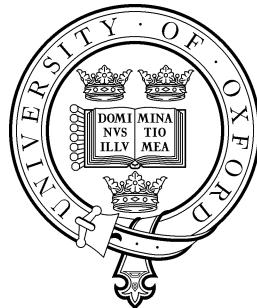


Quantum Pebble Games with Applications to Lower Bounds for Symmetric Quantum Circuits



Ryan Dancy
Somerville College
University of Oxford

A thesis submitted for the degree of
MSc in Mathematics and Foundations of Computer Science

Trinity 2025

Acknowledgements

I would like to thank my supervisor, Sergii Strelchuk, and Davi Castro-Silva for their advice and guidance throughout the research and writing process for this thesis. I would also like to thank my undergraduate research supervisor, Nancy Day, who greatly supported me in beginning my journey in research. Finally, I am grateful to my family for their support and encouragement.

Abstract

Pebble games form a class of combinatorial games with close connections to logic. Work by Dawar and Wilsenach [Daw15a; DW20; DW22] has developed a technique which uses pebble games to prove lower bounds on computation by symmetric circuits, a restricted class of circuits which form a natural model of computation for problems with inherent symmetries, such as isomorphism-invariant graph properties. Recently, Castro-Silva, Gur, and Strelchuk [CGS25] introduced a notion of symmetric quantum circuits, generalizing the classical notion.

In this thesis, we present a novel quantum generalization of pebble games, and we apply our quantum pebble game to prove new lower bounds in the symmetric quantum circuit model. We introduce a general framework for quantum pebble games and define a concrete game based on partial trace, both of which are likely to be of independent interest. We then generalize Dawar and Wilsenach's technique using our quantum pebble game to prove lower bounds for symmetric quantum circuits. We obtain novel lower bounds showing that for a particular graph property \mathcal{P} which is computable in polynomial time by a classical algorithm, there is no family of symmetric quantum circuits of a certain class which computes \mathcal{P} on n -vertex graphs using polynomially many gates which uses $o(n/\log n)$ -partite entanglement. Likewise, we show there is no such family which uses $O(n^{1-\varepsilon})$ -partite entanglement and $2^{o(n^\varepsilon)}$ gates for any $0 < \varepsilon \leq 1$. Our results show that efficient computation of some classically-efficient properties by certain classes of symmetric quantum circuits, if at all possible, requires a large amount of multipartite entanglement.

Contents

1	Introduction	1
I	Pebble games	3
2	Introduction to pebble games	4
2.1	Logical preliminaries	6
2.1.1	First-order logic (FO)	7
2.1.2	Fixed-point logic (FP)	8
2.1.3	Fixed-point logic with counting (FPC)	9
2.1.4	The Ehrenfeucht–Fraïssé game	11
2.2	Finite variable logics: \mathcal{L}_k and \mathcal{C}_k	12
2.3	Pebble games	13
2.3.1	The \mathcal{L}_k pebble game	14
2.3.2	The Immerman–Lander \mathcal{C}_k pebble game	15
2.3.3	Hella’s bijection game	15
2.4	The Cai–Fürer–Immerman results	17
2.5	Connections to symmetric computation	18
2.5.1	From Sym_n to Alt_n	19
3	New quantum pebble game framework	21
3.1	Preliminaries	21
3.1.1	Encoding structures as quantum states	23
3.2	Reformulation of the (G, k) -pebble game	23
3.3	A framework for quantum pebble games	25
3.3.1	Pebbles are self-normalizing subgroups	25
3.3.2	Base observables and partial isomorphism	27
3.4	The quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game	28
4	Partial trace-based quantum pebble game	31
II	Lower bounds for symmetric quantum circuits	36
5	Symmetric circuits	37
5.1	Symmetric classical circuits	37

5.2	Symmetric reversible circuits	39
5.3	Symmetric quantum circuits	41
5.4	Rigid reversible and quantum circuits	43
6	Classical lower bounds for symmetric circuits	45
6.1	The support theorem	46
6.2	The classical indistinguishability theorem	47
6.3	Lower bound results	51
7	Quantum lower bounds without entanglement	53
7.1	Support	54
7.2	Reconstructibility and partition symmetry	55
7.3	A product state indistinguishability theorem	57
7.4	Lower bound results without entanglement	61
8	General quantum lower bounds	63
8.1	Directional partial trace	63
8.2	ℓ -partition symmetry and support	64
8.3	A general quantum indistinguishability theorem	65
8.4	CNOT circuits have $\eta(C)$ -partition symmetry	67
8.5	Quantum lower bound results	70
8.6	Discussion	72
9	Conclusion and future directions	74
A	Additional lemmas	76
References		79

Chapter 1

Introduction

Pebble games are a type of mathematical game used in finite model theory. Their traditional application is in proving inexpressibility results which show that some property cannot be expressed in a particular logic. *Symmetric circuits* [AD17] are circuits whose structure is invariant against a group of permutations of its inputs; they form a natural computational model for properties with inherent symmetries, such as isomorphism-invariant graph properties.

In recent years, a surprising connection has emerged between pebble games, logic, and symmetric computation. Building off Anderson and Dawar’s [AD17] characterization of fixed-point logic with counting in terms of symmetric circuits, work by Dawar [Daw15a] and Dawar and Wilsenach [DW20; DW22] has developed a technique which uses pebble games to prove exponential lower bounds on the sizes of symmetric circuits which compute certain functions. These results are interesting because they show that efficiently solving certain problems, if at all possible, requires breaking the inherent symmetry of the problem. In general, symmetric circuits form an interesting model of computation because their study tells us when symmetry-breaking is necessary for efficient computation, and because they form a powerful yet more tractable subset of the class of all circuits. For instance, Valiant’s conjecture [Val79] that $\text{VP} \neq \text{VNP}$, sometimes described as the algebraic analogue of $\text{P} \neq \text{NP}$, is a major open problem which is equivalent to the nonexistence of a family of arithmetic circuits efficiently computing the matrix permanent [Val79]. While the conjecture has been open since 1979, Dawar and Wilsenach’s technique can show that no such family of *symmetric* circuits exists [DW20].

A natural question is whether this relationship between pebble games and lower bounds for symmetric circuits can be extended to the quantum circuit regime. A notion of *symmetric quantum circuits* has recently been introduced by Castro-Silva, Gur, and Strelchuk [CGS25], who show that this model is powerful enough to efficiently implement several important quantum-algorithmic techniques.

In this thesis, we introduce a corresponding notion of *quantum pebble games*, and we prove a relationship to lower bounds in the symmetric quantum circuit model. We present a novel framework for quantum generalizations of pebble games and derive from it a concrete game based on the partial trace. Using this quantum pebble game, we then generalize Dawar and Wilsenach’s lower bound technique to the quantum case, obtaining new lower bounds on the sizes of families of symmetric quantum circuits from certain classes which compute certain properties. Our work culminates by showing that there exists a graph property \mathcal{P} which can be classically computed in polynomial time, but which cannot be computed on n -vertex graphs by any polynomial-size

family of symmetric quantum circuits from a certain class which entangles together $o(n/\log n)$ qubits (Corollary 8.15).

This thesis is organized into two parts. Part I presents our proposed quantum pebble games and an associated general framework. We begin by reviewing the history of pebble games and the state of the art in Chapter 2, proving a new translation between strategies for two variants of the pebble game in Section 2.5.1. Chapter 3 then presents our novel framework for quantum pebble games, leading to a very general notion of quantum pebble games. In Chapter 4, we derive the *partial trace-based quantum pebble game* which is easier to reason about and which we will apply to prove lower bounds for symmetric circuits. Both the general framework and the partial trace-based quantum pebble game are likely to be of independent interest to future research on quantum applications of pebble games.

Part II presents applications of our quantum pebble games to prove new lower bound results on symmetric quantum circuits. We first give the definitions of symmetric classical, reversible, and quantum circuits of [AD17] and [CGS25] in Chapter 5. In Chapter 6, we present Dawar and Wilzenach's technique for proving lower bounds on symmetric classical circuits. Our main contributions of Part II are presented in Chapters 7 and 8, where we give a substantial generalization of Dawar and Wilzenach's technique to symmetric quantum circuits using our quantum pebble game framework. Our technique depends heavily on the amount of entanglement used by a circuit: Chapter 7 presents our technique in the simpler special case of quantum circuits operating only on product states, and Chapter 8 generalizes our technique to quantum circuits using arbitrary entanglement. We conclude the thesis in Chapter 9 by giving several directions for further research.

Part I

Pebble games

Chapter 2

Introduction to pebble games

This chapter is a comprehensive introduction to pebble games and related concepts based on Dawar’s survey of fixed-point logic with counting [Daw15b]. Section 2.5.1 presents a new translation of strategies for the (Sym_n, k) -pebble game to the (Alt_n, k) -pebble game; otherwise, this chapter contains no original results.

The goal of the field of *descriptive complexity theory* is to understand computational complexity classes in terms of the richness of the logic needed to describe the properties in the class [Imm99]. For instance, Fagin’s theorem [Fag74] shows that NP is exactly the set of properties which can be defined by sentences of existential second-order logic. No such characterization is known for P, the class of properties computable in polynomial time; a proof of the nonexistence of such a logic, however, would imply $P \neq NP$ [Fag74]. The quest for a logic capturing P has hence resulted in a fruitful line of research.

In 1982, Immerman [Imm82a] proposed *fixed-point logic with counting* (FPC), which consists of standard first-order logic augmented with a way to express iteration, by taking fixed points, and a way to count the number of elements for which a formula holds. Immerman asked whether FPC captures P on graphs: that is, is every graph property computable in polynomial time expressible by a sentence of FPC? This question was answered in the negative ten years later by Cai, Fürer, and Immerman [CFI92], who constructed a graph property (the *CFI construction*) which is computable in polynomial time and yet is not expressible in FPC.

For a given logic \mathcal{L} and structures \mathcal{A} and \mathcal{B} over the same vocabulary, write $\mathcal{A} \equiv_{\mathcal{L}} \mathcal{B}$ to mean that \mathcal{A} and \mathcal{B} agree on every sentence in \mathcal{L} . For several logics \mathcal{L} which are related to FPC, the equivalence $\equiv_{\mathcal{L}}$ is characterized by a type of combinatorial game known as *pebble games*, which are used in the CFI construction. These games are variations on the Ehrenfeucht–Fraïssé game [Ehr61; Fra54], which is used to prove that two structures agree on all sentences of first-order logic. Like the Ehrenfeucht–Fraïssé game, a pebble game on two structures \mathcal{A} and \mathcal{B} is played between two players, conventionally named Spoiler and Duplicator. Spoiler is trying to show that the structures are different, and Duplicator is trying to show that they are the same. At a high level, Spoiler and Duplicator take turns placing and removing pebbles on elements of the structures \mathcal{A} and \mathcal{B} such that at most k pebbles are in play at a time. After each round, if Duplicator has managed to play such that there is a *partial isomorphism* between the pebbled elements of \mathcal{A} and \mathcal{B} , then play continues; otherwise, Spoiler wins. Duplicator wins the game if it has a strategy to play indefinitely.

If Duplicator has a winning strategy on the pebble game corresponding to a logic \mathcal{L} on the structures \mathcal{A} and \mathcal{B} , then $\mathcal{A} \equiv_{\mathcal{L}} \mathcal{B}$. Thus, if we can find infinite families of structures $(\mathcal{A}_n)_n$ and $(\mathcal{B}_n)_n$ which differ in some property \mathcal{P} but for which Duplicator has a winning strategy on the corresponding pebble game on \mathcal{A}_n and \mathcal{B}_n , we know that property \mathcal{P} cannot be expressed in \mathcal{L} . This is what is done in the CFI construction: Two equivalent pebble games given by Immerman and Lander [IL90] and Hella [Hel96] express equivalence with respect to all FPC sentences for finite structures, and Cai et al. construct two families of graphs $(G_n)_n$ and $(H_n)_n$ which can be separated in polynomial time but for which Duplicator wins these pebble games.

Despite the failure of FPC to capture P , it remains an interesting logic to study in its own right due to, among other reasons [Daw15b], a connection to circuit complexity and symmetric computation. Anderson and Dawar [AD17] prove that a property is expressible in FPC if and only if it is computed by a polynomially uniform family of *symmetric circuits* using a particular gate set. Here, “symmetric” is meant in the syntactic sense: a circuit is symmetric if any permutation of its input gates respecting the encoded structure can be extended to an automorphism of the whole circuit. Hence, the inexpressibility of a property \mathcal{P} in FPC, like in the result of Cai et al., induces a lower bound on the size of any family of symmetric circuits computing \mathcal{P} [Daw15b].

Since these inexpressibility results are proven using pebble games, this raises the intriguing possibility of using pebble games to prove lower bounds on families of symmetric circuits directly, without reference to the underlying logic. This is carried out by Dawar in [Daw15a], and his technique is generalized by Dawar and Wilsenach in [DW20; DW22] to more general classes of symmetric circuits. They define a generalization of Hella’s pebble game and use it to prove more general lower bounds. A quantum extension of Dawar and Wilsenach’s pebble game is the main focus of Part I of this thesis; their lower bound results are thoroughly explored and generalized to quantum circuits in Part II.

In the quest for a logic capturing P , the most promising remaining candidate is *choiceless polynomial time* (CPT), introduced by Blass, Gurevich, and Shelah [BGS99], which is based on abstract state machines which use parallel computation in lieu of making arbitrary choices. The same authors [BGS02] introduce *choiceless polynomial time with counting* (CPTC), which augments CPT with a cardinality operator. Dawar, Richerby, and Rossman [DRR08] show that CPTC is strictly more powerful than FPC. As of 2023, it is still open whether CPTC captures P [Pag23].

This chapter is organized as follows. In Section 2.1, we build up to a definition of FPC and define the Ehrenfeucht–Fraïssé game, a precursor of pebble games. We then define two logics, \mathcal{L}_k and \mathcal{C}_k , which aid in the study of FPC (Section 2.2) and present several pebble games characterizing them (Section 2.3). We summarize the CFI construction in Section 2.4. Finally, in Section 2.5, we expand on the connection between FPC, pebble games, and symmetric circuits, and we introduce Dawar and Wilsenach’s pebble game which is extended in this thesis. We additionally give an original translation between strategies for two variants of their pebble game.

2.1 Logical preliminaries

We begin by introducing the fundamental logical concepts needed for the remainder of the thesis, then define the logics used in this chapter. For our purposes, it will suffice to use only relation symbols; we do not consider function or constant symbols. Let $\mathbb{Z}_{\geq 1} = \{1, 2, \dots\}$ denote the positive integers, and for $k \in \mathbb{Z}_{\geq 1}$, let $[k] = \{1, 2, \dots, k\}$. We denote a tuple as $\vec{x} = (x_1, \dots, x_n)$, where the arity n is inferred from context.

Definition 2.1 [AD17]. A *relational vocabulary* is a finite tuple $\tau = (R_1^{r_1}, \dots, R_k^{r_k})$ of *relation symbols*, where for each $i \in [k]$, the relation symbol R_i has an associated *arity* $r_i \in \mathbb{Z}_{\geq 1}$.

A relational vocabulary (or just a *vocabulary*) defines the relation symbols which may be used in a logic. The symbols in a vocabulary τ are given meaning via τ -*structures*.

Definition 2.2 [AD17]. A τ -*structure* with respect to a relational vocabulary $\tau = (R_1^{r_1}, \dots, R_k^{r_k})$ is a tuple $\mathcal{A} = \langle A; R_1^{\mathcal{A}}, \dots, R_k^{\mathcal{A}} \rangle$, where A is a set called the *domain* of \mathcal{A} and for each $i \in [k]$, we have $R_i^{\mathcal{A}} \subseteq A^{r_i}$.

When the vocabulary τ is clear, I refer to τ -structures simply as structures. The elements of the domain A are called the *elements* of \mathcal{A} . The *size* of a structure is the size of its domain. A structure \mathcal{A} is *finite* if its domain is finite. Let $\text{fin}[\tau]$ denote the set of finite τ -structures [AD17]. We usually restrict our attention to finite structures.

Many mathematical objects may be described as structures. For example, consider the relational vocabulary $\tau_{\text{graph}} = (E^2)$ consisting of one binary relation E . A directed graph can then be described as a τ_{graph} -structure $\mathcal{G} = \langle V; E^{\mathcal{G}} \rangle$ where the domain is the set of vertices V and the edges are described by $E^{\mathcal{G}} \subseteq V^2$.

A τ -*property* is a subset of $\text{fin}[\tau]$. A τ -property \mathcal{P} is said to be *polynomial time* if there is a polynomial-time algorithm which, given an efficient representation of a finite τ -structure \mathcal{A} , decides whether $\mathcal{A} \in \mathcal{P}$. For example, the τ_{graph} -property consisting of all directed graphs that contain a cycle is polynomial time, because we can determine whether a cycle exists in polynomial time using depth-first search [Cor+22]. Say that a τ -property \mathcal{P} *separates* two structures $\mathcal{A}, \mathcal{B} \in \text{fin}[\tau]$ if \mathcal{A} and \mathcal{B} do not agree on membership in \mathcal{P} , and \mathcal{P} separates two families of τ -structures $(\mathcal{A}_n)_{n \in \mathbb{Z}_{\geq 1}}$ and $(\mathcal{B}_n)_{n \in \mathbb{Z}_{\geq 1}}$ if it separates \mathcal{A}_n and \mathcal{B}_n for each n .

Given a sentence φ of a logic \mathcal{L} over the vocabulary τ and a τ -structure \mathcal{A} , we write $\mathcal{A} \models \varphi$ if \mathcal{A} satisfies φ . We say that φ defines the property $\{\mathcal{A} \in \text{fin}[\tau] : \mathcal{A} \models \varphi\}$. A τ -property \mathcal{P} is *captured* by a logic \mathcal{L} if there is some sentence φ of \mathcal{L} which defines \mathcal{P} . Our motivating open question is then as follows: Is there is a natural logic \mathcal{L} which captures every polynomial-time property on relational structures?

2.1.1 First-order logic (FO)

This section is based on Chapter 1 of [KZ21].

We begin by defining standard first-order logic, denoted FO , beginning with its syntax. Fix a relational vocabulary $\tau = (R_1^{r_1}, \dots, R_k^{r_k})$ and let $\text{FO}[\tau]$ denote first-order logic over τ . Let $V = \{x, y, z, \dots\}$ be an infinite set of variable symbols; we will generally feel free to use arbitrary variable symbols (x, a_1, p_2 , etc.) when the usage is clear.

Definition 2.3. The formulas of $\text{FO}[\tau]$ are defined recursively as follows:

- (i) If $R_i^{r_i} \in \tau$ is a relation symbol with arity r_i and $x_1, \dots, x_{r_i} \in V$ are variables, then $R_i(x_1, \dots, x_{r_i})$ is a formula.
- (ii) If $x_1, x_2 \in V$ are variables, then $x_1 = x_2$ is a formula.
- (iii) If φ_1 and φ_2 are formulas, then so are $(\varphi_1 \wedge \varphi_2)$ and $\neg \varphi_1$.
- (iv) If φ is a formula and $x \in V$ is a variable, then $\exists x \varphi$ is a formula.

Nothing else is a formula of $\text{FO}[\tau]$. Formulas with no quantifiers, i.e. built without using rule (iv), are called *atomic formulas*.

We define the universal quantifier and the rest of the Boolean connectives as shorthand. Define $\forall x \varphi$ to mean $\neg \exists x \neg \varphi$, $(\varphi_1 \vee \varphi_2)$ to mean $\neg(\neg \varphi_1 \wedge \neg \varphi_2)$, $(\varphi_1 \rightarrow \varphi_2)$ to mean $(\neg \varphi_1 \vee \varphi_2)$, and $(\varphi_1 \leftrightarrow \varphi_2)$ to mean $((\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1))$.

