIC (EUROPE), May 2017.
DOI: [10.1142/q0089](#).
- [de 06] Maurice A. de Gosson.
Symplectic Geometry and Quantum Mechanics.
Advances in Partial Differential Equations.
Birkhäuser Basel, 2006.
DOI: [10.1007/3-7643-7575-2](#).
- [de 18] Maurice A. de Gosson.
“Quantum Harmonic Analysis of the Density Matrix”.
In: *Quanta* 7.1 (Sept. 2018), p. 74.
DOI: [10.12743/quanta.v7i1.74](#).
arXiv: [1703.00889](#).
- [Deu85] D. Deutsch.
“Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer”.
In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 400.1818 (July 1985), pp. 97–117.
DOI: [10.1098/rspa.1985.0070](#).
- [DJ92] David Deutsch and Richard Jozsa.
“Rapid Solution of Problems by Quantum Computation”.
In: *Proc. R. Soc. Lond. A* 439.1907 (Dec. 1992), pp. 553–558.
DOI: [10.1098/rspa.1992.0167](#).
- [DF26] Paul Adrien Maurice Dirac and Ralph Howard Fowler.
“On the Theory of Quantum Mechanics”.
In: *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character* 112.762 (Oct. 1926), pp. 661–677.

- DOI: [10.1098/rspa.1926.0133](https://doi.org/10.1098/rspa.1926.0133).
- [Dun+20] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John van de Wetering.
“Graph-Theoretic Simplification of Quantum Circuits with the ZX-calculus”.
In: *Quantum* 4 (June 2020), p. 279.
DOI: [10.22331/q-2020-06-04-279](https://doi.org/10.22331/q-2020-06-04-279).
arXiv: [1902.03178](https://arxiv.org/abs/1902.03178).
- [DP10] Ross Duncan and Simon Perdrix.
“Rewriting Measurement-Based Quantum Computations with Generalised Flow”.
In: *Automata, Languages and Programming*.
Ed. by David Hutchison et al.
Vol. 6199.
Berlin, Heidelberg: Springer Berlin Heidelberg, 2010,
Pp. 285–296.
DOI: [10.1007/978-3-642-14162-1_24](https://doi.org/10.1007/978-3-642-14162-1_24).
- [Ein05] A. Einstein.
“Über Einen Die Erzeugung Und Verwandlung Des Lichtes Betreffenden Heuristischen Gesichtspunkt”.
In: *Annalen der Physik* 322.6 (1905), pp. 132–148.
DOI: [10.1002/andp.19053220607](https://doi.org/10.1002/andp.19053220607).
- [ESP02] J. Eisert, S. Scheel, and M. B. Plenio.
“Distilling Gaussian States with Gaussian Operations Is Impossible”.
In: *Physical Review Letters* 89.13 (Sept. 2002), p. 137903.
DOI: [10.1103/PhysRevLett.89.137903](https://doi.org/10.1103/PhysRevLett.89.137903).
arXiv: [quant-ph/0204052](https://arxiv.org/abs/quant-ph/0204052).
- [Erh+18] Manuel Erhard, Robert Fickler, Mario Krenn, and Anton Zeilinger.
“Twisted Photons: New Quantum Perspectives in High Dimensions”.
In: *Light: Science & Applications* 7.3 (Mar. 2018), pp. 17146–17146.
DOI: [10.1038/lsa.2017.146](https://doi.org/10.1038/lsa.2017.146).
- [FT20] Claude Fabre and Nicolas Treps.
“Modes and States in Quantum Optics”.
In: *Reviews of Modern Physics* 92.3 (Sept. 2020), p. 035005.
DOI: [10.1103/RevModPhys.92.035005](https://doi.org/10.1103/RevModPhys.92.035005).
arXiv: [1912.09321](https://arxiv.org/abs/1912.09321).
- [FRB18] Markus Frembs, Sam Roberts, and Stephen D. Bartlett.
“Contextuality as a Resource for Measurement-Based Quantum Computation beyond Qubits”.