An occurrence of a variable x in a formula φ is *bound* if it occurs within a subformula $\exists x \psi$ in φ ; otherwise it is *free*. The set of *free variables* in a formula φ of $\text{FO}[\tau]$, denoted $\text{FV}(\varphi)$, is the set of variables which occur free in φ . A formula with no free variables is called a *sentence*. We write $\varphi(x_1, \dots, x_n)$, where x_1, \dots, x_n are distinct, to denote that φ is a formula with free variables $\text{FV}(\varphi) \subseteq \{x_1, \dots, x_n\}$.

The semantics of FO are then defined as follows in the standard way. Let $\mathcal{A} = \langle A; R_1^{\mathcal{A}}, \dots, R_k^{\mathcal{A}} \rangle$ be a τ -structure. Following the notation of [EF99], for a formula φ containing free variables x_1, \dots, x_n , we write $\mathcal{A} \models \varphi[a_1, \dots, a_n]$ to mean that φ holds when each variable x_i is interpreted as the element $a_i \in A$.

Definition 2.4. Let $\varphi(\vec{x})$ be a formula of $\text{FO}[\tau]$ and let $\vec{a} = (a_1, \dots, a_n) \in A$ be a tuple of elements of A . We define the relation $\mathcal{A} \models \varphi[\vec{a}]$ recursively as follows.

- $\mathcal{A} \models R_i(x_1, \dots, x_{r_i})[\vec{a}]$ if and only if $(a_1, \dots, a_{r_i}) \in R_i^{\mathcal{A}}$.
- $\mathcal{A} \models x_1 = x_2[\vec{a}]$ if and only if $a_1 = a_2$.
- $\mathcal{A} \models (\varphi_1(\vec{x}) \wedge \varphi_2(\vec{x}))[\vec{a}]$ if and only if $\mathcal{A} \models \varphi_1[\vec{a}]$ and $\mathcal{A} \models \varphi_2[\vec{a}]$.
- $\mathcal{A} \models \neg \varphi[\vec{a}]$ if and only if $\mathcal{A} \not\models \varphi[\vec{a}]$.
- $\mathcal{A} \models \exists y \varphi(\vec{x}, y)[\vec{a}]$ if and only if there is some $b \in A$ such that $\mathcal{A} \models \varphi(\vec{x}, b)[\vec{a}, b]$.

The properties defined by sentences of FO are called *first-order properties* [Kos24]. For example, consider the following sentence of $\text{FO}[\tau_{\text{graph}}]$:

$$\varphi_{\text{symm}} \equiv \forall x \forall y (E(x, y) \rightarrow E(y, x)) \quad (2.1)$$

This sentence defines the τ_{graph} -property of symmetric directed graphs. This property is polynomial-time, but not all polynomial-time properties are captured by FO : for instance, there is no FO sentence defining the property of being a bipartite graph [Czé22].

2.1.2 Fixed-point logic (FP)

This section is based on Chapter 8 of [EF99].

Fixed-point logic, denoted FP , extends first-order logic with a *fixed-point operator* which allows a form of iteration to be expressed within the logic. By adding such computation-like structures to the logic, we can express many polynomial-time properties.

There are several forms of fixed-point logic, including least fixed-point logic and inflationary fixed-point logic. By a result of Gurevich and Shelah [GS86], these are equivalent; hence, following [Daw15b], we present only inflationary fixed-point logic, which is due to Gurevich [Gur83]. For simplicity, we define its semantics (and those of FPC) with respect to finite models only.

Consider a finite set A and a function $f : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$. (Here $\mathcal{P}(A)$ denotes the powerset of A .) Let $P_0^f = \emptyset$ and for each integer $i \geq 1$, let $P_i^f = P_{i-1}^f \cup f(P_{i-1}^f)$. This defines a sequence of subsets of A :

$$P_0^f \subseteq P_1^f \subseteq P_2^f \subseteq \cdots \subseteq A \quad (2.2)$$

Since A is finite, this sequence reaches a fixed point $P_\omega^f := \bigcup_{i \geq 0} P_i^f$ in a finite number of steps. We call P_ω^f the *inflationary fixed point* of f [EF99].

Inflationary fixed-point logic incorporates this notion of fixed point into the logic. Again fix a vocabulary τ , and let $\text{FP}[\tau]$ denote (inflationary) fixed-point logic over τ . To define the syntax of $\text{FP}[\tau]$, in addition to our set of first-order variables V , we require an infinite set of *second-order variables* $S = \{X, Y, Z, \dots\}$, which we denote with uppercase letters. Each second-order variable has an associated arity r . To define FP , we extend the syntax of FO as follows.

Definition 2.5 [Daw15b]. The formulas of $\text{FP}[\tau]$ are defined recursively using the rules of Definition 2.3 together with the following rules:

- (v) If $X \in S$ is a second-order variable with arity r and $x_1, \dots, x_r \in V$ are first-order variables, then $X(x_1, \dots, x_r)$ is a formula.
- (vi) If $X \in S$ is a second-order variable with arity r , φ is a formula, and $x_1, \dots, x_r \in V$ and $t_1, \dots, t_r \in V$ are first-order variables, then $[\mathbf{fp}_{X, x_1, \dots, x_r} \varphi](t_1, \dots, t_r)$ is a formula.

For semantics, fix a finite τ -structure \mathcal{A} with domain A . Intuitively, a second-order variable X with arity r represents a set of r -tuples of elements, and the formula $X(x_1, \dots, x_r)$ asks whether $(x_1, \dots, x_r) \in X$. We can describe the meaning of $[\mathbf{fp}_{X, x_1, \dots, x_r} \varphi](t_1, \dots, t_r)$ as follows [EF99]. A formula $\varphi(x_1, \dots, x_r, \vec{y}, X, \vec{Y})$ defines a function $f_\varphi : \mathcal{P}(A^r) \rightarrow \mathcal{P}(A^r)$ given by

$$f_\varphi(P) = \{(a_1, \dots, a_r) \in A^r : \mathcal{A} \models \varphi[a_1, \dots, a_r, \vec{b}, P, \vec{B}]\} \quad (2.3)$$

for each $P \subseteq A^r$, where \vec{b} and \vec{B} are implicitly-defined interpretations for the variables \vec{y} and \vec{Y} . Then $[\mathbf{fp}_{X, x_1, \dots, x_r} \varphi]$ represents the inflationary fixed point $P_\omega^{f_\varphi}$ of f_φ , and $[\mathbf{fp}_{X, x_1, \dots, x_r} \varphi](t_1, \dots, t_r)$ asks whether $(t_1, \dots, t_r) \in P_\omega^{f_\varphi}$. A formal definition follows.

Definition 2.6 [EF99]. Let $\varphi(\vec{X}, \vec{x})$ be a formula of $\mathbf{FP}[\tau]$. We define the relation $\mathcal{A} \models \varphi[\vec{B}, \vec{a}]$ recursively using the rules of Definition 2.4 together with the following rules:

- $\mathcal{A} \models X(x_1, \dots, x_r)[B, \vec{a}]$ if and only if $(a_1, \dots, a_r) \in B$
- $\mathcal{A} \models [\mathbf{fp}_{X, x_1, \dots, x_r} \varphi(x_1, \dots, x_r, \vec{y}, X, \vec{Y})](t_1, \dots, t_r)[\vec{b}, \vec{B}, \vec{a}]$ if and only if $(a_1, \dots, a_r) \in P_\omega^{f_\varphi}$ where f_φ is defined as above.

Many interesting computational properties can be defined in \mathbf{FP} . For instance, the following sentence of $\mathbf{FP}[\tau_{\text{graph}}]$ defines the τ_{graph} -property of strongly connected directed graphs [Daw15b]:

$$\forall u \forall v [\mathbf{fp}_{T, x, y}(x = y \vee \exists z (E(x, y) \wedge T(y, z)))](u, v) \quad (2.4)$$

In fact, the Immerman–Vardi theorem [Imm86; Var82] shows that on *ordered* structures—those equipped with a binary relation $<$ which is always interpreted as a total order on the domain— \mathbf{FP} captures every polynomial-time property. This is not true on general structures, however: for instance, there is no \mathbf{FP} sentence which is satisfied by exactly the structures with an even number of elements in their domain [Daw15b]. This motivates the introduction of \mathbf{FPC} , which adds counting directly to the logic.

2.1.3 Fixed-point logic with counting (\mathbf{FPC})

This section is based on Section 2 of [Daw15b].

Fixed-point logic with counting, denoted \mathbf{FPC} , further extends \mathbf{FP} with a “counting quantifier” $\#x \varphi$ which counts the number of domain elements x satisfying $\varphi(x)$. This directly patches the shortcoming of \mathbf{FP} pointed out above.

To deal with integers as first-class objects, our logic requires two sorts: elements of the domain, ranged over by first-order *element variables* $V = \{x_1, x_2, \dots\}$, and the nonnegative integers, ranged over by first-order *number variables* $I = \{\nu_1, \nu_2, \dots\}$. In place of an arity, each second-order variable $X \in S$ has a *type*: a finite tuple $\alpha \in \{\text{element}, \text{number}\}^*$, which declares which sort X contains at each position in its tuples [Daw15b]. To ensure the logic is decidable over finite structures, we follow [Daw15b] and require that quantification of number variables is bounded (a convention originating with Grohe [Daw15b]).

The syntax of \mathbf{FPC} is defined as follows. Fix a relational vocabulary τ .

Definition 2.7 [Daw15b]. A *counting term* is a number variable $\nu \in I$ or a term of the form $[\#x \varphi]$, where φ is a formula and $x \in V$ is an element variable.

Definition 2.8 [Daw15b]. The formulas of $\text{FPC}[\tau]$ are defined recursively by extending the rules of Definition 2.5 as follows.

- (vii) If κ_1 and κ_2 are counting terms, then $\kappa_1 = \kappa_2$ and $\kappa_1 < \kappa_2$ are formulas.
- (viii) If φ is a formula, κ is a counting term, and $\nu \in I$ is a number variable, then $\exists \nu \leq \kappa \varphi$ is a formula.

Furthermore, we amend rules (v) and (vi) to allow $x_1, \dots, x_r \in V \cup I$ to be variables of either sort and require that the sorts of the tuple (x_1, \dots, x_r) match the type of X . For rule (vi), we require the same of $t_1, \dots, t_r \in V \cup I$.

The semantics are the obvious ones. Fix a τ -structure \mathcal{A} with domain A . For a counting term κ , let $\kappa^{\mathcal{A}}$ denote the nonnegative integer corresponding to κ in the current context (left implicit). For a number variable $\nu \in I$, $\nu^{\mathcal{A}}$ is the value of ν in context; for a formula $\varphi(x)$ (leaving other free variables implicit),

$$[\#x \varphi(x)]^{\mathcal{A}} = |\{a \in A : \mathcal{A} \models \varphi[a]\}|. \quad (2.5)$$

Then we define $\mathcal{A} \models \kappa_1 = \kappa_2$ iff $\kappa_1^{\mathcal{A}} = \kappa_2^{\mathcal{A}}$, $\mathcal{A} \models \kappa_1 < \kappa_2$ iff $\kappa_1^{\mathcal{A}} < \kappa_2^{\mathcal{A}}$, and $\mathcal{A} \models \exists \nu \leq \kappa \varphi(\nu)$ iff there is some nonnegative integer $n \leq \kappa^{\mathcal{A}}$ such that $\mathcal{A} \models \varphi[n]$ [Daw15b]. We extend the fixed-point operator to the number sort in the obvious way.

To demonstrate the power of FPC , suppose $\varphi(x)$ is a formula of $\text{FPC}[\tau]$. The following sentence is satisfied exactly by the τ -structures that have an even number of elements satisfying $\varphi(x)$ [Daw15b]:

$$\psi_{\text{even}}^{\varphi} = \exists \nu_1 \leq [\#x \varphi(x)] \exists \nu_2 \leq \nu_1 (\nu_1 = [\#x \varphi(x)] \wedge (\nu_2 + \nu_2 = \nu_1)) \quad (2.6)$$

where the addition relation $\nu_1 + \nu_2 = \nu_3$ is defined as

$$\begin{aligned} & [\mathbf{fp}_{X, \nu_1, \nu_2, \nu_3}((\nu_1 = \nu_3 \wedge \nu_2 = 0) \\ & \quad \vee \exists \nu_4 \leq \nu_2 \exists \nu_5 \leq \nu_3 (X(\nu_1, \nu_4, \nu_5) \wedge \nu_2 = \nu_4 + 1 \wedge \nu_3 = \nu_5 + 1))] (\nu_1, \nu_2, \nu_3) \end{aligned} \quad (2.7)$$

and we define $\nu = 0$ as $\neg \exists \nu' \leq \nu (\nu' < \nu)$ and $\nu = \nu' + 1$ as $\nu < \nu' \wedge \neg \exists \nu'' \leq \nu' (\nu < \nu'' \wedge \nu'' < \nu')$. In particular, if $\varphi(x) \equiv x = x$ or some other tautology, then $\psi_{\text{even}}^{\varphi}$ defines the τ -property of having an even number of domain elements [Daw15b].

Immerman asked whether FPC might capture every polynomial-time property [Imm82a; Imm86]. Cai et al. constructed a counterexample [CFI92]; we build up some of the tools used in their construction.

2.1.4 The Ehrenfeucht–Fraïssé game

This section is based on Chapter 6 of [Imm99]. The presentation of the game is influenced by [DW22].

Ehrenfeucht [Ehr61] and Fraïssé [Fra54] invented a game-based technique used in finite model theory to prove that certain properties are not captured by FO . As pebble games are descended from the Ehrenfeucht–Fraïssé (EF) game, I present the EF game for historical background and as an introduction to the technique.

Fix a vocabulary τ and two τ -structures \mathcal{A} and \mathcal{B} with respective domains A and B .

Definition 2.9 [Ehr61]. The r -round Ehrenfeucht–Fraïssé (EF) game on \mathcal{A} and \mathcal{B} is played by two players, Spoiler and Duplicator, using two sequences of pebbles, a_1, \dots, a_r and b_1, \dots, b_r which may be placed on elements of \mathcal{A} and \mathcal{B} respectively. (When clear, I do not distinguish notationally between the pebbles and the elements they are placed on.)

Spoiler and Duplicator take turns placing pebbles on the two structures. Spoiler tries to place pebbles such that the pebbled elements in the two structures look different, and Duplicator tries to match Spoiler’s moves so that the pebbled elements of the structures look the same.

Initially, no pebbles are placed. The i th round proceeds as follows:

1. Spoiler chooses one of the structures \mathcal{A} or \mathcal{B} and places the pebble a_i or b_i on an unpebbled element of that structure.
2. Duplicator places the other pebble a_i or b_i on an unpebbled element of the other structure.

Duplicator tries to place their pebble in each round i to maintain the *partial isomorphism property*: The function $f_i : \{a_1, \dots, a_i\} \rightarrow \{b_1, \dots, b_i\}$ defined by

$$a_1 \mapsto b_1 \quad a_2 \mapsto b_2 \quad \dots \quad a_i \mapsto b_i, \tag{2.8}$$

mapping the pebbled elements of \mathcal{A} to the corresponding pebbled elements of \mathcal{B} , forms a partial isomorphism from \mathcal{A} to \mathcal{B} (defined below). That is, \mathcal{A} and \mathcal{B} must be indistinguishable if we look only at the pebbled elements.

Definition 2.10. Let $A' \subseteq A$ and $B' \subseteq B$. A bijection $f : A' \rightarrow B'$ is a *partial isomorphism* from \mathcal{A} to \mathcal{B} if for every relation symbol $R_i^{r_i} \in \tau$ and every $a_1, \dots, a_{r_i} \in A'$ we have

$$(a_1, \dots, a_{r_i}) \in R_i^{\mathcal{A}} \quad \text{iff} \quad (f(a_1), \dots, f(a_{r_i})) \in R_i^{\mathcal{B}}. \tag{2.9}$$

If after round i , the function f_i is *not* a partial isomorphism, then we have found a difference between the structures, and Spoiler wins the game. Otherwise, play continues. Duplicator wins if it can maintain the partial isomorphism property for r rounds.

Since the EF game on \mathcal{A} and \mathcal{B} is a game of perfect information, either Spoiler or Duplicator has a strategy which allows them to win the game regardless of the other player’s strategy [Imm99]. We say that that player *has a winning strategy* or *wins* the game.

The main application of the EF game is in proving inexpressibility results for FO. As before, for τ -structures \mathcal{A} and \mathcal{B} and a logic \mathcal{L} , we write $\mathcal{A} \equiv_{\mathcal{L}} \mathcal{B}$ if for every sentence φ of \mathcal{L} over τ we have $\mathcal{A} \models \varphi$ iff $\mathcal{B} \models \varphi$.

Definition 2.11 [Imm99]. The *quantifier rank* of a formula φ of FO is the depth of nested quantifiers in φ .

For example, the quantifier rank of any atomic formula is 0, and the quantifier rank of $(\exists x \exists y R_1(x, y)) \wedge (\exists z R_2(z))$ is 2. Let FO^r denote the fragment of FO containing formulas of quantifier rank at most r . We can now state the main theorem linking the EF game to FO.

Theorem 2.12 [Ehr61]. *Let \mathcal{A} and \mathcal{B} be τ -structures. Duplicator has a winning strategy for the r -round EF game on \mathcal{A} and \mathcal{B} if and only if $\mathcal{A} \equiv_{\text{FO}^r} \mathcal{B}$.*

That is, if we can show that Duplicator wins the r -round EF game on \mathcal{A} and \mathcal{B} , then there is no sentence of FO^r separating \mathcal{A} from \mathcal{B} , so any property which separates \mathcal{A} from \mathcal{B} cannot be defined by a first-order formula of quantifier rank r .

In lieu of a proof, I give some intuition for the forwards direction, based on the proof given in Immerman's textbook [Imm99, Thm. 6.10]. First, observe that if k pebbles have been placed, then the partial isomorphism property implies that the structures are equivalent under any atomic formula of FO containing at most k variables x_1, \dots, x_k , where we interpret the variable x_i as a_i in \mathcal{A} and b_i in \mathcal{B} .

If $\mathcal{A} \not\equiv_{\text{FO}^r} \mathcal{B}$, Spoiler can play according to the following strategy. Suppose φ is a sentence of FO^r separating \mathcal{A} and \mathcal{B} . We can assume without loss of generality that φ is of the form $\exists x \psi(x)$ where ψ is of smaller quantifier rank, and that $\mathcal{A} \models \varphi$ but $\mathcal{B} \not\models \varphi$. Then there is some $a \in A$ for such that $\mathcal{A} \models \psi[a]$, but no such witness exists in \mathcal{B} . Spoiler places a pebble on a : then no matter which $b \in B$ Duplicator chooses to pebble, we have $\mathcal{A} \models \psi[a]$ but $\mathcal{B} \not\models \psi[b]$. Since φ has quantifier rank at most r , repeating the strategy for r rounds suffices to obtain some atomic formula χ such that $\mathcal{A} \models \chi[\vec{a}]$ but $\mathcal{B} \not\models \chi[\vec{b}]$, violating the partial isomorphism property.

To prove that a τ -property \mathcal{P} is not captured by FO, it therefore suffices to show that for every $r \geq 0$, there are τ -structures $\mathcal{A}_r \in \mathcal{P}$ and $\mathcal{B}_r \notin \mathcal{P}$ such that Duplicator wins the r -round EF game on \mathcal{A}_r and \mathcal{B}_r . As it turns out, this condition is both necessary and sufficient for proving FO-inexpressibility [Imm99, Thm. 6.18].

2.2 Finite variable logics: \mathcal{L}_k and \mathcal{C}_k

We would like to study inexpressibility in FPC through games, just as EF games allow us to study inexpressibility in FO. For this, it is useful to define some simpler logics.

Definition 2.13 [IL90]. Let \mathcal{L}_k denote the fragment of FO consisting of formulas in which the only variables that appear are from the finite set $\{x_1, \dots, x_k\}$.

Note that variables may be repeated: for instance, $\exists x_1 \forall x_2 (E(x_1, x_2) \rightarrow \exists x_1 E(x_2, x_1))$ is a sentence of $\mathcal{L}_2[\tau_{\text{graph}}]$ stating that there is some vertex whose out-neighbours all have positive out-degree. Intuitively, a formula of \mathcal{L}_k can consider only k elements at a time.

To make the logic useful for working with FPC, we add “counting quantifiers”:

Definition 2.14 [IL90]. Let \mathcal{C}_k denote the extension of \mathcal{L}_k with the following syntax rule: If $n \in \mathbb{Z}_{\geq 1}$, $x \in \{x_1, \dots, x_k\}$ is a variable, and φ is a formula, then $\exists^{\geq n} x \varphi$ is a formula.

The semantics are as follows: If \mathcal{A} is a structure with domain A , $\varphi(x)$ is a formula, and $n \in \mathbb{Z}_{\geq 1}$, then $\mathcal{A} \models \exists^{\geq n} x \varphi(x)$ iff there are at least n distinct elements $a \in A$ such that $\mathcal{A} \models \varphi[a]$. It is conventional to use the shorthand

$$\exists^{=n} x \varphi \equiv (\exists^{\geq n} x \varphi) \wedge \neg(\exists^{\geq n+1} x \varphi) \quad (2.10)$$

to mean that there are exactly n elements x fulfilling $\varphi(x)$ [IL90]. For example, the sentence $\exists^{=n} x_1 (x_1 = x_1)$ of \mathcal{C}_1 defines the property of having exactly n domain elements. Of course, each \mathcal{C}_k formula is equivalent to a formula of FO, but the corresponding FO formula might have far more quantifiers and variables [IL90].

The utility of \mathcal{C}_k for reasoning about FPC is due to the following theorem:

Theorem 2.15 [IL90; Daw15b]. *Let \mathcal{A} and \mathcal{B} be finite structures. For every sentence φ of FPC, there is some natural number k such that if $\mathcal{A} \equiv_{\mathcal{C}_k} \mathcal{B}$, then $\mathcal{A} \models \varphi$ if and only if $\mathcal{B} \models \varphi$.*

Proof sketch (after [Daw15b]). This follows from the following fact: For every sentence φ of FPC, there is some k and some family of sentences $(\theta_n)_n$ of \mathcal{C}_k such that φ is equivalent to θ_n on structures of size at most n . That is, we can express φ on structures of size at most n using counting quantifiers and a fixed number of variables independent of n .

To construct θ_n from φ , we can take advantage of the assumption that the domain has size at most n to express subformulas of φ involving $\#x \psi(x)$ or quantification over integers using a finite number of counting quantifiers. To express fixed points, observe that on at most n elements, n iterations suffice to obtain a fixed point: hence we can express $[\mathbf{fp}_{X, \vec{x}} \varphi](\vec{t})$ by expanding the fixed point n times. This construction uses no more variables than there were element variables in the original formula φ . \square

Hence if we can show that $\mathcal{A} \equiv_{\mathcal{C}_k} \mathcal{B}$ for all k , Theorem 2.15 tells us that $\mathcal{A} \equiv_{\text{FPC}} \mathcal{B}$, so no property captured by FPC separates \mathcal{A} from \mathcal{B} . As with the EF game, a methodology for proving $\mathcal{A} \equiv_{\mathcal{C}_k} \mathcal{B}$ is given by an appropriate game, which we now introduce.

2.3 Pebble games

\mathcal{L}_k and \mathcal{C}_k admit analogues of Theorem 2.12 which characterize $\equiv_{\mathcal{L}_k}$ and $\equiv_{\mathcal{C}_k}$ with respect to variants of the EF game which we refer to as *pebble games*, since they are best explained in terms of picking up and placing pebbles. We first present the original pebble games for

\mathcal{L}_k (Section 2.3.1) and \mathcal{C}_k (Section 2.3.2) by Immerman and Immerman–Lander respectively. These games were used in the CFI results. In Section 2.3.3, we then present the *bijection game*, invented by Hella, which is equivalent to the Immerman–Lander \mathcal{C}_k pebble game but is more applicable to symmetric computation and is generalized in this thesis. The formulation of the games in this section is influenced by that of Dawar and Wilenach [DW22].

2.3.1 The \mathcal{L}_k pebble game

The simplest pebble game is the \mathcal{L}_k pebble game, invented by Immerman [Imm82b]. The key difference between pebble games and the EF game is that the resource parameter is different: there are (countably) infinitely many rounds, but only finitely many pebbles. At the beginning of each round, Spoiler picks up one of the pairs of pebbles: if it chooses to pick up a pair of pebbles that are already placed on the structures, those pebbles are removed from the structures. As a result, pebble games with k pebbles model finite variable logics with k variables, since at most k elements of each structure are pebbled at a time.

Definition 2.16 [Imm82b]. The \mathcal{L}_k pebble game on structures \mathcal{A} and \mathcal{B} is played using two sets of k pebbles, a_1, \dots, a_k and b_1, \dots, b_k , which may be placed on elements of \mathcal{A} and \mathcal{B} respectively. Initially, no pebbles are placed. Each round proceeds as follows:

1. Spoiler picks up a pair of pebbles (a_i, b_i) . If (a_i, b_i) were previously placed, they are removed from the structures.
2. Spoiler chooses one of the structures \mathcal{A} or \mathcal{B} and places the pebble a_i or b_i on an unpebbled element of that structure.
3. Duplicator places the other pebble a_i or b_i on an unpebbled element of the other structure.

Suppose that at the end of the round, the pebbles $a_{i_1}, \dots, a_{i_\ell}$ and $b_{i_1}, \dots, b_{i_\ell}$ are placed. Let $f : \{a_{i_1}, \dots, a_{i_\ell}\} \rightarrow \{b_{i_1}, \dots, b_{i_\ell}\}$ be the function taking each pebble a_{i_j} on \mathcal{A} to the corresponding pebble b_{i_j} on \mathcal{B} . Spoiler wins if f is not a partial isomorphism from \mathcal{A} to \mathcal{B} . Otherwise, play continues, and Duplicator wins if it has a strategy to play forever.

As a formula of \mathcal{L}_k can reference only k elements at a time, the \mathcal{L}_k pebble game can test for a partial isomorphism between only k elements in each structure. The currently pebbled elements of each structure can be thought of as a “window” of visible elements which slides along the structure [ADW17]. It is then intuitive that the game obeys an analogue of Theorem 2.12:

Theorem 2.17 [Imm82b, Thm. C.1]. *Duplicator wins the \mathcal{L}_k pebble game on \mathcal{A} and \mathcal{B} if and only if $\mathcal{A} \equiv_{\mathcal{L}_k} \mathcal{B}$.*

2.3.2 The Immerman–Lander \mathcal{C}_k pebble game

Immerman and Lander [IL90] generalized the \mathcal{L}_k pebble game to characterize \mathcal{C}_k .

Definition 2.18 [IL90]. The *Immerman–Lander \mathcal{C}_k pebble game* on structures \mathcal{A} and \mathcal{B} with respective domains A and B is played using two sets of k pebbles, a_1, \dots, a_k and b_1, \dots, b_k , which may be placed on elements of \mathcal{A} and \mathcal{B} respectively. Initially, no pebbles are placed. Each round proceeds as follows:

1. Spoiler picks up a pair of pebbles (a_i, b_i) . If (a_i, b_i) were previously placed, they are removed from the structures.
2. Spoiler chooses one of the structures \mathcal{A} or \mathcal{B} (say \mathcal{A}) and chooses a subset $X \subseteq A$ of the unpebbled elements of its domain.
3. Duplicator chooses a subset $Y \subseteq B$ of the unpebbled elements of the domain of the other structure such that $|X| = |Y|$.
4. Spoiler places the pebble b_i on some $y \in Y$.
5. Duplicator places the pebble a_i on some $x \in X$.

As before, Spoiler wins if the placed pebbles induce a partial isomorphism $a_j \mapsto b_j$ from \mathcal{A} to \mathcal{B} . Otherwise, play continues, and Duplicator wins if it has a strategy to play forever.

An interpretation of this game is that in each round, Spoiler asserts that there are $|X|$ elements in one structure with some property, and Duplicator must respond with $|Y| = |X|$ elements in the other structure with the same property [IL90]. This gives some intuition for the result that this game indeed characterizes \mathcal{C}_k :

Theorem 2.19 [IL90, Thm. 1.7.3]. *Duplicator wins the Immerman–Lander \mathcal{C}_k pebble game on \mathcal{A} and \mathcal{B} if and only if $\mathcal{A} \equiv_{\mathcal{C}_k} \mathcal{B}$.*

2.3.3 Hella’s bijection game

Hella [Hel96] introduced a pebble game known as the bijection game, which is equivalent to the Immerman–Lander \mathcal{C}_k pebble game on finite structures of the same size (and so it also characterizes \mathcal{C}_k on those structures).¹ It somewhat obscures the connection to logic, but has closer connections to computation.

Definition 2.20 [Hel96]. Let \mathcal{A} and \mathcal{B} be finite structures with respective domains A and B of the same size. The *k -pebble bijection game* on \mathcal{A} and \mathcal{B} is played using two sets of k pebbles, a_1, \dots, a_k and b_1, \dots, b_k . Initially, no pebbles are placed. Each round proceeds as follows:

1. Spoiler picks up a pair of pebbles (a_i, b_i) .

¹Hella in fact defined a more general “ n -bijective k -pebble game”, in which Spoiler may place up to n pebbles in each round. On finite structures, this game characterizes \mathcal{L}_k extended by all n -ary “generalized quantifiers” [Hel96].

2. Duplicator chooses a bijection $f : A \rightarrow B$ which respects the pebbles in the sense that for every pair of pebbles (a_j, b_j) which are placed on the structures, we have $f(a_j) = b_j$.
3. Spoiler places a_i on some unpebbled element $a \in A$ and places b_i on $f(a) \in B$.

Again, Spoiler wins if the pebbles fail to induce a partial isomorphism $a_j \mapsto b_j$ from \mathcal{A} to \mathcal{B} . Otherwise play continues, and Duplicator wins if it has a strategy to play forever.

Observe that the function $a_j \mapsto b_j$ induced by the pebbles in each round is just the domain restriction of f to the pebbles placed on \mathcal{A} . Let $f|_{\vec{a}}$ denote this restriction: hence we can alternatively say that Spoiler wins if $f|_{\vec{a}}$ is not a partial isomorphism from \mathcal{A} to \mathcal{B} .

We can show this game is equivalent to the Immerman–Lander \mathcal{C}_k game.

Theorem 2.21 [Hel96]. *Let \mathcal{A} and \mathcal{B} be finite structures of the same size. Duplicator wins the k -pebble bijection game on \mathcal{A} and \mathcal{B} if and only if Duplicator wins the Immerman–Lander \mathcal{C}_k pebble game \mathcal{A} and \mathcal{B} .*

Proof. Hella [Hel96] shows (in more generality) that the k -pebble bijection game captures \mathcal{C}_k ; instead, I give what is to my knowledge an original direct proof of equivalence. Let A and B be the domains of \mathcal{A} and \mathcal{B} , respectively.

(\Rightarrow) Suppose Duplicator has a winning strategy for the bijection game: we simulate this strategy in the Immerman–Lander game. At round r , suppose our bijection game strategy would play a bijection $f : A \rightarrow B$. In the Immerman–Lander game, suppose without loss of generality that Spoiler chooses \mathcal{A} . If Spoiler chooses a set $X \subseteq A$, respond with $Y = \{f(x) : x \in X\}$. Spoiler then places a pebble on some $f(x) \in Y$: respond with $x \in X$. Under this strategy, Spoiler may choose to place pebbles on exactly the unpebbled pairs of elements in $\{(a, f(a)) : a \in A\}$, which is the same set of options as in the bijection game.

(\Leftarrow) Suppose Duplicator has a winning strategy for the Immerman–Lander game. Let A' and B' be the sets of unpebbled elements in \mathcal{A} and \mathcal{B} , respectively. At round r , the Immerman–Lander strategy, assuming Spoiler chooses \mathcal{A} , is described by a function $g : \mathcal{P}(A') \rightarrow \mathcal{P}(B')$ such that $|g(X)| = |X|$ for each $X \subseteq A'$, describing Duplicator's response to each subset $X \subseteq A'$ which Spoiler could choose, together with a family of functions $h_X : g(X) \rightarrow X$ for each $X \subseteq A'$ describing Duplicator's response $h_X(b) \in X$ to the subsequent $b \in g(X)$ chosen by Spoiler.

With this Duplicator strategy, the possible pairs of elements which Spoiler could cause to be pebbled in this round are

$$P = \{(h_X(b), b) : X \subseteq A', b \in g(X)\}. \quad (2.11)$$

Since Duplicator's strategy is winning, Duplicator wins regardless of which pair $(a, b) \in P$ Spoiler chooses to pebble.

Think of P as the edges of a bipartite graph on (A', B') . For every $X \subseteq A'$, there is a set $Y = g(X) \subseteq B'$ with $|Y| = |X|$ such that every $b \in Y$ is adjacent to some $h_X(b) \in X$ in this

graph. This is Hall's condition, so by Hall's theorem [Hal35], there is a perfect matching in this graph: that is, there is some bijection $f : A' \rightarrow B'$ such that $\{(a, f(a)) : a \in A'\} \subseteq P$.

Therefore in the bijection game, Duplicator plays f , extended to a bijection $A \rightarrow B$ by setting $f(a_j) = b_j$ for each pebbled pair (a_j, b_j) . The pairs $\{(a, f(a)) : a \in A'\}$ which could be pebbled are a subset of those allowed by our Immerman–Lander strategy, which is winning for Duplicator, so this strategy also wins. \square

Corollary 2.22. *Duplicator wins the k -pebble bijection game on \mathcal{A} and \mathcal{B} if and only if $\mathcal{A} \equiv_{\mathcal{C}_k} \mathcal{B}$.*

In Section 2.5, we discuss a generalization of Hella's bijection game with connections to symmetric circuits. This game proves to be the most useful formulation for a generalization to quantum pebble games, which is the subject of Part I of this thesis.

2.4 The Cai–Fürer–Immerman results

Cai, Fürer, and Immerman [CFI92] constructed a remarkable counterexample showing that FPC, even on τ_{graph} , does not capture all polynomial-time properties. I present their results in this section but omit the details of the construction; the interested reader may refer to [CFI92].

Theorem 2.23 [CFI92]. *There exist families of undirected graphs $(G_n)_n$ and $(H_n)_n$, $n \in \mathbb{Z}_{\geq 1}$, called the CFI graphs, with the following properties for each n :*

1. *G_n and H_n have the same number $v = O(n)$ of vertices with $v \geq n + 1$.²*
2. *Every vertex in G_n and H_n has degree at most 3.*
3. *$G_n \equiv_{\mathcal{C}_n} H_n$ when interpreted as τ_{graph} -structures.*
4. *G_n is not isomorphic to H_n .*

Furthermore, there is a polynomial-time algorithm which outputs “yes” on every G_n and “no” on every H_n .

The “furthermore” part of Theorem 2.23 implies that there is a polynomial-time τ_{graph} -property, the *CFI property* \mathcal{P}_{CFI} , such that $G_n \in \mathcal{P}_{\text{CFI}}$ but $H_n \notin \mathcal{P}_{\text{CFI}}$ for each n . Since $G_n \equiv_{\mathcal{C}_n} H_n$ for each n , Theorem 2.15 tells us that \mathcal{P}_{CFI} is not captured by FPC.

The authors prove that $G_n \equiv_{\mathcal{C}_n} H_n$ by providing a winning Duplicator strategy for the Immerman–Lander \mathcal{C}_n pebble game and applying Theorem 2.19. By Theorem 2.21, Duplicator also wins the corresponding n -pebble bijection game.

Cai et al. also proved that two graphs are equivalent under $\equiv_{\mathcal{C}_{k+1}}$ if and only if they are equivalent under the *k -dimensional Weisfeiler–Lehman method* [WL68; Wei76], an approximation algorithm for graph isomorphism. Theorem 2.23 thus disproves conjectures that the Weisfeiler–Lehman method might provide a polynomial-time graph isomorphism algorithm for graphs of bounded degree [CFI92].

²That $v \geq n + 1$ follows easily from properties 3 and 4, since Spoiler wins the n -pebble bijection game on any pair of non-isomorphic graphs on $v \leq n$ vertices simply by pebbling every vertex.

2.5 Connections to symmetric computation

This section is based in part on Section 5 of [Daw15b].

Though FPC does not capture all polynomial-time properties, Dawar [Daw15b] argues that the FPC-expressible properties form a natural class to study due in part to the more recent results of Anderson and Dawar [AD17] showing a connection to computation by symmetric circuits.

I leave a formal definition of symmetric circuits for Chapter 5, but in brief, a *Boolean circuit* is a directed acyclic graph in which we think of the vertices as *gates*. The gates with no incoming edges are called *input gates*, labelled x_1, \dots, x_m , and each non-input gate is labelled by a Boolean function, such as AND, OR, or NOT. One gate determines the output of the circuit, and we think of the circuit as computing a Boolean function $f : \{0, 1\}^m \rightarrow \{0, 1\}$. A *threshold circuit* is a Boolean circuit whose non-input gates are labelled by *threshold functions* $\text{Th}_{\geq k}^n$, which output 1 iff at least k of their n inputs are 1. The *size* of a Boolean circuit is its number of gates.

To encode a directed graph G on the vertices $[n]$ as inputs to a Boolean circuit, we need n^2 input gates, labelled $x_{(i,j)}$ for each $i, j \in [n]$: one for each of the *potential edges* of G [Daw15b]. The input gate $x_{(i,j)}$ gets the value 1 if the edge (i, j) appears in G and 0 otherwise. A Boolean circuit with n^2 input gates labelled like this is called a *graph circuit*.

Let Sym_n denote the group of permutations of $[n]$. A graph circuit is *graph symmetric* if, for every $\sigma \in \text{Sym}_n$, the permutation of the input gates given by

$$x_{(i,j)} \mapsto x_{(\sigma(i),\sigma(j))} \tag{2.12}$$

extends to an automorphism of the circuit: that is, the structure of the circuit is such that moving the input gates in accordance with (2.12) can be done without changing the circuit structure just by permuting some of the other gates. The output of a graph-symmetric circuit C on a graph G does not depend on the order in which the vertices of G are written—that is, it depends only on the isomorphism class of G [Daw15b].

Consider a family of graph-symmetric circuits $(C_n)_n$, where C_n accepts graphs on n vertices. $(C_n)_n$ defines a τ_{graph} -property \mathcal{P} , where for each graph G with n vertices, we have $G \in \mathcal{P}$ iff C_n outputs 1 on G . We say $(C_n)_n$ *computes* \mathcal{P} . Anderson and Dawar found that surprisingly, the FPC-expressible graph properties have a precise characterization in terms of symmetric circuits.

Theorem 2.24 [AD17]. *A τ_{graph} -property is computed by a polynomially uniform³ family of graph-symmetric threshold circuits if and only if it is captured by FPC.*

Theorem 2.24 allows us to interpret inexpressibility results for FPC as lower bounds on the size of uniform families of symmetric circuits computing a property. For instance, it follows that there is no polynomially uniform family of graph-symmetric threshold circuits computing the CFI property \mathcal{P}_{CFI} .