- In: *arXiv:1804.07364 [quant-ph]* (Apr. 2018).
arXiv: [1804.07364 \[quant-ph\]](#).
- [Fri+18] Nicolai Friis et al.
“Observation of Entangled States of a Fully Controlled 20-Qubit System”.
In: *Physical Review X* 8.2 (Apr. 2018), p. 021012.
DOI: [10.1103/PhysRevX.8.021012](#).
arXiv: [1711.11092](#).
- [FAF20] Kosuke Fukui, Warit Asavanant, and Akira Furusawa.
“Temporal-Mode Continuous-Variable 3-Dimensional Cluster State for Topologically-Protected Measurement-Based Quantum Computation”.
In: *Physical Review A* 102.3 (Sept. 2020), p. 032614.
DOI: [10.1103/PhysRevA.102.032614](#).
arXiv: [2004.05750](#).
- [Gao+19] Xiaoqin Gao, Mario Krenn, Jaroslav Kysela, and Anton Zeilinger.
“Arbitrary d -Dimensional Pauli X Gates of a Flying Qudit”.
In: *Physical Review A* 99.2 (Feb. 2019), p. 023825.
DOI: [10.1103/PhysRevA.99.023825](#).
- [Gok+19] Pranav Gokhale, Jonathan M. Baker, Casey Duckering, Natalie C. Brown, Kenneth R. Brown, and Frederic T. Chong.
“Asymptotic Improvements to Quantum Circuits via Qutrits”.
In: *Proceedings of the 46th International Symposium on Computer Architecture*.
Phoenix Arizona: ACM, June 2019,
Pp. 554–566.
DOI: [10.1145/3307650.3322253](#).
- [Got99] Daniel Gottesman.
“Fault-Tolerant Quantum Computation with Higher-Dimensional Systems”.
In: *Chaos, Solitons & Fractals* 10.10 (Sept. 1999), pp. 1749–1758.
DOI: [10.1016/S0960-0779\(98\)00218-5](#).
arXiv: [quant-ph/9802007](#).
- [GC99] Daniel Gottesman and Isaac L. Chuang.
“Demonstrating the Viability of Universal Quantum Computation Using Teleportation and Single-Qubit Operations”.
In: *Nature* 402.6760 (Nov. 1999), pp. 390–393.
DOI: [10.1038/46503](#).
- [GKP01] Daniel Gottesman, Alexei Kitaev, and John Preskill.

- “Encoding a Qubit in an Oscillator”.
In: *Physical Review A* 64.1 (June 2001).
DOI: [10.1103/PhysRevA.64.012310](https://doi.org/10.1103/PhysRevA.64.012310).
arXiv: [quant-ph/0008040](https://arxiv.org/abs/quant-ph/0008040).
- [Gro96] Lov K. Grover.
“A Fast Quantum Mechanical Algorithm for Database Search”.
In: *arXiv:quant-ph/9605043* (May 1996).
arXiv: [quant-ph/9605043](https://arxiv.org/abs/quant-ph/9605043).
- [Gu+09] Mile Gu, Christian Weedbrook, Nicolas C. Menicucci, Timothy C. Ralph, and Peter van Loock.
“Quantum Computing with Continuous-Variable Clusters”.
In: *Physical Review A* 79.6 (June 2009).
DOI: [10.1103/PhysRevA.79.062318](https://doi.org/10.1103/PhysRevA.79.062318).
arXiv: [0903.3233](https://arxiv.org/abs/0903.3233).
- [Hal13] Brian C. Hall.
Quantum Theory for Mathematicians.
Graduate Texts in Mathematics.
New York: Springer-Verlag, 2013.
- [Hao+21] Shuhong Hao, Meihong Wang, Dong Wang, and Xiaolong Su.
“Topological Error Correction with a Gaussian Cluster State”.
In: *Physical Review A* 103.5 (May 2021), p. 052407.
DOI: [10.1103/PhysRevA.103.052407](https://doi.org/10.1103/PhysRevA.103.052407).
- [Hay17] Masahito Hayashi.
A Group Theoretic Approach to Quantum Information.
Springer International Publishing, 2017.
DOI: [10.1007/978-3-319-45241-8](https://doi.org/10.1007/978-3-319-45241-8).
- [Hei25] Werner Heisenberg.
“Über Quantentheoretische Umdeutung Kinematischer Und Mechanischer Beziehungen”.
In: *Zeitschrift für Physik volume 33* (1925), pp. 879–893.
- [Hol01] A. S. Holevo.
Statistical Structure of Quantum Theory.
Lecture Notes in Physics. New Series m, Monographs 67.
Berlin ; New York: Springer, 2001.
- [Hor11] Dominic Horsman.
“Quantum Pictorialism for Topological Cluster-State Computing”.
In: *New Journal of Physics* 13.9 (Sept. 2011), p. 095011.
DOI: [10.1088/1367-2630/13/9/095011](https://doi.org/10.1088/1367-2630/13/9/095011).