³A family of circuits $(C_n)_n$ is *polynomially uniform* if there is an algorithm computing C_n from n in time polynomial in n . Every polynomially uniform family of circuits has size polynomial in n .

Recall that we prove FPC-inexpressibility results using pebble games. Dawar [Daw15a] and Dawar and Wilenach [DW20; DW22] prove symmetric circuit lower bounds of this form using a direct pebble game argument, without reference to logic. To do so, they define a generalization of Hella’s bijection game which is suitable for proving lower bounds on circuit families exhibiting more refined symmetries.

Let \mathcal{A} and \mathcal{B} be finite τ -structures of the same size n , and suppose without loss of generality that they have the domain $[n]$. Let G be a group acting on $[n]$. (Without loss of generality, we may take $G \leq \text{Sym}_n$.)

Definition 2.25 [DW22]. The k -pebble G -bijection game on \mathcal{A} and \mathcal{B} is played using two sets of k pebbles, a_1, \dots, a_k and b_1, \dots, b_k . Initially, no pebbles are placed. Each round proceeds as follows:

1. Spoiler picks up a pair of pebbles (a_i, b_i) .
2. Duplicator chooses some $\sigma \in G$ such that for every pair of pebbles (a_j, b_j) which are placed on the structures, we have $\sigma(a_j) = b_j$.
3. Spoiler places a_i on some unpebbled element a of \mathcal{A} and places b_i on $\sigma(a)$.

The winning condition is the same as before.⁴

We abbreviate “ k -pebble G -bijection game” to “ (G, k) -pebble game”. To recover Hella’s bijection game, take $G = \text{Sym}_n$. The remainder of Part I is devoted to a quantum generalization of the (G, k) -pebble game, while Part II presents its applications to lower bounds for symmetric quantum circuits, generalizing Dawar and Wilenach’s technique.

2.5.1 From Sym_n to Alt_n

Except as noted, this section contains entirely original material.

By the observation that the (Sym_n, k) -pebble game is equivalent to Hella’s k -bijection game, we immediately obtain the following [Daw15a]:

Theorem 2.26 [Daw15a]. *Let $(G_n)_n$ and $(H_n)_n$ be the families of CFI graphs of Theorem 2.23, interpreted as τ_{graph} -structures, and suppose G_n and H_n have the same set of vertices V . Then Duplicator wins the (Sym_V, n) -pebble game on G_n and H_n .*

Proof. $G_n \equiv_{\mathcal{C}_n} H_n$ (Theorem 2.23), so by Corollary 2.22, Duplicator wins the n -bijection game on G_n and H_n . So by the observation, Duplicator wins the (Sym_V, n) -pebble game. \square

⁴Dawar and Wilenach’s definition in [DW22] actually uses a stronger definition of partial isomorphism which matches the classical restriction of the quantum notion of partial isomorphism introduced in Chapter 3.

For the quantum circuit lower bounds in Chapters 7 and 8, it is convenient to instead have families of structures on which Duplicator wins the (Alt_n, k) -pebble game, where $\text{Alt}_n \leq \text{Sym}_n$ is the *alternating group* consisting of all even permutations of $[n]$ [DM96]. The following original theorem provides a way to translate Duplicator strategies for the (Sym_n, k) -pebble game on graphs to the (Alt_n, k) -pebble game.

Theorem 2.27. *Let G and H be nonisomorphic graphs on the same set of vertices V , interpreted as τ_{graph} -structures, such that Duplicator wins the (Sym_V, k) -pebble game on G and H . There are nonisomorphic graphs G' and H' on vertices V' with $|V'| = |V| + k + 2$ such that Duplicator wins the $(\text{Alt}_{V'}, k)$ -pebble game on G' and H' .*

Proof. Add $k + 2$ isolated vertices to each of G and H to form G' and H' . Let I be the set of isolated vertices added; we have $V' = V \cup I$. In the $(\text{Alt}_{V'}, k)$ -pebble game on G' and H' , Duplicator will play only bijections that map vertices in V to vertices in V and vertices in I to vertices in I , so no pair of pebbles (a_i, b_i) will ever map a vertex in V to a vertex in I or vice versa. Our strategy is as follows: Suppose that in the (Sym_V, k) -pebble game, ignoring the vertices I , Duplicator would play $\sigma \in \text{Sym}_V$. Let $\pi \in \text{Sym}_I$ be a bijection on I respecting the pebbles placed on I , i.e., such that for every pair of pebbles (a_j, b_j) placed on I , $\pi(a_j) = b_j$. Since there are only k pebbles and $|I| = k + 2$, there are at least two distinct isolated vertices $i_1, i_2 \in I$ which are unpebbled in G' . So $\pi(i_1 i_2)$ also respects the pebbles on I . Thus, if $\sigma\pi$ (considered by abuse of notation as an element of $\text{Sym}_{V'}$) is an even permutation, Duplicator plays $\sigma\pi$; if $\sigma\pi$ is odd, then it plays $\sigma\pi(i_1 i_2)$, which is even. This strategy simulates the (Sym_V, k) -pebble game strategy on the reduction to V and wins since the pebbles on I cannot cause a partial isomorphism violation. \square

We usually have $k \leq |V|$ since Spoiler always wins if there are more pebbles than domain elements and the structures are nonisomorphic; then $|V'| \leq 2|V| + 2$ and so Theorem 2.27 involves merely a constant factor blowup. It can easily be generalized to arbitrary relational structures. Applying Theorem 2.27 to the CFI graphs, we obtain concrete graphs on which Duplicator wins the (Alt_n, k) -pebble game:

Corollary 2.28. *There are families of graphs $(G_n)_n$ and $(H_n)_n$, interpreted as τ_{graph} -structures, where G_n and H_n have vertices V with $|V| = O(n)$ such that each G_n and H_n are not isomorphic and Duplicator wins the (Alt_V, k) -pebble game on G_n and H_n for some $k = \Omega(n)$. Furthermore, there is a polynomial-time algorithm which outputs “yes” on every G_n and “no” on every H_n .*

Proof. Apply the transformation of Theorem 2.27 to the CFI graphs (Theorems 2.23, 2.26). For the “furthermore” part, the algorithm simply removes the $k + 2$ isolated vertices and applies the algorithm separating the CFI graphs (Theorem 2.23). \square

I call $(G_n)_n$ and $(H_n)_n$ the *Alt-CFI graphs*. There is therefore a polynomial-time τ_{graph} -property, the *Alt-CFI property* $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$, such that $G_n \in \mathcal{P}_{\text{CFI}}^{\text{Alt}}$ and $H_n \notin \mathcal{P}_{\text{CFI}}^{\text{Alt}}$ for each n . This property is used throughout Part II to prove lower bounds for Alt_n -symmetric circuits.

Chapter 3

New quantum pebble game framework

This chapter presents an original framework for formulating quantum pebble games. Except for the preliminaries in Section 3.1, this chapter contains entirely original material. The notions of support and partial isomorphism in Section 3.3.2 are based on [DW22].

In this chapter, I present a novel framework for a quantum extension of the classical (G, k) -pebble game of Definition 2.25. To my knowledge, this is the first attempt to formulate a quantum pebble game. I assume familiarity with basic quantum theory; a good introduction is [KLM06], and a standard reference is [NC10].

3.1 Preliminaries

We denote a Hilbert space by \mathcal{H} . All Hilbert spaces considered in this thesis are finite-dimensional and of the form $(\mathbb{C}^2)^{\otimes n}$ for some number of qubits n . We also write $(\mathbb{C}^2)^{\otimes S}$ when the qubits are labelled by elements of a set S . We use Dirac notation: denote a pure quantum state by a ket $|\psi\rangle \in \mathcal{H}$, its corresponding bra by $|\psi\rangle^\dagger = \langle\psi|$ (a member of the dual space \mathcal{H}^*), and the inner product of $|\psi\rangle$ and $|\varphi\rangle$ by $(\langle\psi|)(|\varphi\rangle) = \langle\psi|\varphi\rangle \in \mathbb{C}$, linear in the second argument. We use \otimes to denote the standard tensor product. We sometimes abbreviate $|\psi\rangle \otimes |\varphi\rangle$ to $|\psi\rangle|\varphi\rangle$ and $\langle\psi| \otimes \langle\varphi|$ to $\langle\psi|\langle\varphi|$. Every pure state $|\psi\rangle$ in this thesis is assumed to be normalized, i.e. $\langle\psi|\psi\rangle = 1$, unless otherwise specified. A *basis* for \mathcal{H} is a set of states $\{|b_i\rangle\}_i$ such that every $|\psi\rangle \in \mathcal{H}$ can be written as a finite complex linear combination of the basis states. A basis $\{|b_i\rangle\}_i$ is *orthonormal* if $\langle b_i|b_j\rangle = \delta_{ij}$ for all i, j , where $\delta_{ij} = 1$ if $i = j$ and 0 if $i \neq j$. The *computational basis* of $(\mathbb{C}^2)^{\otimes n}$ is an orthonormal basis given by $\{|b\rangle : b \in \{0, 1\}^n\}$.

An *operator* on $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ is a linear map $A : \mathcal{H} \rightarrow \mathcal{H}$, identified with a matrix in $\mathbb{C}^{2^n \times 2^n}$. We denote both the application of A to a state $|\psi\rangle \in \mathcal{H}$ and the composition of operators $A, B : \mathcal{H} \rightarrow \mathcal{H}$ by juxtaposition: $A|\psi\rangle = A(|\psi\rangle)$ and $AB = A \circ B$. We write $\langle\psi|A|\varphi\rangle$ for $\langle\psi|(A|\varphi\rangle)$. The *adjoint* of A is the unique operator $A^\dagger : \mathcal{H} \rightarrow \mathcal{H}$ such that $(\langle\psi|A|\varphi\rangle)^* = \langle\varphi|A^\dagger|\psi\rangle$ for all $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ [NC10], where z^* denotes the complex conjugate of $z \in \mathbb{C}$. The adjoint is identified with the conjugate transpose, and we have $(AB)^\dagger = B^\dagger A^\dagger$. Denote the identity operator by \mathbb{I} . An operator A is *normal* if $A^\dagger A = AA^\dagger$, *Hermitian* if $A = A^\dagger$, an *orthogonal projection* if $A^2 = A = A^\dagger$, and *unitary* if A is invertible and $A^\dagger = A^{-1}$. We also refer to

Hermitian operators as *observables*. We often refer to unitary operators simply as *unitaries*. Two operators $A, B : \mathcal{H} \rightarrow \mathcal{H}$ commute if $AB = BA$.

For any orthonormal basis $\{|b_i\rangle\}_i$ of \mathcal{H} , the *trace* of an operator A on \mathcal{H} is $\text{Tr}(A) = \sum_i \langle b_i | A | b_i \rangle$; its value is independent of the basis used [NC10]. The trace obeys the *cyclic property* $\text{Tr}(AB) = \text{Tr}(BA)$ [NC10]. A is *positive* if $\langle \psi | A | \psi \rangle$ is a nonnegative real number for all $|\psi\rangle \in \mathcal{H}$. A *density matrix* is a positive Hermitian operator ρ with $\text{Tr}(\rho) = 1$ and represents a *mixed state*, a statistical ensemble of pure states [NC10]. Every density matrix can be written as $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for some pure states $\{|\psi_i\rangle\}$ and some positive real coefficients $\{p_i\}$ with $\sum_i p_i = 1$ [KLM06]. Denote the set of density matrices on \mathcal{H} by $D(\mathcal{H})$.

If $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, let $\text{Tr}_2 : D(\mathcal{H}) \rightarrow D(\mathcal{H}_1)$ denote the partial trace operation which “traces out” system 2 given by the linear extension of the map $|a_i\rangle\langle a_j| \otimes |b_k\rangle\langle b_\ell| \mapsto |a_i\rangle\langle a_j| \otimes |b_\ell\rangle\langle b_k|$, where $\{|a_i\rangle\}_i$ and $\{|b_j\rangle\}_j$ are orthonormal bases for \mathcal{H}_1 and \mathcal{H}_2 respectively [KLM06]. Furthermore, if $\mathcal{H} = (\mathbb{C}^2)^{\otimes X}$ is composed of $|X|$ qubits labelled by elements of a finite set X and $S \subseteq X$ is nonempty, let $\text{Tr}_S : D((\mathbb{C}^2)^{\otimes X}) \rightarrow D((\mathbb{C}^2)^{\otimes(X \setminus S)})$ denote the partial trace operation which “traces out” the qubits S given by viewing $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1 = (\mathbb{C}^2)^{\otimes(X \setminus S)}$ and $\mathcal{H}_2 = (\mathbb{C}^2)^{\otimes S}$, then taking $\text{Tr}_S = \text{Tr}_2$. Additionally, let $\text{Tr}_{\overline{S}} = \text{Tr}_{X \setminus S} : D((\mathbb{C}^2)^{\otimes X}) \rightarrow D((\mathbb{C}^2)^{\otimes S})$ denote the partial trace operation which “traces out” the other qubits, leaving only the qubits S . If $x \in X$ is a single qubit, write $\text{Tr}_{\overline{x}}$ for $\text{Tr}_{\{x\}}$.

If G and H are groups, write $H \leq G$ to mean that H is a subgroup of G . If $\varphi : G \rightarrow H$ is a group homomorphism and $K \leq G$, write $\varphi(K) = \{\varphi(k) : k \in K\}$; it is a subgroup of H . For a finite set S , let Sym_S denote the *symmetric group* of all permutations on S . Let $\text{Alt}_S \leq \text{Sym}_S$ denote the *alternating group* of even permutations on S . Write Sym_n for $\text{Sym}_{[n]}$ and Alt_n for $\text{Alt}_{[n]}$. If G is a group acting on S and $s \in S$, let $\text{Stab}_G(s) = \{\sigma \in G : \sigma(s) = s\}$ denote the stabilizer group of s and $\text{Orb}_G(s) = \{\sigma(s) : \sigma \in G\}$ denote the orbit of s under G . If $T \subseteq S$, following the notation of [DW22], let $\sigma(T) = \{\sigma(t) : t \in T\}$, let $\text{Stab}_G(T) = \bigcap_{t \in T} \text{Stab}_G(t)$ denote the *pointwise stabilizer* of T , and let $\text{SetStab}_G(T) = \{\sigma \in G : \sigma(T) = T\}$ denote the *setwise stabilizer* of T under G . I omit G when it is clear from context.

Denote the group of unitaries on \mathcal{H} by $\text{U}(\mathcal{H})$. If $\mathcal{H}_S = (\mathbb{C}^2)^{\otimes S}$ and G is a group acting on S , there is a natural embedding $G \rightarrow \text{U}(\mathcal{H}_S)$ which maps $\sigma \in G$ to the unitary on \mathcal{H}_S which permutes the qubits according to the action of σ . Write U_σ for this unitary, which is defined as follows: If $|\psi\rangle = |\psi_{s_1}\rangle \otimes \cdots \otimes |\psi_{s_n}\rangle \in \mathcal{H}_S$ where $S = \{s_1, \dots, s_n\}$, then $U_\sigma|\psi\rangle = |\psi_{\sigma^{-1}(s_1)}\rangle \otimes \cdots \otimes |\psi_{\sigma^{-1}(s_n)}\rangle$. That is, qubit $s \in S$ of a state $|\psi\rangle \in \mathcal{H}_S$ corresponds to qubit $\sigma(s)$ of $U_\sigma|\psi\rangle$: hence qubit s of $U_\sigma|\psi\rangle$ is qubit $\sigma^{-1}(s)$ of $|\psi\rangle$. Write $\Gamma_G = \{U_\sigma : \sigma \in G\}$ for the image of G in $\text{U}(\mathcal{H}_S)$ under this embedding.

I generally write G for “classical” symmetry groups, often taken to be subgroups of Sym_n , and $\Gamma \leq \text{U}(\mathcal{H})$ for groups of unitaries. If $U \in \text{U}(\mathcal{H})$ and $\Gamma \leq \text{U}(\mathcal{H})$, let $U\Gamma = \{UV : V \in \Gamma\}$ and $\Gamma U = \{VU : V \in \Gamma\}$.

3.1.1 Encoding structures as quantum states

Fix a relational vocabulary $\tau = (R_1^{r_1}, \dots, R_k^{r_k})$, and let $\text{fin}_n[\tau]$ denote the τ -structures of size $n \in \mathbb{Z}_{\geq 1}$. For simplicity, assume every structure in $\text{fin}_n[\tau]$ has domain $[n]$. To define a quantum pebble game, we need to encode the τ -structures as quantum states: we wish to define a Hilbert space \mathcal{H}_n^τ such that each $\mathcal{A} \in \text{fin}_n[\tau]$ is encoded as a computational basis state $|\mathcal{A}\rangle \in \mathcal{H}_n^\tau$.

We can encode each structure $\mathcal{A} \in \text{fin}_n[\tau]$ as a bitstring $b(\mathcal{A})$ of length $\ell_\tau(n) = \sum_{i=1}^k n^{r_i}$ as follows. Index the bitstring by the tuples

$$Q^\tau = \{(i, n_1, \dots, n_{r_i}) : i \in [k], n_1, \dots, n_{r_i} \in [n]\} \quad (3.1)$$

which we refer to as *qubit labels*, and define the bit labelled by each $(i, n_1, \dots, n_{r_i}) \in Q^\tau$ as

$$b(\mathcal{A})_{(i, n_1, \dots, n_{r_i})} = \begin{cases} 1 & \text{if } (n_1, \dots, n_{r_i}) \in R_i^\mathcal{A} \\ 0 & \text{if } (n_1, \dots, n_{r_i}) \notin R_i^\mathcal{A} \end{cases} \quad (3.2)$$

This encoding forms a bijection between the bitstrings $\{0, 1\}^{\ell_\tau(n)}$ and the structures in $\text{fin}_n[\tau]$. (Observe furthermore that $\ell_\tau(n)$ is polynomial in n .) We can then define

$$\mathcal{H}_n^\tau = (\mathbb{C}^2)^{\otimes Q^\tau} \quad (3.3)$$

and we encode each structure $\mathcal{A} \in \text{fin}_n[\tau]$ as the computational basis state $|\mathcal{A}\rangle = |b(\mathcal{A})\rangle$. We often abbreviate (i, n_1, \dots, n_{r_i}) to (i, \vec{n}) .

We refer to general states $|A\rangle \in \mathcal{H}_n^\tau$ as *quantum τ -structures*. One can think of them either as superpositions $\sum_i \alpha_i |\mathcal{A}_i\rangle$ of τ -structures or as quantum generalizations of τ -structures in which whether each query $R_i(a_1, \dots, a_{r_i})$ holds is given by a qubit, which may be entangled with other queries. In the latter sense, they can be thought of as quantum generalizations of “probabilistic τ -structures”, in which each query $R_i(a_1, \dots, a_{r_i})$ is assigned a probability $p \in [0, 1]$ of holding. For instance, the quantum τ_{graph} -structures given by $\mathcal{H}_n^{\tau_{\text{graph}}}$ correspond precisely to the “quantum graphs” defined by Freedman, Lovász, and Schrijver [FLS06].

The action of a group G on the domain $[n]$ of \mathcal{A} , as used in the classical (G, k) -pebble game, can be extended to an action on Q^τ by letting $\sigma(i, \vec{n}) = (i, \sigma(\vec{n}))$, where if $\vec{n} = (n_1, \dots, n_{r_i})$ then $\sigma(\vec{n}) = (\sigma(n_1), \dots, \sigma(n_{r_i}))$. $\Gamma_G \leq \text{U}(\mathcal{H}_n^\tau)$ is then the group of unitaries which permutes the qubits according to G : we say Γ_G is the *classical unitary group* corresponding to G .

3.2 Reformulation of the (G, k) -pebble game

We begin with a reformulation of the classical (G, k) -pebble game of Dawar and Wilenach [DW22] which is equivalent to the formulation of Definition 2.25, but more readily admits a quantum generalization. As before, let \mathcal{A} and \mathcal{B} be finite τ -structures of the same size n . As in [DW22], by fixing bijections from the domains of \mathcal{A} and \mathcal{B} to $[n]$, we may assume without loss of generality that both structures have domain $[n]$. Let $G \leq \text{Sym}_n$.

Definition 3.1. The (G, k) -pebble game on \mathcal{A} and \mathcal{B} is defined as follows. The state of the game consists of a set $P \subseteq [n]$ with $|P| \leq k$ of pebbled elements and a permutation $\sigma \in G$. Initially, no pebbles are placed and σ is the identity element of G . Each round proceeds as follows:

1. Optionally, Spoiler removes an element from P . (If $|P| = k$, Spoiler must remove an element.)
2. Duplicator chooses some $\rho \in \text{Stab}_G(P)$, the pointwise stabilizer of P , and sets $\sigma := \sigma\rho$.
3. Spoiler chooses an element $a \in [n] \setminus P$ and adds it to P .

We define the partial isomorphism property as follows:

Definition 3.2. A permutation $\sigma \in G$ is a *partial isomorphism* from \mathcal{A} to \mathcal{B} with respect to a set of pebbled elements $P \subseteq [n]$ if the function $\sigma(-) : P \rightarrow \sigma(P)$ given by the action of σ restricted to P , $a \mapsto \sigma(a)$, is a partial isomorphism from \mathcal{A} to \mathcal{B} .

At the end of each round, Spoiler wins if σ fails to form a partial isomorphism from \mathcal{A} to \mathcal{B} with respect to P . Otherwise, play continues; Duplicator wins if it has a strategy to play forever.

Proposition 3.3. *The reformulated (G, k) -pebble game defined by Definition 3.1 is equivalent to the original game defined by [DW22] (Definition 2.25).*

Proof. There is a correspondence between the states of the games and between the options offered to the players in each game. The pebbled elements $P = \{a_1, \dots, a_\ell\} \subseteq \mathcal{A}$ correspond to the currently pebbled elements a_1, \dots, a_ℓ of \mathcal{A} in the original game. The permutation $\sigma \in G$ corresponds to Duplicator's most recently chosen σ , which maps each pebble a_i on \mathcal{A} to the pebble b_i on \mathcal{B} : hence the locations of the pebbles b_1, \dots, b_ℓ in the original game are just $\sigma(a_1), \dots, \sigma(a_\ell)$. The action of σ restricted to P is then just the function $a_i \mapsto b_i$ mapping the pebbles on \mathcal{A} to those on \mathcal{B} , so the notions of partial isomorphism in both games are equivalent.

Spoiler's removing an element from P in Step 1 corresponds to picking up a pair of previously placed pebbles, and adding the element a to P in Step 3 corresponds to placing the pair of pebbles $(a, \sigma(a))$. It remains to show that Duplicator chooses from the same permutations in Step 2 in both games. In the original game, Duplicator may choose any $\sigma' \in G$ such that $\sigma'(a_i) = \sigma(a_i) = b_i$ for each $a_i \in P$. But then $\sigma^{-1}\sigma'$ stabilizes each $a \in P$, so $\sigma^{-1}\sigma' \in \text{Stab}_G(P)$, and so Duplicator can play σ' in the reformulated game by choosing $\rho = \sigma^{-1}\sigma'$ and setting $\sigma := \sigma\rho = \sigma'$. Conversely, if Duplicator chooses $\rho \in \text{Stab}_G(P)$ in the reformulated game, then $\sigma\rho$ still maps each pebble a_i to $\sigma\rho(a_i) = \sigma(a_i) = b_i$, so Duplicator can play $\sigma\rho$ in the original game. Hence Duplicator has exactly the same set of options in both games in Step 2. \square

One insight offered by this reformulation is that pebbles can be viewed as *restrictions* on the permutations that Duplicator may choose and on the domain elements which may be “observed” to test for partial isomorphism. This idea is developed further in the quantum framework.

3.3 A framework for quantum pebble games

We now generalize our reformulated (G, k) -pebble game. For the rest of this chapter, fix a relational vocabulary τ and a domain size n . The game will be played on quantum τ -structures $|A\rangle, |B\rangle \in \mathcal{H}_n^\tau$, which are not necessarily encodings of classical structures. We replace the classical symmetry group G with an arbitrary group of unitaries $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$; in Part II, these will correspond to the symmetries of a quantum circuit. In the classical restriction, Γ is a classical unitary group Γ_G .

3.3.1 Pebbles are self-normalizing subgroups

Intuitively, placing a pebble just restricts the symmetries that Duplicator can choose. We formalize this intuition by defining pebbles as subgroups of Γ obeying certain properties.

Definition 3.4. Given a group $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$, a *pebble set* \mathcal{P} for Γ is a set of subgroups of Γ , called *pebble groups* or simply *pebbles* and denoted $\Gamma_p \in \mathcal{P}$, obeying the following properties:

- (a) \mathcal{P} is closed under conjugation by Γ : for every $\Gamma_p \in \mathcal{P}$ and every $U \in \Gamma$, $U\Gamma_p U^\dagger \in \mathcal{P}$.
- (b) Each pebble group $\Gamma_p \in \mathcal{P}$ is a *self-normalizing subgroup* of Γ : for every $U \in \Gamma$, if $U\Gamma_p U^\dagger = \Gamma_p$ then $U \in \Gamma_p$.

These properties about the behaviour of pebbles under conjugation are the essential technical properties needed for the proofs in Chapters 7 and 8 in Part II; we will see that they hold in the classical case.

Each pebble group $\Gamma_p \in \mathcal{P}$ is just the subgroup of Γ of symmetries which “respect the pebble”—in the classical case, stabilizing a particular element. If $P \subseteq \mathcal{P}$ is a set of pebbles, we write $\bigcap P := \bigcap_{\Gamma_p \in P} \Gamma_p$ for the intersection of the pebble groups in P , which is just the group of symmetries respecting all the pebbles in P . By convention, we set $\bigcap \emptyset := \Gamma$.

To recover the classical case, in which each pebble stabilizes a domain element under the action of a classical symmetry group $G \leq \mathrm{Sym}_n$, we require the following property of G :

Definition 3.5. A permutation group $G \leq \mathrm{Sym}_n$ has *distinct stabilizers* if for every $a, b \in [n]$ with $a \neq b$, we have $\mathrm{Stab}_G(a) \neq \mathrm{Stab}_G(b)$.

We can then set the pebbles as follows.

Definition 3.6. Suppose $\Gamma_G \leq \mathrm{U}(\mathcal{H}_n^\tau)$ is the classical unitary group corresponding to a group $G \leq \mathrm{Sym}_n$ which has distinct stabilizers, and let $\varphi : G \rightarrow \Gamma_G$ be the isomorphism mapping $\sigma \mapsto U_\sigma$. The *classical pebble set* for Γ_G is

$$\mathcal{P}_G = \{\varphi(\mathrm{Stab}_G(a)) : a \in [n]\}. \quad (3.4)$$

That is, the classical pebble groups in \mathcal{P}_G are just the subgroups which do not move each domain element. Using the distinct stabilizers property, we can show that \mathcal{P}_G is a pebble set by the above definition.

Proposition 3.7. *For every $G \leq \text{Sym}_n$ with distinct stabilizers, \mathcal{P}_G obeys the conditions of Definition 3.4.*

Proof. Observe that $\sigma \text{Stab}_G(a) \sigma^{-1} = \text{Stab}_G(\sigma a)$ for each $\sigma \in G$. For (a), for each $U_\sigma \in \Gamma_G$ and each pebble group $\varphi(\text{Stab}_G(a))$ we have

$$U_\sigma \varphi(\text{Stab}_G(a)) U_\sigma^\dagger = \varphi(\sigma \text{Stab}_G(a) \sigma^{-1}) = \varphi(\text{Stab}_G(\sigma a)) \in \mathcal{P}_G. \quad (3.5)$$

For (b), suppose that $U_\sigma \varphi(\text{Stab}_G(a)) U_\sigma^\dagger = \varphi(\text{Stab}_G(a))$: that is, $\sigma \text{Stab}_G(a) \sigma^{-1} = \text{Stab}_G(a)$. Then $\text{Stab}_G(\sigma a) = \text{Stab}_G(a)$, so since G has distinct stabilizers, $\sigma a = a$ and so $\sigma \in \text{Stab}_G(a)$, so $U_\sigma \in \varphi(\text{Stab}_G(a))$. \square

When we refer to a classical unitary group Γ_G or its classical pebble set \mathcal{P}_G in the remainder of this thesis, we always implicitly assume that G has distinct stabilizers.

We now discuss the distinct stabilizers property further. It is a natural condition in the context of pebble games because the function of placing a pebble on $a \in [n]$ in the reformulated game is to restrict Duplicator's playable permutations to $\text{Stab}_G(a)$, so if $\text{Stab}(a) = \text{Stab}(b)$ for some $a \neq b$, then there is no difference between pebbling a and b . It is also not a very restrictive condition: recall that G is not a group of automorphisms of the input structures, but rather a large group of bijections from which Duplicator may choose. In our applications, we typically take G to be Sym_n or Alt_n , and it is easy to show that both of these groups have distinct stabilizers for sufficiently large n :

Lemma 3.8. *Sym_n and Alt_n have distinct stabilizers whenever $n \geq 4$.*

Proof. Suppose $n \geq 4$ and let $a \in [n]$. Let $b, c, d \in [n]$ such that a, b, c, d are all distinct. Then $(b\ c\ d)$ is an even permutation which stabilizes a but not b , so $\text{Stab}(a) \neq \text{Stab}(b)$. \square

Our results in Part II are asymptotic, so we typically may ignore the case where $n < 4$.

We work with the distinct stabilizers property because it is a more interpretable sufficient condition for property (b) of Definition 3.4, that each pebble in \mathcal{P}_G is a self-normalizing subgroup of Γ_G (or equivalently, that each $\text{Stab}_G(a)$ is self-normalizing in G). This condition is needed in Chapters 7 and 8 due to our abstract approach which treats pebbles as subgroups; Dawar and Wilzenach's [DW22] classical technique presented in Chapter 6, which works directly with the pebbled elements, does not require this property.

Finally, note that if G is transitive (that is, for every $a, b \in [n]$, there is some $\sigma \in G$ with $\sigma a = b$), it is not hard to show that the distinct stabilizers property is in fact both necessary and sufficient for each $\text{Stab}_G(a)$ to be self-normalizing in G .

3.3.2 Base observables and partial isomorphism

To provide a flexible framework for how we recover information from the quantum states on which the game is played, we define partial isomorphism in terms of observables. The definition of partial isomorphism here is a generalization of that of Dawar and Wilsenach [DW22].

Definition 3.9. A *base observable set* \mathcal{O} for a group $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$ is a set of observables on \mathcal{H}_n^τ which is closed under conjugation by Γ : for every $O \in \mathcal{O}$ and every $U \in \Gamma$, $OUU^\dagger \in \mathcal{O}$.

Fix a group $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$ and a pebble set \mathcal{P} . The elements of \mathcal{O} are called *base observables*, and they are the only way we are allowed to obtain information about the quantum τ -structures. Specifically, if $|A\rangle \in \mathcal{H}_n^\tau$ is a state and $O \in \mathcal{O}$ is a base observable, we evaluate the *expectation value* $\langle A|O|A\rangle$ to obtain information about $|A\rangle$. The quantity $\langle A|O|A\rangle$ corresponds physically to the mean value obtained by measuring the observable O on the state $|A\rangle$ [NC10]. These possible measurement values are the eigenvalues of O ; hence for simplicity, we usually take the base observables to be orthogonal projections because their eigenvalues are just 0 and 1 [NC10].

Definition 3.10. The *classical base observable set* for a classical unitary group Γ_G on a Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes m}$ of m qubits is $\mathcal{O}_{\text{clas}} = \{O_i : i \in [m]\}$, where

$$O_i = |1\rangle_i \langle 1|_i \otimes \mathbb{I}_{[m] \setminus \{i\}}. \quad (3.6)$$

The subscripts indicate the qubits each tensor product component acts upon: each observable O_i applies the projection $|1\rangle\langle 1|$ on the i th qubit and acts trivially on the other qubits. That is, it is a measurement of the i th qubit in the computational basis.

Observe that for any $U_\sigma \in \Gamma_G$ we have $U_\sigma O_i U_\sigma^\dagger = O_{\sigma(i)}$. For \mathcal{H}_n^τ , we can write the classical base observables as $O_{(i,\vec{n})}$ for each qubit label $(i,\vec{n}) \in Q^\tau$. Then for any τ -structure \mathcal{A} , $\langle \mathcal{A}|O_{(i,\vec{n})}|\mathcal{A}\rangle$ is 1 if $\vec{n} \in R_i^\mathcal{A}$ and 0 otherwise; hence the classical base observables just ask each relational query. Furthermore, we have $U_\sigma O_{(i,\vec{n})} U_\sigma^\dagger = O_{(i,\sigma(\vec{n}))}$.

We now give a new definition of partial isomorphism in terms of base observables. Because we define pebbles abstractly as subgroups of Γ , our notion of partial isomorphism is abstract and based on the concept of support.

Definition 3.11. A set of pebbles $P \subseteq \mathcal{P}$ *supports* an observable O if every $U \in \bigcap P$ commutes with O .

Note that a unitary U commutes with O iff $OUU^\dagger = O$. If $P \subseteq \mathcal{P}$ supports O , then for every $U \in \bigcap P$ we have $\langle A|OUU^\dagger|A\rangle = \langle A|O|A\rangle$: that is, the value of O on $|A\rangle$ is invariant under permuting $|A\rangle$ by any $U \in \bigcap P$. Hence, restricting the permutations to $\bigcap P$ fixes the value of O . Thus in the classical case, P supports $O_{(i,\vec{n})}$ if P contains the pebble stabilizing each element of $\vec{n} = (n_1, \dots, n_{r_i})$.

Definition 3.12. Let $P \subseteq \mathcal{P}$ be a set of pebbles, let \mathcal{O} be a set of base observables for Γ , and let $|A\rangle, |B\rangle \in \mathcal{H}_n^\tau$. A unitary $U \in \Gamma$ is an \mathcal{O} -partial isomorphism with respect to P from $|A\rangle$ to $|B\rangle$ if for every base observable $O \in \mathcal{O}$ which is supported by P , we have $\langle A|O|A\rangle = \langle B|OUU^\dagger|B\rangle$.

Informally, U is an \mathcal{O} -partial isomorphism if $|A\rangle$ and $U^\dagger|B\rangle$ are indistinguishable to every base observable whose value is invariant under every symmetry which respects the pebbles. We now show that this definition is at least as strong as the classical notion of partial isomorphism.

Proposition 3.13. Let $\Gamma_G \leq \mathrm{U}(\mathcal{H}_n^\tau)$ be a classical unitary group and let \mathcal{P}_G be its classical pebble set. Suppose $P \subseteq \mathcal{P}_G$ are the classical pebble groups corresponding to the stabilizers of some set $P' \subseteq [n]$ of domain elements. Let \mathcal{A}, \mathcal{B} be τ -structures. If $U_\sigma \in \Gamma_G$ is an $\mathcal{O}_{\text{clas}}$ -partial isomorphism with respect to P from $|\mathcal{A}\rangle$ to $|\mathcal{B}\rangle$, then σ is a partial isomorphism with respect to P' from \mathcal{A} to \mathcal{B} .

Proof. For every $n_1, \dots, n_{r_i} \in P'$, $\bigcap P$ contains the pebble stabilizing each of n_1, \dots, n_{r_i} , so P supports each $O_{(i, \vec{n})} = |1\rangle_{(i, \vec{n})}\langle 1|_{(i, \vec{n})} \otimes \mathbb{I} \in \mathcal{O}_{\text{clas}}$, where $\vec{n} = (n_1, \dots, n_{r_i})$. So if $U_\sigma \in \Gamma_G$ is an $\mathcal{O}_{\text{clas}}$ -partial isomorphism from $|\mathcal{A}\rangle$ to $|\mathcal{B}\rangle$, then $\langle \mathcal{A}|O_{(i, \vec{n})}|\mathcal{A}\rangle = \langle \mathcal{B}|U_\sigma O_{(i, \vec{n})}U_\sigma^\dagger|\mathcal{B}\rangle = \langle \mathcal{B}|O_{(i, \sigma(\vec{n}))}|\mathcal{B}\rangle$, and so $\vec{n} \in R_i^{\mathcal{A}}$ iff $\sigma(\vec{n}) \in R_i^{\mathcal{B}}$. \square

Note that the converse does not necessarily hold, because P might support base observables $O_{(i, \vec{n})} \in \mathcal{O}_{\text{clas}}$ where some domain element $n_j \in \vec{n}$ is not in P' if n_j happens to be stabilized by every permutation in G stabilizing P' . (This technicality also occurs in the original formulation of the classical (G, k) -pebble game in [DW22], which defines partial isomorphism similarly.) Under some particular conditions which are relevant for the CFI results (Section 2.4), however, the notions of partial isomorphism are equivalent.

Lemma 3.14. In the setting of Proposition 3.13, if $G = \mathrm{Sym}_n$ or Alt_n and $|P| \leq n - 3$, then $U_\sigma \in \Gamma_G$ is an $\mathcal{O}_{\text{clas}}$ -partial isomorphism with respect to P from $|\mathcal{A}\rangle$ to $|\mathcal{B}\rangle$ if and only if σ is a partial isomorphism with respect to P' from \mathcal{A} to \mathcal{B} .

Proof. Since $|P'| = |P| \leq n - 3$ and $G = \mathrm{Sym}_n$ or Alt_n , every domain element $j \in [n]$ which is not in P' is moved by some even permutation $\sigma \in \mathrm{Stab}_G(P')$, namely the cyclic permutation $(j \ j' \ j'')$ between j and two other distinct domain elements $j', j'' \notin P'$. So each base observable $O_{(i, \vec{n})} \in \mathcal{O}_{\text{clas}}$ is supported by P if and only if $\vec{n} \subseteq P'$. As above, for each $U_\sigma \in \Gamma_G$, $\langle \mathcal{A}|O_{(i, \vec{n})}|\mathcal{A}\rangle = \langle \mathcal{B}|U_\sigma O_{(i, \vec{n})}U_\sigma^\dagger|\mathcal{B}\rangle$ is equivalent to $\vec{n} \in R_i^{\mathcal{A}}$ holding just when $\sigma(\vec{n}) \in R_i^{\mathcal{B}}$, so the notions of partial isomorphism are equivalent. \square

3.4 The quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game

We are ready to define the generalized pebble game. Let $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$ be a group of unitaries, \mathcal{P} be a pebble set for Γ , \mathcal{O} be a base observable set for Γ , and k be an integer. Let $|A\rangle, |B\rangle \in \mathcal{H}_n^\tau$ be quantum τ -structures.

Definition 3.15. The *quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game* on $|A\rangle$ and $|B\rangle$ is defined as follows. The state of the game consists of a subset of pebbles $P \subseteq \mathcal{P}$ with $|P| \leq k$ and a unitary $U \in \Gamma$. Initially, no pebbles are placed and $U = \mathbb{I}$. Each round proceeds as follows.