- arXiv: [1101.4722](#).
- [HQ12] JinChuan Hou and XiaoFei Qi.
 “Fidelity of States in Infinite-Dimensional Quantum Systems”.
 In: *Science China Physics, Mechanics and Astronomy* 55.10 (Oct. 2012), pp. 1820–1827.
 DOI: [10.1007/s11433-012-4840-4](#).
- [JPV17] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart.
 “A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics”.
 In: *arXiv:1705.11151 [quant-ph]* (May 2017).
 arXiv: [1705.11151 \[quant-ph\]](#).
- [JP05] Philippe Jorrand and Simon Perdrix.
 “Unifying Quantum Computation with Projective Measurements Only and One-Way Quantum Computation”.
 In: *arXiv:quant-ph/0404125* (June 2005), p. 44.
 DOI: [10.1117/12.620302](#).
 arXiv: [quant-ph/0404125](#).
- [KKW16] Michael Keyl, Jukka Kiukas, and Reinhard F. Werner.
 “Schwartz Operators”.
 In: *Reviews in Mathematical Physics* 28.03 (Apr. 2016), p. 1630001.
 DOI: [10.1142/S0129055X16300016](#).
 arXiv: [1503.04086](#).
- [Kik+20] E. O. Kiktenko, A. S. Nikolaeva, Peng Xu, G. V. Shlyapnikov, and A. K. Fedorov.
 “Scalable Quantum Computing with Qudits on a Graph”.
 In: *Physical Review A* 101.2 (Feb. 2020), p. 022304.
 DOI: [10.1103/PhysRevA.101.022304](#).
 arXiv: [1909.08973](#).
- [Kv20] Aleks Kissinger and John van de Wetering.
 “Reducing T-count with the ZX-calculus”.
 In: *arXiv:1903.10477 [quant-ph]* (Jan. 2020).
 arXiv: [1903.10477 \[quant-ph\]](#).
- [Kli+03] A. B. Klimov, R. Guzmán, J. C. Retamal, and C. Saavedra.
 “Qutrit Quantum Computer with Trapped Ions”.
 In: *Physical Review A* 67.6 (June 2003), p. 062313.
 DOI: [10.1103/PhysRevA.67.062313](#).

- [Kon+21a] Shunya Konno, Warit Asavanant, Kosuke Fukui, Atsushi Sakaguchi, Fumiya Hanamura, Petr Marek, Radim Filip, Jun-ichi Yoshikawa, and Akira Furusawa.
“Non-Clifford Gate on Optical Qubits by Nonlinear Feedforward”.
In: *arXiv:2103.10644 [quant-ph]* (Aug. 2021).
arXiv: [2103.10644 \[quant-ph\]](#).
- [Kon+21b] Shunya Konno, Atsushi Sakaguchi, Warit Asavanant, Hisashi Ogawa, Masaya Kobayashi, Petr Marek, Radim Filip, Jun-ichi Yoshikawa, and Akira Furusawa.
“Nonlinear Squeezing for Measurement-Based Non-Gaussian Operations in Time Domain”.
In: *Physical Review Applied* 15.2 (Feb. 2021), p. 024024.
DOI: [10.1103/PhysRevApplied.15.024024](#).
arXiv: [2011.14576](#).
- [Kra83] Karl Kraus.
States, Effects, and Operations: Fundamental Notions of Quantum Theory.
Ed. by Arno Bohm.
Lecture Notes in Physics 190.
Berlin Heidelberg: Springer, 1983.
- [Leu02] D. W. Leung.
“Two-Qubit Projective Measurements Are Universal for Quantum Computation”.
In: *arXiv:quant-ph/0111122* (Apr. 2002).
arXiv: [quant-ph/0111122](#).
- [Leu04] Debbie W. Leung.
“Quantum Computation by Measurements”.
In: *arXiv:quant-ph/0310189* (Feb. 2004).
arXiv: [quant-ph/0310189](#).
- [Lig58] M. J. Lighthill.
An Introduction to Fourier Analysis and Generalised Functions.
London: Cambridge University Press, 1958.
- [LB99] Seth Lloyd and Samuel L. Braunstein.
“Quantum Computation over Continuous Variables”.
In: *Physical Review Letters* 82.8 (Feb. 1999), pp. 1784–1787.
DOI: [10.1103/PhysRevLett.82.1784](#).
arXiv: [quant-ph/9810082](#).
- [LDR15] Leon Loveridge, Raouf Dridi, and Robert Raussendorf.