1. Optionally, Spoiler removes a pebble from P . (If $|P| = k$, Spoiler must remove a pebble.)
2. Duplicator chooses a unitary $V \in \cap P$ and sets $U := UV$.
3. Spoiler chooses a pebble from $\mathcal{P} \setminus P$ and adds it to P .

Spoiler wins if U is not an \mathcal{O} -partial isomorphism from $|A\rangle$ to $|B\rangle$ with respect to P . Otherwise, play continues, and Duplicator wins if it has a strategy to play forever.

We recover the classical (G, k) -pebble game on \mathcal{A} and \mathcal{B} , except for the partial isomorphism condition, by setting $\Gamma = \Gamma_G$, $\mathcal{P} = \mathcal{P}_G$, $\mathcal{O} = \mathcal{O}_{\text{clas}}$, $|A\rangle = |\mathcal{A}\rangle$, and $|B\rangle = |\mathcal{B}\rangle$. Since $\mathcal{O}_{\text{clas}}$ -partial isomorphism is, in general, strictly stronger than the classical notion of partial isomorphism as discussed above, the resulting quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game can be harder for Duplicator and easier for Spoiler than the (G, k) -pebble game. (The quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game on classical structures is in fact identical to the version of the (G, k) -pebble game originally defined by Dawar and Wilzenach [DW22].) Due to Lemma 3.14, however, the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -game still cannot distinguish the CFI graphs:

Proposition 3.16. *Let $(G_n)_n$ and $(H_n)_n$ be the families of CFI graphs of Theorem 2.23, interpreted as τ_{graph} -structures, and suppose G_n and H_n have the same set of vertices V . Let $G = \text{Sym}_V$. Then for $n \geq 3$, Duplicator wins the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game on G_n and H_n for some $k = \Omega(n)$.*

Proof. By Theorem 2.26, Duplicator wins the (Sym_V, n) -pebble game on G_n and H_n . Let $k = n - 2$: reducing the number of pebbles only makes a pebble game easier for Duplicator, so Duplicator also wins the (Sym_V, k) -pebble game on G_n and H_n . Since $n \leq |V| - 1$ by Theorem 2.23, we have $k \leq |V| - 3$, so by Lemma 3.14, $\mathcal{O}_{\text{clas}}$ -partial isomorphism is equivalent to classical partial isomorphism in this setting with at most k pebbles. So from the discussion above, Duplicator wins the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game on G_n and H_n . \square

By the same proof, we have the analogous result for $G = \text{Alt}_n$:

Proposition 3.17. *Let $(G_n)_n$ and $(H_n)_n$ be the families of Alt-CFI graphs of Corollary 2.28, interpreted as τ_{graph} -structures, and suppose G_n and H_n have the same set of vertices V . Let $G = \text{Alt}_V$. Then for $n \geq 3$, Duplicator wins the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game on G_n and H_n for some $k = \Omega(n)$.*

Propositions 3.16 and 3.17 are important in applications since they provide a methodology for showing that a model of computation cannot compute the CFI or Alt-CFI property by showing that it cannot distinguish between inputs on which Duplicator wins the corresponding

pebble game. Dawar applies this methodology to symmetric classical circuits in [Daw15a], and Part II generalizes the technique to some classes of symmetric quantum circuits.

The notion of quantum pebble game of Definition 3.15 defined in this chapter is very general, giving us several directions for quantum extension: by using a larger group of unitaries Γ , by allowing more general pebbles in \mathcal{P} or base observables in \mathcal{O} , and by playing the game on quantum structures $|A\rangle$ and $|B\rangle$. This framework provides a starting point for any investigation of quantum pebble games, which might begin by taking a special case of the $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game appropriate to the application. In the next chapter, we do just this: we derive a less general but more directly useful and interpretable quantum pebble game which we apply in Part II.

Chapter 4

Partial trace-based quantum pebble game

This chapter derives a concrete quantum pebble game from the framework presented in Chapter 3. Except where noted, this chapter contains entirely original material.

In this chapter, we derive a more operational special case of the quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game. The resulting *partial trace-based quantum pebble game* is simpler than the general game; we will apply it to prove our results in Part II, and it may also be of independent interest as a natural quantum pebble game.

Fix a relational vocabulary τ and a domain size n . We begin by asking which base observable sets \mathcal{O} are reasonable to choose. As before, for simplicity, we use only orthogonal projections, which have eigenvalues 0 and 1. The classical base observable set $\mathcal{O}_{\text{clas}}$ has one base observable $|1\rangle_i\langle 1|_i \otimes \mathbb{I}$ measuring each qubit i in the computational basis. This works well for computational basis states $|\mathcal{A}\rangle$ but is not enough for more general states: for instance, computational basis measurements cannot distinguish the qubit states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Thus we wish to include in \mathcal{O} observables measuring each qubit in every basis: that is, we would like to include $|\chi\rangle_i\langle\chi|_i \otimes \mathbb{I}$ for every qubit i and every single-qubit state $|\chi\rangle$.

This strategy is enough to distinguish distinct *product states*, which are states of the form $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle$ where each $|\psi_i\rangle$ is a single-qubit state; they have no entanglement between qubits. States with entanglement might not be distinguished by single-qubit measurements, however: e.g., the states $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ (two of the states of the *Bell basis* [KLM06]) cannot be distinguished by any single-qubit measurement since their single-qubit partial traces are identical [NC10].

Thus in general we must measure several qubits at a time. With an eye to the applications to quantum circuits in Part II, suppose we wish to measure at most ℓ qubits at once.

Definition 4.1 [AKS12]. An ℓ -local rank 1 projector on an m -qubit Hilbert space is an orthogonal projection of the form $\Pi = |\chi\rangle_S\langle\chi|_S \otimes \mathbb{I}_{[m]\setminus S}$ for some $S \subseteq [m]$ with $|S| = \ell$ and some $|\chi\rangle \in (\mathbb{C}^2)^{\otimes \ell}$, where the subscripts again specify the subsystems: Π projects onto $|\chi\rangle$ on the qubits in S and acts trivially on the other qubits. We say Π *acts on* S .

Strictly speaking, the rank of Π is 1 only in its restriction to the qubits S , $|\chi\rangle\langle\chi|$. We say an operator is ℓ -local if it acts nontrivially on at most ℓ qubits.

Definition 4.2. The ℓ -local base observable set \mathcal{O}_ℓ for \mathcal{H}_n^τ is the set of all ℓ' -local rank 1 projectors on \mathcal{H}_n^τ for all positive integers $\ell' \leq \ell$.

For \mathcal{O}_ℓ to be closed under conjugation by Γ as required by Definition 3.9, we require Γ to map ℓ -local rank 1 projectors to other ℓ -local rank 1 projectors. This is the case for each classical unitary group Γ_G , which just permutes the qubits, as well as, for instance, unitary groups Γ whose elements permute the qubits and apply some local unitaries to each qubits.

Let $O_\chi = |\chi\rangle_S\langle\chi|_S \otimes \mathbb{I}$ be an ℓ -local rank 1 projector acting on a set of qubits S with $|S| = \ell$ and let $|\psi\rangle, |\varphi\rangle \in \mathcal{H}_n^\tau$. Let $\rho_\psi = |\psi\rangle\langle\psi|$ and $\rho_\varphi = |\varphi\rangle\langle\varphi|$. Observe that

$$\langle\psi|O_\chi|\psi\rangle = \text{Tr}((|\chi\rangle_S\langle\chi|_S \otimes \mathbb{I})|\psi\rangle\langle\psi|) \quad (4.1)$$

$$= \text{Tr}(|\chi\rangle\langle\chi| \text{Tr}_{\bar{S}}(|\psi\rangle\langle\psi|)) \quad (4.2)$$

$$= \langle\chi|\text{Tr}_{\bar{S}}(\rho_\psi)|\chi\rangle. \quad (4.3)$$

Here equation (4.2) follows from Lemma A.1 (proven in Appendix A) and moves from the Heisenberg picture to the Schrödinger picture. Hence, $\langle\psi|O_\chi|\psi\rangle = \langle\varphi|O_\chi|\varphi\rangle$ for every ℓ -local rank 1 projector O_χ acting on the qubits S if and only if

$$\langle\chi|\text{Tr}_{\bar{S}}(\rho_\psi)|\chi\rangle = \langle\chi|\text{Tr}_{\bar{S}}(\rho_\varphi)|\chi\rangle \quad (4.4)$$

for all $|\chi\rangle \in (\mathbb{C}^2)^{\otimes\ell}$. But then by Lemma A.2, $\text{Tr}_{\bar{S}}(\rho_\psi) = \text{Tr}_{\bar{S}}(\rho_\varphi)$. We obtain the following:

Lemma 4.3. *For every $|\psi\rangle, |\varphi\rangle \in \mathcal{H}_n^\tau$, $\langle\psi|O_\chi|\psi\rangle = \langle\varphi|O_\chi|\varphi\rangle$ for every ℓ -local rank 1 projector O_χ acting on a set of qubits S with $|S| = \ell$ if and only if $\text{Tr}_{\bar{S}}(|\psi\rangle\langle\psi|) = \text{Tr}_{\bar{S}}(|\varphi\rangle\langle\varphi|)$.*

This allows us to give a characterization of \mathcal{O}_ℓ -partial isomorphism in terms of the partial trace. Fix a unitary group Γ obeying the condition above and a pebble set \mathcal{P} for Γ . Recall that the set of labels of qubits Q^τ in \mathcal{H}_n^τ was defined in equation (3.1). For each qubit label $(i, \vec{n}) \in Q^\tau$, define the abuse of notation

$$\text{Stab}_\Gamma(i, \vec{n}) := \{U \in \Gamma : \text{Tr}_{\overline{(i, \vec{n})}}(U\rho) = \text{Tr}_{\overline{(i, \vec{n})}}(\rho) \text{ for all } \rho \in \text{D}(\mathcal{H}_n^\tau)\} \quad (4.5)$$

to be the subgroup of Γ which acts trivially on qubit i . In particular, if Γ_G is a classical unitary group and φ is the natural embedding of G into Γ_G , then $\text{Stab}_{\Gamma_G}(i, \vec{n}) = \varphi(\text{Stab}_G((i, \vec{n})))$.

Definition 4.4 [DW22]. Let $P \subseteq \mathcal{P}$ be a set of pebbles. The *lift* of P is the set of qubits

$$Q_P^\tau = \{(i, \vec{n}) \in Q^\tau : \bigcap P \leq \text{Stab}_\Gamma(i, \vec{n})\}. \quad (4.6)$$

That is, Q_P^τ is the set of qubit labels which are pointwise stabilized by the pebbles. This definition of lift is similar to that given by Dawar and Wilsenach [DW22].

Lemma 4.5. *Let $P \subseteq \mathcal{P}$ be a set of pebbles. If $S \subseteq Q_P^\tau$ is a set of ℓ qubits, then P supports every ℓ -local rank 1 projector acting on S .*

Proof. Let $O_\chi = |\chi\rangle_S\langle\chi|_S \otimes \mathbb{I}$ be any such projector. We have $\bigcap P \leq \text{Stab}_\Gamma(i, \vec{n})$ for every $(i, \vec{n}) \in S$, so $\bigcap P \leq \bigcap_{(i, \vec{n}) \in S} \text{Stab}_\Gamma(i, \vec{n})$. Hence every $U \in \bigcap P$ acts trivially on the qubits S , so $U(|\chi\rangle_S\langle\chi|_S \otimes \mathbb{I})U^\dagger = |\chi\rangle_S\langle\chi|_S \otimes \mathbb{I}$ and so O_χ commutes with U . \square

Thus by Lemmas 4.3 and 4.5, the following simpler notion of partial isomorphism gives a weaker version of \mathcal{O}_ℓ -partial isomorphism.

Definition 4.6. A unitary $U \in \Gamma$ is an *ℓ -partial trace-based partial isomorphism*, abbreviated *ℓ -PT partial isomorphism*, from $|A\rangle$ to $|B\rangle$ with respect to $P \subseteq \mathcal{P}$ if for every $S \subseteq Q_P^\tau$ with $1 \leq |S| \leq \ell$ we have

$$\text{Tr}_{\overline{S}}(|A\rangle\langle A|) = \text{Tr}_{\overline{S}}(U^\dagger|B\rangle\langle B|U). \quad (4.7)$$

Proposition 4.7. If $U \in \Gamma$ is an \mathcal{O}_ℓ -partial isomorphism from $|A\rangle$ to $|B\rangle$ with respect to $P \subseteq \mathcal{P}$, then it is also an ℓ -PT partial isomorphism from $|A\rangle$ to $|B\rangle$ with respect to P .

Proof. Let $S \subseteq Q_P^\tau$ with $1 \leq |S| \leq \ell$. By Lemma 4.5, P supports every $O \in \mathcal{O}_\ell$ acting on S , so $\langle A|O|A\rangle = \langle B|OUU^\dagger|B\rangle$. So by Lemma 4.3, $\text{Tr}_{\overline{S}}(|A\rangle\langle A|) = \text{Tr}_{\overline{S}}(U^\dagger|B\rangle\langle B|U)$. \square

Note that the converse does not necessarily hold, because it is possible that P supports some base observable $O_\chi = |\chi\rangle_S\langle\chi|_S \otimes \mathbb{I} \in \mathcal{O}_\ell$ acting on qubits S which are not all in the lift of P ; this might for example occur if the state $|\chi\rangle$ itself has nontrivial symmetries. Hence ℓ -PT partial isomorphism is strictly weaker than \mathcal{O}_ℓ -partial isomorphism, but is easier to reason about.

We can then define a pebble game based on our new notion of partial isomorphism.

Definition 4.8. The (Γ, \mathcal{P}, k) - *ℓ -partial trace-based quantum pebble game*, abbreviated as the (Γ, \mathcal{P}, k) - *ℓ -PT quantum pebble game*, is defined identically to the quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game with the notion of \mathcal{O} -partial isomorphism replaced by ℓ -PT partial isomorphism.

Since the notion of partial isomorphism is weaker, this game is *easier* for Duplicator and harder for Spoiler than the $(\Gamma, \mathcal{P}, \mathcal{O}_\ell, k)$ -pebble game. Nevertheless, it is simpler and easier to apply, as we do in Part II.

Setting ℓ to the number of qubits $|Q^\tau|$, we obtain an even simpler notion of partial isomorphism which allows us to simultaneously measure all the qubits in the lift of P .

Definition 4.9. A unitary $U \in \Gamma$ is a *partial trace-based partial isomorphism*, abbreviated *PT partial isomorphism*, from $|A\rangle$ to $|B\rangle$ with respect to $P \subseteq \mathcal{P}$ if

$$\text{Tr}_{\overline{Q_P^\tau}}(|A\rangle\langle A|) = \text{Tr}_{\overline{Q_P^\tau}}(U^\dagger|B\rangle\langle B|U). \quad (4.8)$$

Definition 4.10. The (Γ, \mathcal{P}, k) -*partial trace-based quantum pebble game*, abbreviated as the (Γ, \mathcal{P}, k) -*PT quantum pebble game*, is defined identically to the quantum $(\Gamma, \mathcal{P}, \mathcal{O}, k)$ -pebble game with the notion of \mathcal{O} -partial isomorphism replaced by PT partial isomorphism.

Clearly if Duplicator wins the (Γ, \mathcal{P}, k) -PT quantum pebble game, then it also wins the $(\Gamma, \mathcal{P}, k)\text{-}\ell$ -PT quantum pebble game for every ℓ . The PT quantum pebble game provides a simple and natural quantum generalization of Dawar and Wilenach's (G, k) -pebble game. In the classical restriction, the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game is in fact equivalent to the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game:

Lemma 4.11. *Let Γ_G be a classical unitary group, let $P \subseteq \mathcal{P}_G$, and let $|\mathcal{A}\rangle, |\mathcal{B}\rangle \in \mathcal{H}_n^\tau$ be computational basis states encoding classical structures. $U \in \Gamma_G$ is a $\mathcal{O}_{\text{clas}}$ -partial isomorphism from $|\mathcal{A}\rangle$ to $|\mathcal{B}\rangle$ iff it is a PT partial isomorphism from $|\mathcal{A}\rangle$ to $|\mathcal{B}\rangle$, both with respect to P .*

Proof. P supports each $O_{(i, \vec{n})} = |1\rangle_{(i, \vec{n})}\langle 1|_{(i, \vec{n})} \otimes \mathbb{I} \in \mathcal{O}_{\text{clas}}$ iff qubit (i, \vec{n}) is not moved by $\bigcap P$: that is, $(i, \vec{n}) \in Q_P^\tau$. Since $U \in \Gamma_G$ just permutes the qubits, $\text{Tr}_{Q_P^\tau}(|\mathcal{A}\rangle\langle \mathcal{A}|)$ and $\text{Tr}_{Q_P^\tau}(U^\dagger|\mathcal{B}\rangle\langle \mathcal{B}|U)$ are both computational basis states, so they are equal iff $\langle \mathcal{A}|O_{(i, \vec{n})}|\mathcal{A}\rangle = \langle \mathcal{B}|UO_{(i, \vec{n})}U^\dagger|\mathcal{B}\rangle$ for all $(i, \vec{n}) \in Q_P^\tau$ since $O_{(i, \vec{n})}$ measures qubit (i, \vec{n}) in the computational basis. \square

Corollary 4.12. *On classical structures, the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game is equivalent to the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game.*

We can then show that the PT quantum pebble game also cannot distinguish the CFI graphs:

Proposition 4.13. *Let $(G_n)_n$ and $(H_n)_n$ be the families of CFI graphs of Theorem 2.23, interpreted as τ_{graph} -structures, and suppose G_n and H_n have the same set of vertices V . Let $G = \text{Sym}_V$. Then for $n \geq 3$, Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game on G_n and H_n for some $k = \Omega(n)$.*

Proof. By Proposition 3.16, Duplicator wins the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game on G_n and H_n for some such k , so by Corollary 4.12, it also wins the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game. \square

Similarly, by Proposition 3.17 and Corollary 4.12:

Proposition 4.14. *Let $(G_n)_n$ and $(H_n)_n$ be the families of Alt-CFI graphs of Corollary 2.28, interpreted as τ_{graph} -structures, and suppose G_n and H_n have the same set of vertices V . Let $G = \text{Alt}_V$. Then for $n \geq 3$, Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game on G_n and H_n for some $k = \Omega(n)$.*

Proposition 4.14 is a key ingredient in the quantum lower bounds in Part II.

Finally, it should be noted that the partial trace-based pebble games in this chapter, and the concept of an ℓ -local projector from which they are derived, inherently privilege one particular division of the Hilbert space into qubits. Indeed, while conjugating by an arbitrary unitary—corresponding to an arbitrary quantum change of basis—preserves the rank of an operator, it does not preserve ℓ -locality, and an arbitrary change of basis might encode the information of one qubit as part of an entangled state of several qubits. (For example, consider the unitary mapping the computational basis on two qubits to the Bell basis, which consists of maximally

entangled states.) Thus our partial trace-based notions of partial isomorphism are not robust to arbitrary changes of basis. The partial trace-based pebble games are thus best suited to applications where the division of the Hilbert space into qubits is significant; this is the case in the applications to quantum circuit complexity in Part II, where the qubits correspond to wires.

Part II

Lower bounds for symmetric quantum circuits

Chapter 5

Symmetric circuits

This chapter presents the definitions of symmetric circuits given by Castro-Silva, Gur, and Strelchuk and is based on Sections 2 and 3 of [CGS25]. The material on symmetric classical circuits is originally due to Anderson and Dawar [AD17].

Part II of this thesis is devoted to applications of pebble games in proving lower bounds on the size of symmetric quantum circuits needed to compute certain properties. In this chapter, we work our way up to a definition of symmetric quantum circuits, presenting first symmetric classical circuits as defined by Anderson and Dawar [AD17], then presenting Castro-Silva, Gur, and Strelchuk's extension to symmetric reversible and quantum circuits [CGS25]. Fix a relational vocabulary τ and assume without loss of generality that all structures of size n have domain $[n]$.

5.1 Symmetric classical circuits

We start by formally defining classical symmetric circuits, which were informally introduced in Section 2.5. We focus on Boolean circuits since they are generalized by quantum circuits, but more general types of circuits may also be defined (e.g., arithmetic circuits [DW20]).

Definition 5.1 [AD17]. A *Boolean τ -circuit* $C = (V, E)$ of order $n \in \mathbb{Z}_{\geq 1}$ is a directed acyclic graph (DAG) on vertices V and edges $E \subseteq V^2$ whose vertices are called *gates*, obeying the following conditions:

- (a) Every gate with at least one incoming edge, called an *internal gate*, is labelled by an element of a *gate set* \mathbb{G} .
- (b) Every gate with no incoming edges, called an *input gate*, is labelled by some qubit label $(i, \vec{n}) \in Q^\tau$, and every $(i, \vec{n}) \in Q^\tau$ labels exactly one input gate, denoted $x_{(i, \vec{n})}$.
- (c) There is exactly one gate with no outgoing edges, called the *output gate* g_{out} .

We often omit the word “Boolean” and leave τ implicit for brevity. In a circuit (V, E) , the *children* of a gate $g \in V$ are the gates $\text{child}(g) := \{h \in V : (h, g) \in E\}$. The gate set \mathbb{G} is also called a *basis* in [AD17]. The elements of a gate set are Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$, where the arity n must match the in-degree of the gates labelled by f . We are interested in the *threshold gate set* \mathbb{G}_{thr} consisting of the unary NOT gate and the *threshold functions*

$$\text{Th}_{\geq k}^n(a_1, \dots, a_n) = \begin{cases} 1 & \text{if at least } k \text{ of } a_1, \dots, a_n \text{ equal 1} \\ 0 & \text{otherwise} \end{cases} \quad (5.1)$$

for each integer $n \geq 1$ and $0 \leq k \leq n$. Note that the standard Boolean operators can be expressed in terms of these gates (e.g., AND_n is just $\text{Th}_{\geq n}^n$). As described in Section 2.5, this gate set is interesting because the graph properties that can be efficiently computed by fully symmetric circuits over \mathbb{G}_{thr} are precisely those expressible in FPC [AD17].

A Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is *fully symmetric* if it does not depend on the ordering of its inputs. That is, f is fully symmetric if $f(a_1, \dots, a_n) = f(\sigma(a_1), \dots, \sigma(a_n))$ for every $a_1, \dots, a_n \in \{0, 1\}$ and $\sigma \in \text{Sym}_n$. We always assume that the functions in every classical gate set \mathbb{G} are fully symmetric. A τ -circuit over \mathbb{G}_{thr} is called a *threshold τ -circuit*.

Definition 5.2. Let C be a τ -circuit of order n over a gate set \mathbb{G} and \mathcal{A} be a τ -structure of size n . Let g be a gate of C . The *value of C at g on \mathcal{A}* , denoted $C[\mathcal{A}](g)$, is a value in $\{0, 1\}$ defined recursively as follows:

- (a) If g is an input gate labelled $x_{(i, \vec{n})}$, then $C[\mathcal{A}](g) = 1$ if $\vec{n} \in R_i^{\mathcal{A}}$ and 0 otherwise.
- (b) If g is an internal gate labelled by an m -ary function $f \in \mathbb{G}$ with incoming edges from gates g_1, \dots, g_m , then $C[\mathcal{A}](g) = f(C[\mathcal{A}](g_1), \dots, C[\mathcal{A}](g_m))$.

We write $C[\mathcal{A}]$ for $C[\mathcal{A}](g_{\text{out}})$, where g_{out} is the output gate of C .

Note that (b) is well-defined because $f \in \mathbb{G}$ is assumed to be fully symmetric. We can then define a model of computation as follows.

Definition 5.3. A *family of τ -circuits* $(C_n)_n$ consists of a τ -circuit C_n of order n for each $n \in \mathbb{Z}_{\geq 1}$. $(C_n)_n$ is said to *compute* the property

$$\bigcup_{n \in \mathbb{Z}_{\geq 1}} \{\mathcal{A} \in \text{fin}_n[\tau] : C_n[\mathcal{A}] = 1\}. \quad (5.2)$$

We often write (C_n) for $(C_n)_n$.

Our complexity measure is the *size* of a circuit C , denoted $s(C)$, which is just the number of gates in C . Our notion of symmetry for circuits is syntactic.

Definition 5.4 [AD17; CGS25]. An *automorphism* of a circuit C with vertices V and edge set $E \subseteq V^2$ is a permutation $\pi \in \text{Sym}_V$ such that:

- (a) For each $(g, h) \in E$, we have $(\pi(g), \pi(h)) \in E$.
- (b) For each internal gate $g \in V$, $\pi(g)$ is an internal gate with the same label as g .

Such a π must map input gates to input gates. Let $X = \{x_{(i, \vec{n})}\}$ be the set of input gates of a τ -circuit C of order n . Then Sym_n acts on X by $\sigma(x_{(i, \vec{n})}) = x_{(i, \sigma(\vec{n}))}$. A permutation $\sigma \in \text{Sym}_n$ is said to *induce* an automorphism π of C if π acts the same as σ on the input gates X , i.e. $\pi(x) = \sigma(x)$ for all $x \in X$ [AD17].

Definition 5.5 [AD17]. Let $G \leq \text{Sym}_n$. A τ -circuit C of order n is *G -symmetric* if every $\sigma \in G$ induces an automorphism of C .

It is convenient to constrain the possible automorphisms of a circuit.

Definition 5.6 [DW20]. A τ -circuit C of order n is *rigid* if every $\sigma \in \text{Sym}_n$ induces at most one automorphism of C .

Hence in a rigid G -symmetric circuit C , every $\sigma \in G$ induces exactly one automorphism, and so G acts on the gates of C via this unique automorphism. For this reason, it is convenient—and essential for the support theorem in Chapter 6—to deal only with rigid circuits. We are allowed to do so by the following lemma.

Lemma 5.7 [AD17, Lem. 7]. *Any G -symmetric τ -circuit may be transformed into an equivalent rigid G -symmetric τ -circuit of the same size in polynomial time.*

Here “equivalent” means that the circuits compute the same function. See [AD17] for the proof. Hence we often assume without loss of generality that we are working with rigid G -symmetric circuits. The computational power of families of G -symmetric circuits¹ is the subject of Chapter 6, which presents the pebble game-based lower bound technique of [Daw15a; DW22].

5.2 Symmetric reversible circuits

Moving towards a quantum notion of symmetric circuits, we present [CGS25]’s notion of symmetric reversible circuits, which are equivalent in power to symmetric classical circuits.

A reversible circuit consists of a fixed set of wires W carrying Boolean values, upon which a sequence of gates act. Each gate transforms the wires *reversibly*, meaning it applies an invertible function $g : \{0, 1\}^W \rightarrow \{0, 1\}^W$ to the wires. The invertibility requirement means that no information is lost through the circuit, which is crucial for quantum computation.

Any Boolean function $g : \{0, 1\}^n \rightarrow \{0, 1\}$ can be transformed into an invertible function by adding one “ancilla” bit [CGS25]:

$$(a_1, \dots, a_n, b) \mapsto (a_1, \dots, a_n, b \oplus g(a_1, \dots, a_n)) \quad (5.3)$$

Here \oplus denotes XOR. The primary reversible gate set considered by [CGS25] is just the application of this transform to the threshold functions above.

Definition 5.8 [CGS25]. The *reversible threshold gate set* $\mathbb{G}_{\text{thr}}^R$ on a set of wires W consists of unary NOT gates $\{\text{NOT}_h : h \in W\}$, where NOT_h maps $(a_w)_w \in \{0, 1\}^W$ to $(b_w)_w \in \{0, 1\}^W$ with $b_h = \neg a_h$ and $b_w = a_w$ for $w \neq h$, together with the *reversible threshold gates* $\{\text{Th}_{\geq k}^{S,h} : S \subseteq W, h \in W \setminus S, 0 \leq k \leq |S|\}$, where $\text{Th}_{\geq k}^{S,h}$ maps $(a_w)_w$ to $(b_w)_w$, defined as

$$b_w = \begin{cases} a_w & \text{if } w \neq h \\ a_w \oplus \text{Th}_{\geq k}^{|S|}(a_{s_1}, \dots, a_{s_\ell}) & \text{if } w = h \end{cases} \quad (5.4)$$

where $S = \{s_1, \dots, s_\ell\}$.

¹Technically, defining a “family of G -symmetric circuits” (C_n) requires us to specify a different symmetry group $G_n \leq \text{Sym}_n$ for each n against which each C_n is symmetric. We generally leave the dependence on n implicit and refer simply to families of G -symmetric circuits; for example, we might refer to families of Sym_n -symmetric or Alt_n -symmetric circuits.

Two functions $f, g : \{0, 1\}^W \rightarrow \{0, 1\}^W$ commute if $f \circ g = g \circ f$: that is, they have no intrinsic order of application in a reversible circuit. To ease the definition of symmetry, as in [CGS25], we define reversible circuits in terms of groupings of commuting gates called *layers*.

Definition 5.9 [CGS25]. A *reversible circuit*² over a reversible gate set \mathbb{G}^R consists of a set of wires W and a sequence of *layers* $(\mathcal{L}_1, \dots, \mathcal{L}_m)$. Each layer \mathcal{L} is a set of pairwise commuting invertible functions $\{0, 1\}^W \rightarrow \{0, 1\}^W$ from \mathbb{G}^R .

Reversible circuits naturally define invertible functions $\{0, 1\}^W \rightarrow \{0, 1\}^W$. To define a model of computation, we use some of the wires to encode the input structure and initialize the rest to 0, and we fix an “output wire”.

Definition 5.10. An *output reversible τ -circuit of order n* is a reversible circuit whose wires are partitioned as $W = X \sqcup A$, where $X = \{x_{(i, \vec{n})} : (i, \vec{n}) \in Q^\tau\}$ is the set of *input wires* and A is the set of *ancilla wires*, and which has a distinguished *output wire* $w_{\text{out}} \in W$.

An output reversible τ -circuit R of order n defines a function $\text{fin}_n[\tau] \rightarrow \{0, 1\}$ informally as follows. Each wire carries a Boolean value. We initialize the input wires X to the binary encoding $b(\mathcal{A})$ of $\mathcal{A} \in \text{fin}_n[\tau]$ as given in Section 3.1.1 by initializing each wire $x_{(i, \vec{n})}$ to $b(\mathcal{A})_{(i, \vec{n})}$, and we initialize the ancilla wires A to 0. We then apply the gates in each layer in turn, then read the output off the value of w_{out} at the end. Write $R[\mathcal{A}] \in \{0, 1\}$ for this output. As in Definition 5.3, we can define the notion of a *family of output reversible τ -circuits* (R_n) which computes the property $\bigcup_{n \in \mathbb{Z}_{\geq 1}} \{\mathcal{A} \in \text{fin}_n[\tau] : R_n[\mathcal{A}] = 1\}$.

We have two complexity measures for output reversible circuits R : the *size* $s(R)$, defined as the number of gates in R , and the *number of ancillas* $a(R)$, which is the size of the set A of ancilla wires. These measures are roughly analogous to time and space requirements, respectively.

To define symmetry, we again define a syntactic notion of automorphism. Instead of permuting the gates, we permute the wires W and allow such permutations $\pi \in \text{Sym}_W$ to act on the gates as follows. Our definition of automorphism is more general than that of [CGS25].

Definition 5.11. A permutation $\pi \in \text{Sym}_W$ acts on a reversible gate set \mathbb{G}^R by mapping $g : \{0, 1\}^W \rightarrow \{0, 1\}^W$ to $\pi \circ g \circ \pi^{-1}$, where we treat π as a function $\{0, 1\}^W \rightarrow \{0, 1\}^W$ which permutes tuples by mapping $(a_{w_1}, \dots, a_{w_n})$ to $(a_{\pi^{-1}(w_1)}, \dots, a_{\pi^{-1}(w_n)})$.

We require reversible gate sets \mathbb{G}^R to be closed under the action of all $\pi \in \text{Sym}_W$. In particular, π maps NOT_h to $\text{NOT}_{\pi(h)}$ and $\text{Th}_{\geq k}^{S, h}$ to $\text{Th}_{\geq k}^{\pi(S), \pi(h)}$, as in [CGS25].

Definition 5.12 [CGS25]. An *automorphism* of a reversible circuit R with wires W is a permutation $\pi \in \text{Sym}_W$ such that for each layer \mathcal{L} of R we have $\mathcal{L} = \{\pi(g) : g \in \mathcal{L}\}$.

²Referred to as a *layered reversible circuit* in [CGS25].

That is, an automorphism is a permutation of the wires which leaves each layer unchanged up to an ordering of the gates [CGS25]. Since the gates within a layer commute, they have no intrinsic order of application, so such an automorphism leaves the circuit effectively the same.

Consider an output reversible τ -circuit R of order n with wires $W = X \sqcup A$ and let $G \leq \text{Sym}_n$. Then G acts on the input wires X : each $\sigma \in G$ maps $x_{(i,\vec{n})} \mapsto x_{(i,\sigma(\vec{n}))}$. We say $\sigma \in G$ induces an automorphism π of R if σ acts the same as π on X , i.e. $\pi(x) = \sigma(x)$ for all $x \in X$.

Definition 5.13 [CGS25]. Let $G \leq \text{Sym}_n$. An output reversible τ -circuit R of order n is *G-symmetric* if every $\sigma \in G$ induces an automorphism π of R such that $\pi(w_{\text{out}}) = w_{\text{out}}$.

Intuitively, we require w_{out} to be stabilized so that where we measure the output of the circuit is invariant under the symmetry.

It can be shown that the *G*-symmetric threshold circuits and the *G*-symmetric output reversible circuits over $\mathbb{G}_{\text{thr}}^R$ are equivalent in computational power up to a constant factor [CGS25]:

Proposition 5.14. *A τ -property is computed by a family of *G*-symmetric threshold τ -circuits (C_n) of size $s(C_n) = O(f(n))$ if and only if it is computed by a family of *G*-symmetric output reversible τ -circuits (R_n) over $\mathbb{G}_{\text{thr}}^R$ with $s(R_n) + a(R_n) = O(f(n))$.*

Proof. This follows directly from Proposition 1 of [CGS25]. □

5.3 Symmetric quantum circuits

We now extend the above definitions to symmetric quantum circuits, following [CGS25]. As a contribution, we somewhat generalize [CGS25]'s notion of a symmetric quantum circuit, though the remainder of the thesis will use only the special case studied by [CGS25].

A quantum circuit consists of a set of wires W which define a Hilbert space $\mathcal{H}_W := (\mathbb{C}^2)^{\otimes W}$ upon which a sequence of unitary operators called *gates* act, chosen from a *quantum gate set* \mathbb{G}^Q . The primary gate set considered by [CGS25] consists of all single-qubit unitaries and the unitary extensions of the reversible threshold gates.

Definition 5.15 [CGS25]. The *quantum threshold gate set* $\mathbb{G}_{\text{thr}}^Q$ on a set of wires W consists of all single-qubit unitaries $\{U_h : h \in W, U \in \text{U}(\mathbb{C}^2)\}$, where U_h maps the computational basis state $\bigotimes_w |a_w\rangle$ to $\bigotimes_w |b_w\rangle$ with $|b_h\rangle = U|a_h\rangle$ and $|b_w\rangle = |a_w\rangle$ for $w \neq h$, together with the *quantum threshold gates* $\{\text{Th}_{\geq k}^{S,h} : S \subseteq W, h \in W \setminus S, 0 \leq k \leq |S|\}$, where $\text{Th}_{\geq k}^{S,h}$ is the unitary extension of the reversible threshold gate $\text{Th}_{\geq k}^{S,h}$ acting on the computational basis.

As before, we define quantum circuits in terms of layers of commuting gates.

Definition 5.16 [CGS25]. A *quantum circuit*³ over a quantum gate set \mathbb{G}^Q consists of a set of wires W and a sequence of *layers* $(\mathcal{L}_1, \dots, \mathcal{L}_m)$. Each layer \mathcal{L} is a set of pairwise commuting unitary gates U_g acting on \mathcal{H}_W from \mathbb{G}^Q .

³Referred to as a *layered quantum circuit* in [CGS25].

To define a model of computation, we again fix an output wire.

Definition 5.17. An *output quantum τ -circuit of order n* is a quantum circuit whose wires are partitioned as $W = X \sqcup A$, where $X = \{x_{(i,\vec{n})} : (i, \vec{n}) \in Q^\tau\}$ is the set of *input wires* and A is the set of *ancilla wires*, and which has a distinguished *output wire* $w_{\text{out}} \in W$.

Again, we often leave τ implicit for brevity. The Hilbert space of an output quantum τ -circuit of order n is partitioned as $\mathcal{H}_W = \mathcal{H}_n^\tau \otimes \mathcal{H}_A$, where \mathcal{H}_n^τ is encoded on the input wires X and the ancilla wires A form the space $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes A}$. Such a circuit C on layers $(\mathcal{L}_1, \dots, \mathcal{L}_m)$ then defines a function $\mathcal{H}_n^\tau \rightarrow [0, 1]$ as follows: We begin by initializing the input wires X to a quantum τ -structure $|\psi\rangle \in \mathcal{H}_n^\tau$ and each ancilla wire to $|0\rangle$, forming the state $|\psi\rangle|0\rangle^{\otimes A} \in \mathcal{H}_W$. We then apply the unitaries from each layer in turn. For each layer \mathcal{L}_i , let L_i denote the product of the unitaries in \mathcal{L}_i (in arbitrary order, since they commute); we say that \mathcal{L}_i is *represented* by the unitary L_i . We then form the state

$$|\psi'\rangle := L_m L_{m-1} \cdots L_2 L_1 |\psi\rangle |0\rangle^{\otimes A}. \quad (5.5)$$

Finally, we measure the wire w_{out} in the computational basis using the observable $O_{\text{out}} := |1\rangle_{w_{\text{out}}} \langle 1|_{w_{\text{out}}} \otimes \mathbb{I}_{W \setminus \{w_{\text{out}}\}}$, obtaining the result

$$\langle \psi' | O_{\text{out}} | \psi' \rangle \in [0, 1] \quad (5.6)$$

which we interpret as the classical probability of measuring $|1\rangle$. We let $C[|\psi\rangle] = \langle \psi' | O_{\text{out}} | \psi' \rangle$ denote this probability.

Our model of quantum computation therefore takes a quantum τ -structure as input and produces a classical probabilistic Boolean output. In our results, we will typically be concerned only with inputs $|\mathcal{A}\rangle$ which represent classical τ -structures \mathcal{A} . The above definition could be extended to take a density matrix $\rho \in D(\mathcal{H}_n^\tau)$ as input, apply the unitaries, and output the partial trace to the wire w_{out} , thus forming a quantum channel $D(\mathcal{H}_n^\tau) \rightarrow D(\mathbb{C}^2)$; however, the above model is sufficient for our results.

As before, a family of output quantum τ -circuits (C_n) consists of one such circuit C_n of order n for each $n \in \mathbb{Z}_{\geq 1}$. We use the following BQP-like [BV97] definition of the classical property computed by a family of quantum circuits.