- “Topos Logic in Measurement-Based Quantum Computation”.
In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 471.2176 (Apr. 2015), p. 20140716.
DOI: [10.1098/rspa.2014.0716](https://doi.org/10.1098/rspa.2014.0716).
arXiv: [1408.0745](https://arxiv.org/abs/1408.0745).
- [Man+17] Atul Mantri, Tommaso F. Demarie, Nicolas C. Menicucci, and Joseph F. Fitzsimons.
“Flow Ambiguity: A Path Towards Classically Driven Blind Quantum Computation”.
In: *Physical Review X* 7.3 (July 2017).
DOI: [10.1103/PhysRevX.7.031004](https://doi.org/10.1103/PhysRevX.7.031004).
arXiv: [1608.04633](https://arxiv.org/abs/1608.04633).
- [MMP13] Anne Marin, Damian Markham, and Simon Perdrix.
“Access Structure in Graphs in High Dimension and Application to Secret Sharing”.
In: (2013), 17 pages.
DOI: [10.4230/LIPICS.TQC.2013.308](https://doi.org/10.4230/LIPICS.TQC.2013.308).
- [MK14] Damian Markham and Elham Kashefi.
“Entanglement, Flow and Classical Simulatability in Measurement Based Quantum Computation”.
In: *Horizons of the Mind. A Tribute to Prakash Panangaden: Essays Dedicated to Prakash Panangaden on the Occasion of His 60th Birthday*.
Ed. by Franck van Breugel, Elham Kashefi, Catuscia Palamidessi, and Jan Rutten.
Lecture Notes in Computer Science.
Cham: Springer International Publishing, 2014,
Pp. 427–453.
DOI: [10.1007/978-3-319-06880-0_22](https://doi.org/10.1007/978-3-319-06880-0_22).
- [Max61] J.C. Maxwell.
“On Physical Lines of Force”.
In: *Philosophical Magazine* 4 (1861), pp. 12–24.
DOI: [10.1080/14786431003659180](https://doi.org/10.1080/14786431003659180).
- [Men14] Nicolas C. Menicucci.
“Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States”.
In: *Physical Review Letters* 112.12 (Mar. 2014), p. 120504.
DOI: [10.1103/PhysRevLett.112.120504](https://doi.org/10.1103/PhysRevLett.112.120504).
- [MFv11] Nicolas C. Menicucci, Steven T. Flammia, and Peter van Loock.

- “Graphical Calculus for Gaussian Pure States”.
In: *Physical Review A* 83.4 (Apr. 2011).
DOI: [10.1103/PhysRevA.83.042335](https://doi.org/10.1103/PhysRevA.83.042335).
arXiv: [1007.0725](https://arxiv.org/abs/1007.0725).
- [Men+06] Nicolas C. Menicucci, Peter van Loock, Mile Gu, Christian Weedbrook, Timothy C. Ralph, and Michael A. Nielsen.
“Universal Quantum Computation with Continuous-Variable Cluster States”.
In: *Physical Review Letters* 97.11 (Sept. 2006).
DOI: [10.1103/PhysRevLett.97.110501](https://doi.org/10.1103/PhysRevLett.97.110501).
arXiv: [quant-ph/0605198](https://arxiv.org/abs/quant-ph/0605198).
- [MP08] Mehdi Mhalla and Simon Perdrix.
“Finding Optimal Flows Efficiently”.
In: *Automata, Languages and Programming*.
Ed. by Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfssdóttir, and Igor Walukiewicz.
Lecture Notes in Computer Science.
Berlin, Heidelberg: Springer, 2008,
Pp. 857–868.
DOI: [10.1007/978-3-540-70575-8_70](https://doi.org/10.1007/978-3-540-70575-8_70).
- [Mic+16] Marios H. Michael, Matti Silveri, R. T. Brierley, Victor V. Albert, Juha Salmilehto, Liang Jiang, and S. M. Girvin.
“New Class of Quantum Error-Correcting Codes for a Bosonic Mode”.
In: *Physical Review X* 6.3 (July 2016), p. 031006.
DOI: [10.1103/PhysRevX.6.031006](https://doi.org/10.1103/PhysRevX.6.031006).
- [Miy+16] Kazunori Miyata, Hisashi Ogawa, Petr Marek, Radim Filip, Hidehiro Yonezawa, Jun-ichi Yoshikawa, and Akira Furusawa.
“Implementation of a Quantum Cubic Gate by Adaptive Non-Gaussian Measurement”.
In: *Physical Review A* 93.2 (Feb. 2016), p. 022301.
DOI: [10.1103/PhysRevA.93.022301](https://doi.org/10.1103/PhysRevA.93.022301).
arXiv: [1507.08782](https://arxiv.org/abs/1507.08782).
- [MHM15] Jisho Miyazaki, Michal Hajdušek, and Mio Murao.
“An Analysis of the Trade-off between Spatial and Temporal Resources for Measurement-Based Quantum Computation”.
In: *Physical Review A* 91.5 (May 2015), p. 052302.
DOI: [10.1103/PhysRevA.91.052302](https://doi.org/10.1103/PhysRevA.91.052302).
arXiv: [1310.4043](https://arxiv.org/abs/1310.4043).
- [Mor17] Valter Moretti.

- Spectral Theory and Quantum Mechanics: Mathematical Foundations of Quantum Theories, Symmetries and Introduction to the Algebraic Formulation.*
Second.
La Matematica per Il 3+2.
Springer International Publishing, 2017.
DOI: [10.1007/978-3-319-70706-8](https://doi.org/10.1007/978-3-319-70706-8).
- [MN36] F. J. Murray and J. v. Neumann.
“On Rings of Operators”.
In: *Annals of Mathematics* 37.1 (1936), pp. 116–229.
DOI: [10.2307/1968693](https://doi.org/10.2307/1968693).
- [Nee+09] Matthew Neeley et al.
“Emulation of a Quantum Spin with a Superconducting Phase Qudit”.
In: *Science* 325.5941 (Aug. 2009), pp. 722–725.
DOI: [10.1126/science.1173440](https://doi.org/10.1126/science.1173440).
- [NW17] Kang Feng Ng and Quanlong Wang.
“A Universal Completion of the ZX-calculus”.
In: *arXiv:1706.09877 [quant-ph]* (June 2017).
arXiv: [1706.09877 \[quant-ph\]](https://arxiv.org/abs/1706.09877).
- [NC10] M.A. Nielsen and I.L. Chuang.
Quantum Computation and Quantum Information: 10th Anniversary Edition.
Cambridge University Press, 2010.
- [Nie03] Michael A. Nielsen.
“Universal Quantum Computation Using Only Projective Measurement, Quantum Memory, and Preparation of the 0 State”.
In: *Physics Letters A* 308.2-3 (Feb. 2003), pp. 96–100.
DOI: [10.1016/S0375-9601\(02\)01803-0](https://doi.org/10.1016/S0375-9601(02)01803-0).
arXiv: [quant-ph/0108020](https://arxiv.org/abs/quant-ph/0108020).
- [Nie06] Michael A. Nielsen.
“Cluster-State Quantum Computation”.
In: *Reports on Mathematical Physics* 57.1 (Feb. 2006), pp. 147–161.
DOI: [10.1016/S0034-4877\(06\)80014-5](https://doi.org/10.1016/S0034-4877(06)80014-5).
arXiv: [quant-ph/0504097](https://arxiv.org/abs/quant-ph/0504097).
- [NFC09] Julien Niset, Jaromír Fiurášek, and Nicolas J. Cerf.
“No-Go Theorem for Gaussian Quantum Error Correction”.
In: *Physical Review Letters* 102.12 (Mar. 2009), p. 120501.
DOI: [10.1103/PhysRevLett.102.120501](https://doi.org/10.1103/PhysRevLett.102.120501).

- [NGJ20] Kyungjoo Noh, S. M. Girvin, and Liang Jiang.
“Encoding an Oscillator into Many Oscillators”.
In: *Physical Review Letters* 125.8 (Aug. 2020), p. 080503.
DOI: [10.1103/PhysRevLett.125.080503](https://doi.org/10.1103/PhysRevLett.125.080503).
arXiv: [1903.12615](https://arxiv.org/abs/1903.12615).
- [Pea08] K.A. Peacock.
The Quantum Revolution: A Historical Perspective.
Greenwood Guides to Great Ideas in Science.
Greenwood Press, 2008.
- [Per05] Simon Perdrix.
“State Transfer Instead of Teleportation in Measurement-based Quantum Computation”.
In: *International Journal of Quantum Information* 03.01 (Mar. 2005), pp. 219–223.
DOI: [10.1142/S0219749905000785](https://doi.org/10.1142/S0219749905000785).
arXiv: [quant-ph/0402204](https://arxiv.org/abs/quant-ph/0402204).
- [Per06] Simon Perdrix.
“Modèles formels du calcul quantique: ressources, machines abstraites et calcul par mesure”.
PhD thesis. Institut National Polytechnique de Grenoble, Dec. 2006.
- [PSM] Simon Perdrix, Luc Sanselme, and Mehdi Mhalla.
“Characterising Determinism in MBQCs Involving Pauli Measurements”.
To Appear.
- [PLB18] Stefano Pirandola, Riccardo Laurenza, and Samuel L. Braunstein.
“Teleportation Simulation of Bosonic Gaussian Channels: Strong and Uniform Convergence”.
In: *The European Physical Journal D* 72.9 (Sept. 2018), p. 162.
DOI: [10.1140/epjd/e2018-90253-1](https://doi.org/10.1140/epjd/e2018-90253-1).
arXiv: [1712.01615](https://arxiv.org/abs/1712.01615).
- [Pla01] Max Planck.
“Ueber Das Gesetz Der Energieverteilung Im Normalspectrum”.
In: *Annalen der Physik* 309.3 (1901), pp. 553–563.
DOI: [10.1002/andp.19013090310](https://doi.org/10.1002/andp.19013090310).
- [RBB03] R. Raussendorf, D. E. Browne, and H. J. Briegel.
“Measurement-Based Quantum Computation with Cluster States”.
In: *Physical Review A* 68.2 (Aug. 2003).
DOI: [10.1103/PhysRevA.68.022312](https://doi.org/10.1103/PhysRevA.68.022312).
arXiv: [quant-ph/0301052](https://arxiv.org/abs/quant-ph/0301052).

- [RHG06] R. Raussendorf, J. Harrington, and K. Goyal.
“A Fault-Tolerant One-Way Quantum Computer”.
In: *Annals of Physics* 321.9 (Sept. 2006), pp. 2242–2270.
DOI: [10.1016/j.aop.2006.01.012](https://doi.org/10.1016/j.aop.2006.01.012).
- [Rau+11] R. Raussendorf, P. Sarvepalli, T.-C. Wei, and P. Haghnegahdar.
“Measurement-Based Quantum Computation—a Quantum-Mechanical Toy Model for Spacetime?”
In: *arXiv:1108.5774 [quant-ph]* (Aug. 2011).
arXiv: [1108.5774 \[quant-ph\]](https://arxiv.org/abs/1108.5774).
- [Rau13] Robert Raussendorf.
“Contextuality in Measurement-based Quantum Computation”.
In: *Physical Review A* 88.2 (Aug. 2013), p. 022322.
DOI: [10.1103/PhysRevA.88.022322](https://doi.org/10.1103/PhysRevA.88.022322).
arXiv: [0907.5449](https://arxiv.org/abs/0907.5449).
- [RB01] Robert Raussendorf and Hans J. Briegel.
“A One-Way Quantum Computer”.
In: *Physical Review Letters* 86.22 (May 2001), pp. 5188–5191.
DOI: [10.1103/PhysRevLett.86.5188](https://doi.org/10.1103/PhysRevLett.86.5188).
- [RB02] Robert Raussendorf and Hans J. Briegel.
“Computational Model Underlying the One-Way Quantum Computer”.
In: *Quantum Info. Comput.* 2.6 (Oct. 2002), pp. 443–486.
DOI: [10.5555/2011492.2011495](https://doi.org/10.5555/2011492.2011495).
- [RBB02] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel.
“The One-Way Quantum Computer - a Non-Network Model of Quantum Computation”.
In: *Journal of Modern Optics* 49.8 (July 2002), pp. 1299–1306.
DOI: [10.1080/09500340110107487](https://doi.org/10.1080/09500340110107487).
arXiv: [quant-ph/0108118](https://arxiv.org/abs/quant-ph/0108118).
- [Rei+19] Christian Reimer et al.
“High-Dimensional One-Way Quantum Processing Implemented on d-Level Cluster States”.
In: *Nature Physics* 15.2 (Feb. 2019), pp. 148–153.
DOI: [10.1038/s41567-018-0347-x](https://doi.org/10.1038/s41567-018-0347-x).
- [SP17] Luc Sanselme and Simon Perdrix.
“Determinism and Computational Power of Real Measurement-Based Quantum Computation”.
In: *Fundamentals of Computation Theory*.
Ed. by Ralf Klasing and Marc Zeitoun.

- Vol. 10472.
Berlin, Heidelberg: Springer Berlin Heidelberg, 2017,
Pp. 395–408.
DOI: [10.1007/978-3-662-55751-8_31](https://doi.org/10.1007/978-3-662-55751-8_31).
- [SK17a] Adam Sawicki and Katarzyna Karnas.
“Criteria for Universality of Quantum Gates”.
In: *Physical Review A* 95.6 (June 2017), p. 062303.
DOI: [10.1103/PhysRevA.95.062303](https://doi.org/10.1103/PhysRevA.95.062303).
arXiv: [1610.00547](https://arxiv.org/abs/1610.00547).
- [SK17b] Adam Sawicki and Katarzyna Karnas.
“Universality of Single Qudit Gates”.
In: *Annales Henri Poincaré* 18.11 (Nov. 2017), pp. 3515–3552.
DOI: [10.1007/s00023-017-0604-z](https://doi.org/10.1007/s00023-017-0604-z).
arXiv: [1609.05780](https://arxiv.org/abs/1609.05780).
- [Sch26] Erwin Schrödinger.
“Quantisierung Als Eigenwertproblem”.
In: *Annalen der Physik* 79 (1926), pp. 361–376.
- [Sch95] Benjamin Schumacher.
“Quantum Coding”.
In: *Physical Review A* 51.4 (Apr. 1995), pp. 2738–2747.
DOI: [10.1103/PhysRevA.51.2738](https://doi.org/10.1103/PhysRevA.51.2738).
- [Sch50] Laurent Schwartz.
Théorie Des Distributions.
Publications de l’Institut de Mathématique de l’Université de Strasbourg.
1950.
- [SW20] Kunal Sharma and Mark M. Wilde.
“Characterizing the Performance of Continuous-Variable Gaussian Quantum Gates”.
In: *Physical Review Research* 2.1 (Feb. 2020), p. 013126.
DOI: [10.1103/PhysRevResearch.2.013126](https://doi.org/10.1103/PhysRevResearch.2.013126).
arXiv: [1810.12335](https://arxiv.org/abs/1810.12335).
- [SS10] Lana Sheridan and Valerio Scarani.
“Security Proof for Quantum Key Distribution Using Qudit Systems”.
In: *Physical Review A* 82.3 (Sept. 2010), p. 030301.
DOI: [10.1103/PhysRevA.82.030301](https://doi.org/10.1103/PhysRevA.82.030301).
- [SCC19] Yunong Shi, Christopher Chamberland, and Andrew W. Cross.
“Fault-Tolerant Preparation of Approximate GKP States”.

- In: *New Journal of Physics* 21.9 (Sept. 2019), p. 093007.
DOI: [10.1088/1367-2630/ab3a62](#).
arXiv: [1905.00903](#).
- [SH08] M. E. Shirokov and A. S. Holevo.
“On Approximation of Infinite-Dimensional Quantum Channels”.
In: *Problems of Information Transmission* 44.2 (June 2008), pp. 73–90.
DOI: [10.1134/S0032946008020014](#).
- [Sho94] P.W. Shor.
“Algorithms for Quantum Computation: Discrete Logarithms and Factoring”.
In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*.
Nov. 1994,
Pp. 124–134.
DOI: [10.1109/SFCS.1994.365700](#).
- [Sho97] Peter W. Shor.
“Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”.
In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509.
DOI: [10.1137/S0097539795293172](#).
arXiv: [quant-ph/9508027](#).
- [Sim21] Will Simmons.
“Relating Measurement Patterns to Circuits via Pauli Flow”.
In: *Electronic Proceedings in Theoretical Computer Science* 343 (Sept. 2021), pp. 50–101.
DOI: [10.4204/EPTCS.343.4](#).
arXiv: [2109.05654](#).
- [Sti55] W. Forrest Stinespring.
“Positive Functions on C^* -Algebras”.
In: *Proceedings of the American Mathematical Society* 6.2 (Apr. 1955), p. 211.
DOI: [10.2307/2032342](#).
- [SWB18] Daiqin Su, Christian Weedbrook, and Kamil Brádler.
“Correcting Finite Squeezing Errors in Continuous-Variable Cluster States”.
In: *arXiv:1801.03488 [quant-ph]* (Jan. 2018).
arXiv: [1801.03488 \[quant-ph\]](#).

- [Tur36] Alan M. Turing.
“On Computable Numbers, with an Application to the Entscheidungsproblem”.
In: *Proceedings of the London Mathematical Society*. 2nd ser. 42 (Nov. 1936), pp. 230–265.
- [Uhl76] Armin Uhlmann.
“The “Transition Probability” in the State Space of a $\ast$ -Algebra”.
In: *Reports on Mathematical Physics* 9.2 (Apr. 1976), pp. 273–279.
DOI: [10.1016/0034-4877\(76\)90060-4](https://doi.org/10.1016/0034-4877(76)90060-4).
- [van20] John van de Wetering.
“ZX-calculus for the Working Quantum Computer Scientist”.
In: *arXiv:2012.13966 [quant-ph]* (Dec. 2020).
arXiv: [2012.13966 \[quant-ph\]](https://arxiv.org/abs/2012.13966).
- [Vil19] Renaud Vilmart.
“ZX-Calculi for Quantum Computing and Their Completeness”.
PhD thesis. Université de Lorraine, Sept. 2019.
- [von30] J. von Neumann.
“Allgemeine Eigenwerttheorie Hermitescher Funktionaloperatoren”.
In: *Mathematische Annalen* 102.1 (Dec. 1930), pp. 49–131.
DOI: [10.1007/BF01782338](https://doi.org/10.1007/BF01782338).
- [von27] John von Neumann.
“Mathematische Begründung der Quantenmechanik”.
In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen* (1927), pp. 1–57.
- [von32] John von Neumann.
Mathematische Grundlagen der Quantenmechanik.
Berlin: J. Springer, 1932.
- [von18] John von Neumann.
Mathematical Foundations of Quantum Mechanics.
Ed. by Nicholas Wheeler and Robert T. Beyer.
Princeton University Press, 2018.
- [Vui+19] Christophe Vuillot, Hamed Asasi, Yang Wang, Leonid P. Pryadko, and Barbara M. Terhal.
“Quantum Error Correction with the Toric-GKP Code”.
In: *Physical Review A* 99.3 (Mar. 2019), p. 032344.
DOI: [10.1103/PhysRevA.99.032344](https://doi.org/10.1103/PhysRevA.99.032344).
arXiv: [1810.00047](https://arxiv.org/abs/1810.00047).
- [Wan18] Quanlong Wang.

- “Qutrit ZX-calculus Is Complete for Stabilizer Quantum Mechanics”.
In: *Electronic Proceedings in Theoretical Computer Science* 266 (Feb. 2018), pp. 58–70.
DOI: [10.4204/EPTCS.266.3](#).
arXiv: [1803.00696](#).
- [Wan21] Quanlong Wang.
“Qufinite ZX-calculus: A Unified Framework of Qudit ZX-calculi”.
In: *arXiv:2104.06429 [quant-ph]* (Apr. 2021).
arXiv: [2104.06429 \[quant-ph\]](#).
- [Wan+20] Yuchen Wang, Zixuan Hu, Barry C. Sanders, and Sabre Kais.
“Qudits and High-Dimensional Quantum Computing”.
In: *Frontiers in Physics* 8 (2020).
DOI: [10.3389/fphy.2020.589504](#).
- [Wei64] André Weil.
“Sur certains groupes d’opérateurs unitaires”.
In: *Acta Mathematica* 111 (1964), pp. 143–211.
DOI: [10.1007/BF02391012](#).
- [WZ15] Richard L. Wheeden and Antoni Zygmund.
Measure and Integral: An Introduction to Real Analysis.
Second.
Chapman and Hall/CRC, Apr. 2015.
- [Wil18] Mark M. Wilde.
“Strong and Uniform Convergence in the Teleportation Simulation of Bosonic Gaussian Channels”.
In: *Physical Review A* 97.6 (June 2018), p. 062305.
DOI: [10.1103/PhysRevA.97.062305](#).
arXiv: [1712.00145](#).
- [Yok+13] Shota Yokoyama, Ryuji Ukai, Seiji C. Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C. Menicucci, and Akira Furusawa.
“Ultra-Large-Scale Continuous-Variable Cluster States Multiplexed in the Time Domain”.
In: *Nature Photonics* 7.12 (Dec. 2013), pp. 982–986.
DOI: [10.1038/nphoton.2013.287](#).
- [Yos+16] Jun-ichi Yoshikawa, Shota Yokoyama, Toshiyuki Kaji, Chanond Sornphiphatphong, Yu Shiozawa, Kenzo Makino, and Akira Furusawa.
“Generation of One-Million-Mode Continuous-Variable Cluster State by Unlimited Time-Domain Multiplexing”.

- In: *APL Photonics* 1.6 (Sept. 2016), p. 060801.
DOI: [10.1063/1.4962732](#).
arXiv: [1606.06688](#).
- [Zha08] Jing Zhang.
“Graphical Description of Local Gaussian Operations for Continuous-Variable Weighted Graph States”.
In: *Physical Review A* 78.5 (Nov. 2008), p. 052307.
DOI: [10.1103/PhysRevA.78.052307](#).
arXiv: [0810.1343](#).
- [Zha10] Jing Zhang.
“Graphical Rule of Transforming Continuous-Variable Graph States by Local Homodyne Detection”.
In: *Physical Review A* 82.3 (Sept. 2010), p. 034303.
DOI: [10.1103/PhysRevA.82.034303](#).
arXiv: [1006.3974](#).
- [ZB06] Jing Zhang and Samuel L. Braunstein.
“Continuous-Variable Gaussian Analog of Cluster States”.
In: *Physical Review A* 73.3 (Mar. 2006).
DOI: [10.1103/PhysRevA.73.032318](#).
- [Zho+03] D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun.
“Quantum Computation Based on D-Level Cluster States”.
In: *Physical Review A* 68.6 (Dec. 2003), p. 062303.
DOI: [10.1103/PhysRevA.68.062303](#).
arXiv: [quant-ph/0304054](#).
- [ZLC00] Xinlan Zhou, Debbie W. Leung, and Isaac L. Chuang.
“Methodology for Quantum Logic Gate Constructions”.
In: *Physical Review A* 62.5 (Oct. 2000), p. 052316.
DOI: [10.1103/PhysRevA.62.052316](#).
arXiv: [quant-ph/0002039](#).