Definition 5.18. A family of output quantum τ -circuits (C_n) *computes* a τ -property \mathcal{P} if for every $n \in \mathbb{Z}_{\geq 1}$ and $\mathcal{A} \in \text{fin}_n[\tau]$, we have $C_n[|\mathcal{A}\rangle] \geq 2/3$ if $\mathcal{A} \in \mathcal{P}$ and $C_n[|\mathcal{A}\rangle] \leq 1/3$ if $\mathcal{A} \notin \mathcal{P}$.

We use the same complexity measures as for reversible circuits: the *size* $s(C)$ is the number of gates in an output quantum circuit C and the *number of ancillas* $a(C)$ is the size of its set A of ancilla wires.

The following is an original quantum generalization of the reversible notion of a circuit automorphism to arbitrary unitaries.

Definition 5.19. An *automorphism* of a quantum circuit C with wires W is a unitary $V \in U(\mathcal{H}_W)$ such that for each layer \mathcal{L} of C we have $\mathcal{L} = \{VU_gV^\dagger : U_g \in \mathcal{L}\}$.

That is, an automorphism is a change of basis which leaves each layer the same up to an unimportant permutation of the gates; in other words, an automorphism V acts on the gates in each layer by conjugation. We also say that $V \in U(\mathcal{H}_W)$ is an automorphism of a layer \mathcal{L} if $\mathcal{L} = \{VU_gV^\dagger : U_g \in \mathcal{L}\}$, and of a unitary $L \in U(\mathcal{H}_W)$ if $L = VLV^\dagger$ (that is, V commutes with L). Observe that if a unitary L represents a layer \mathcal{L} and V is an automorphism of \mathcal{L} , then V is also an automorphism of L .

Consider an output quantum τ -circuit C of order n with wires $W = X \sqcup A$ and a symmetry group $\Gamma \leq U(\mathcal{H}_n^\tau)$. A unitary $U \in \Gamma$ *induces* an automorphism $V \in U(\mathcal{H}_W)$ of C if $V = U \otimes U_A$ for some unitary $U_A \in U(\mathcal{H}_A)$; note that the automorphism must act separately on the input wires and ancillas.

Definition 5.20. Let $\Gamma \leq U(\mathcal{H}_n^\tau)$. An output quantum τ -circuit C of order n is Γ -*symmetric* if every $U \in \Gamma$ induces an automorphism V of C which acts trivially on w_{out} in the sense that $V = \mathbb{I}_{w_{\text{out}}} \otimes V'_{W \setminus \{w_{\text{out}}\}}$ for some V' acting on the other qubits.

As before, intuitively, the requirement that V acts trivially on w_{out} ensures that we can measure the output of the circuit in the same place under any symmetry. For proving lower bounds, we typically restrict ourselves to automorphisms from Γ_{Sym_W} , which recovers the original definition of a quantum circuit automorphism of [CGS25]:

Definition 5.21. Suppose $G \leq \text{Sym}_n$. Recall that $\Gamma_G \leq U(\mathcal{H}_n^\tau)$ is the unitary group which permutes the qubits according to the action of G . An output quantum τ -circuit of order n is Γ_G -*permutation symmetric* if every $U_\sigma \in \Gamma_G$ induces an automorphism $V \in \Gamma_{\text{Sym}_W}$ of G which acts trivially on w_{out} in the above sense.

That is, in a Γ_G -permutation symmetric circuit, every permutation of the input wires $U \in \Gamma_G$ induces a permutation of the ancillas V' such that $V = U \otimes V'$ is an automorphism fixing w_{out} , which coincides with the notion of a G -symmetric reversible circuit and the notion of a symmetric quantum circuit of [CGS25].

5.4 Rigid reversible and quantum circuits

We may also define rigidity for reversible and quantum circuits.

Definition 5.22. Let $G \leq \text{Sym}_n$. A G -symmetric output reversible τ -circuit R is *rigid* if every $\sigma \in G$ induces exactly one automorphism of R .

For ease of notation, we define rigid quantum circuits with reference to a group of allowable automorphisms.

Definition 5.23. Let $\Gamma \leq \mathrm{U}(\mathcal{H}_n^\tau)$ and $\Gamma' \leq \mathrm{U}(\mathcal{H}_W)$. A Γ -symmetric output quantum τ -circuit C is Γ' -*rigid* if for every $U \in \Gamma$, there is exactly one automorphism in Γ' which is induced by U .

If C is Γ_G -permutation symmetric, we simply use *rigid* to mean Sym_W -rigid. Thus the possible automorphisms of rigid Γ_G -permutation symmetric quantum circuits are just permutations of the wires. In a Γ_G -permutation symmetric quantum circuit C , G acts on the set of wires via these permutations.

Our lower bound techniques in Chapters 7 and 8 require us to work with rigid quantum circuits. It is left as an open problem in this thesis whether there exists an analogue of Lemma 5.7 for quantum circuits which would allow us to translate any symmetric quantum circuit into an equivalent rigid such circuit without too much blowup. In the absence of such a transformation, our results in Chapters 7 and 8 are stated for rigid circuits only. If such an analogue of Lemma 5.7 exists, then our results can be extended to all symmetric quantum circuits. I expect this to be the case, but a proof is not immediately apparent: the proof of Lemma 5.7 in [AD17] relies heavily on the DAG structure of a classical circuit and so is not directly applicable to quantum circuits.

Chapter 6

Classical lower bounds for symmetric circuits

This chapter is an exposition of a lower bound technique by Dawar originating in [Daw15a] and developed further by Dawar and Wilkenbach in [DW20; DW21; DW22]. The presentation is influenced by [DW22]. Corollary 6.12 is, to the author’s knowledge, new; otherwise, this chapter contains no original material.

We now present a technique originated by Dawar [Daw15a] for proving exponential lower bounds on the size of the symmetric classical circuits needed to compute a property. The technique applies the classical (G, k) -pebble game (Definition 2.25). The remaining chapters of this thesis generalize this technique to quantum circuits using the quantum pebble games introduced in Part I.

Fix a relational vocabulary τ and again assume every structure of size n has domain $[n]$. The technique aims to prove lower bounds of the following form: For a particular τ -property \mathcal{P} and symmetry group G , every family of G -symmetric classical circuits (C_n) computing \mathcal{P} has exponential size, $s(C_n) = 2^{\Omega(n)}$. Thus, any family of circuits that efficiently computes \mathcal{P} must break the symmetry represented by G in some way. Results of this form therefore give instances where symmetry-breaking is necessary for efficient computation. For example, when \mathcal{P} is the CFI property \mathcal{P}_{CFI} and $G = \text{Sym}_n$, Corollary 6.11 shows that breaking graph symmetry—that is, dealing with the vertices in some order—is necessary to efficiently distinguish the CFI graphs.

The argument consists of three key technical ingredients.

1. A *support theorem*, which is a combinatorial argument showing that in every small family of G -symmetric circuits, every gate has a particular property called its *support size* which is sufficiently small.
2. A theorem which I call the *indistinguishability theorem*, which states that for every G -symmetric classical τ -circuit C in which every gate has support size at most k , if \mathcal{A} and \mathcal{B} are τ -structures on which Duplicator wins the $(G, 2k)$ -pebble game, then $C[\mathcal{A}] = C[\mathcal{B}]$: that is, C cannot distinguish between \mathcal{A} and \mathcal{B} .
3. *Families of indistinguishable τ -structures* (\mathcal{A}_n) and (\mathcal{B}_n) such that Duplicator wins the (G, k) -pebble game on \mathcal{A}_n and \mathcal{B}_n for a sufficiently fast-growing number of pebbles k .

We then argue that no small family of G -symmetric circuits can compute any property which separates (\mathcal{A}_n) from (\mathcal{B}_n) , because any such family has small support size by the support theorem, and so its circuits cannot distinguish between each \mathcal{A}_n and \mathcal{B}_n by the indistinguishability theorem. Our quantum generalizations of the technique in Chapters 7 and 8 also follow this basic structure.

6.1 The support theorem

We begin by presenting the theory of supports of [DW22]. The main ideas originated with Anderson and Dawar [AD17]; the support theorem was strengthened by Dawar and Wilsenach [DW21] and extended to the form presented here in [DW22].

Definition 6.1 [DW22; AD17]. Let $G \leq \text{Sym}_n$ and let C be a rigid G -symmetric τ -circuit of order n . A set $S \subseteq [n]$ is a *support* of a gate g of C if $\text{Stab}_G(S) \leq \text{Stab}_G(g)$.

That is, pointwise stabilizing S is sufficient to stabilize g . Following the notation of [DW22], for each gate g in a rigid G -symmetric circuit C , write **min-supp**(g) for the size of the smallest support $S \subseteq [n]$ of g , and let **max-supp**(C) be the largest value of **min-supp**(g) over all gates g of C . Write **max-orbit**(C) for the size of the largest orbit of any gate g in C under G .

The support theorem for a particular group G states that in any family of rigid G -symmetric τ -circuits (C_n) , if **max-orbit**(C_n) = $2^{o(n)}$ then **max-supp**(C_n) = $o(n)$. This gives us a path to prove an exponential lower bound on size: if we can show that **max-supp**(C_n) = $\Omega(n)$, then the support theorem gives us **max-orbit**(C_n) = $2^{\Omega(n)}$ and so $s(C_n) = 2^{\Omega(n)}$.

The support theorem must be proved separately for each group G . Below, we give a slightly expanded version of Dawar and Wilsenach's [DW22] proof for $G = \text{Alt}_n$, which we present because it is useful for quantum circuits as well. The proof is based on the following group-theoretic lemma.

Lemma 6.2 [DM96, Thm. 5.2B]; [DW22, Thm. 4.10]. *Suppose that $n > 8$ is an integer, and let k be an integer such that $1 \leq k \leq \frac{n}{4}$. Suppose that $H \leq \text{Alt}_n$ has index $[\text{Alt}_n : H] < \binom{n}{k}$. Then there exists some $S \subseteq [n]$ with $|S| < k$ such that $\text{Stab}_{\text{Alt}_n}(S) \leq H$.*

Below, $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ denote the floor and ceiling operators, respectively.

Theorem 6.3 (Support theorem for Alt_n) [DW22, Thm. 4.11]. *Let (C_n) be a family of rigid Alt_n -symmetric circuits. If **max-orbit**(C_n) = $2^{o(n)}$ then **max-supp**(C_n) = $o(n)$.*

Proof. From [DW22]. Let k be the smallest positive integer such that **max-orbit**(C_n) < $\binom{n}{k}$. I claim that by the assumption that **max-orbit**(C_n) = $2^{o(n)}$, we have $k = o(n)$. Indeed, otherwise there is a constant c with $0 < c < \frac{1}{2}$ such that $k - 1 \geq cn \geq \lfloor cn \rfloor \geq 1$ for infinitely many n . Since k is the smallest value such that **max-orbit**(C_n) < $\binom{n}{k}$, we have $k \leq \lceil \frac{n}{2} \rceil$, since otherwise

$\binom{n}{k-1} > \binom{n}{k}$. Hence $\binom{n}{k-1} \geq \binom{n}{\lfloor cn \rfloor}$ for infinitely many n . Since $\binom{n}{\ell} \geq \left(\frac{n}{\ell}\right)^\ell$ for all integers $1 \leq \ell \leq n$,

$$\binom{n}{k-1} \geq \binom{n}{\lfloor cn \rfloor} \geq \left(\frac{n}{\lfloor cn \rfloor}\right)^{\lfloor cn \rfloor} \geq (1/c)^{cn-1} > 2^{cn-1}. \quad (6.1)$$

By the definition of k , we have $\mathbf{max-orbit}(C_n) \geq \binom{n}{k-1} > 2^{cn-1}$ for infinitely many n , contradicting the assumption that $\mathbf{max-orbit}(C_n) = 2^{o(n)}$.

Hence $k = o(n)$, and so for large enough n we have $k \leq \frac{n}{4}$. By the orbit-stabilizer theorem, for every gate g of C_n , we have $[\mathrm{Alt}_n : \mathrm{Stab}_{\mathrm{Alt}_n}(g)] < \binom{n}{k}$. By Lemma 6.2, there is some $S \subseteq [n]$ with $|S| < k$ such that $\mathrm{Stab}_{\mathrm{Alt}_n}(S) \leq \mathrm{Stab}_{\mathrm{Alt}_n}(g)$, and so S is a support of g . Hence $\mathbf{max-supp}(C_n) < k = o(n)$. \square

Note that the rigidity assumption is essential for the above proof as it allows us to identify the group of automorphisms of the circuit moving each gate g with Alt_n , which allows us to apply Lemma 6.2 after invoking the orbit-stabilizer theorem.

In [DW21], Dawar and Wilsenach also prove a support theorem for $G = \mathrm{Sym}_n$. However, their method uses induction on the DAG structure of the circuit and so it is not simple to adapt to quantum circuits. I state the result and refer the reader to [DW21] for the proof; the result follows from their Theorem 4.8 by the same argument as in the proof above.

Theorem 6.4 (Support theorem for Sym_n) [DW21, Thm. 4.8]. *Let (C_n) be a family of rigid Sym_n -symmetric circuits. If $\mathbf{max-orbit}(C_n) = 2^{o(n)}$ then $\mathbf{max-supp}(C_n) = o(n)$.*

6.2 The classical indistinguishability theorem

I now present Dawar and Wilsenach's proof of the indistinguishability theorem. The following presentation is expanded and somewhat clarified compared to the original [DW22, Thm. 4.8].

The classical indistinguishability theorem uses the original definition of the (G, k) -pebble game given by Dawar and Wilsenach [DW22]. Their game differs from our definition in Section 2.5 in that it uses the following lift-based definition of partial isomorphism, which is very similar to that used in Chapters 3 and 4:

Definition 6.5 [DW22, Def. 4.4]. Let $G \leq \mathrm{Sym}_n$, $\mathcal{A}, \mathcal{B} \in \mathrm{fin}_n[\tau]$, and $S \subseteq [n]$. For every $r \in \mathbb{Z}_{\geq 1}$, recall that G acts on tuples in $[n]^r$ elementwise. The r -lift of S is the set of tuples

$$L_r^S = \{\vec{n} \in [n]^r : \mathrm{Stab}_G(S) \leq \mathrm{Stab}_G(\vec{n})\}. \quad (6.2)$$

A permutation $\sigma \in \mathrm{Sym}_n$ is a *lift-based partial isomorphism* from \mathcal{A} to \mathcal{B} with respect to S if for every relation $R_i^{r_i} \in \tau$ and every $\vec{n} \in L_{r_i}^S$, we have $\vec{n} \in R_i^{\mathcal{A}}$ iff $\sigma(\vec{n}) \in R_i^{\mathcal{B}}$.

Dawar and Wilsenach's (G, k) -pebble game on \mathcal{A} and \mathcal{B} , which we refer to as the *lift-based (G, k) -pebble game*, is defined identically to the (G, k) -pebble game of Definition 2.25 except that the winning condition is as follows: At the end of every round, suppose Duplicator's most recently chosen bijection is $\sigma \in G$ and the pebbles a_1, \dots, a_ℓ and b_1, \dots, b_ℓ are currently placed.

Spoiler wins if σ is not a lift-based partial isomorphism from \mathcal{A} to \mathcal{B} with respect to $\{a_1, \dots, a_\ell\}$. Otherwise play continues, and Duplicator wins if it can play forever.

As remarked in Section 3.4, this lift-based (G, k) -pebble game is in fact equivalent to the quantum $(\Gamma_G, \mathcal{P}_G, \mathcal{O}_{\text{clas}}, k)$ -pebble game played on classical structures, as defined in Chapter 3. It is also equivalent to the $(\Gamma_G, \mathcal{P}_G, k)$ -partial trace-based quantum pebble game played on classical structures by Corollary 4.12, and indeed it is not hard to see that lift-based partial isomorphism coincides with PT partial isomorphism (Definition 4.9) on classical structures. Hence Propositions 4.13 and 4.14 imply that Duplicator wins the lift-based (G, k) -pebble game on the CFI graphs ($G = \text{Sym}_n$) and the Alt-CFI graphs ($G = \text{Alt}_n$) for some $k = \Omega(n)$.

We now proceed to prove the indistinguishability theorem. Fix for the following lemmas a group $G \leq \text{Sym}_n$ and a rigid G -symmetric circuit C of order n . Crucial to the proof is the ability to assign to each gate g in C a support $sp(g) \subseteq [n]$ respecting the action of G in a precise sense. The following lemma allows us to do so.

Lemma 6.6. *Suppose S is a support of a gate g of C and $\sigma \in G$. Then $\sigma S = \{\sigma s : s \in S\}$ is a support of σg .*

Proof. Suppose $\pi \in \text{Stab}(\sigma S)$. Then $\sigma^{-1}\pi\sigma \in \text{Stab}(S) \leq \text{Stab}(g)$, so $\sigma(\sigma^{-1}\pi\sigma)\sigma^{-1} = \pi \in \text{Stab}(\sigma g)$. So $\text{Stab}(\sigma S) \leq \text{Stab}(\sigma g)$. \square

Hence we may assign a support $sp(g)$ of every gate g in C such that $sp(\sigma g) = \sigma sp(g)$ for every $\sigma \in G$. Furthermore, since $|\sigma S| = |S|$ for all $S \subseteq [n]$, if $\text{max-supp}(C) \leq k$, we may choose supports such that $|sp(g)| \leq k$ for each g .

Lemma 6.7. *Suppose that $\sigma \in G$ maps a gate g to g' and that S is a support of g . Then every $\sigma' \in G$ such that $\sigma's = \sigma s$ for all $s \in S$ also maps g to g' .*

Proof. We have $\sigma^{-1}\sigma's = s$ for all $s \in S$, so $\sigma^{-1}\sigma' \in \text{Stab}(S) \leq \text{Stab}(g)$ since S is a support of g . So $\sigma^{-1}\sigma'g = g$, i.e. $\sigma'g = \sigma g = g'$. \square

Theorem 6.8 (Indistinguishability theorem) [DW22, Thm. 4.8]. *Let $G \leq \text{Sym}_n$ and let C be a rigid G -symmetric τ -circuit of order n with $\text{max-supp}(C) \leq k$. Let $\mathcal{A}, \mathcal{B} \in \text{fin}_n[\tau]$. If Duplicator wins the lift-based $(G, 2k)$ -pebble game on \mathcal{A} and \mathcal{B} , then $C[\mathcal{A}] = C[\mathcal{B}]$.*

Proof. From [DW22]. We prove the contrapositive. Suppose $C[\mathcal{A}] \neq C[\mathcal{B}]$: We give a winning Spoiler strategy for the lift-based $(G, 2k)$ -pebble game on \mathcal{A} and \mathcal{B} . As usual, we assume without loss of generality that \mathcal{A} and \mathcal{B} have the same domain $[n]$.

We maintain a pointer to a gate g , initially the single output gate g_{out} . Observe that every automorphism of C fixes g_{out} , since it is the only gate with zero out-degree: hence $C[\mathcal{A}] = C[\mathcal{A}](g_{\text{out}}) \neq C[\mathcal{B}](\sigma g_{\text{out}}) = C[\mathcal{B}]$ for every $\sigma \in G$. Spoiler will then aim to pebble the support of a child gate h of g such that $C[\mathcal{A}](h) \neq C[\mathcal{B}](\sigma h)$, where $\sigma \in G$ is Duplicator's most recently chosen permutation. That is, Spoiler aims to place pebbles on some domain elements \vec{a} in \mathcal{A} and \vec{b} in \mathcal{B} such that $sp(h) \subseteq \vec{a}$ and $C[\mathcal{A}](h) \neq C[\mathcal{B}](\sigma h)$, where σ maps \vec{a} to \vec{b} pointwise (and so

$sp(\sigma h) \subseteq \vec{b}$ by the choice of supports above). In fact, then by Lemma 6.7, every $\sigma' \in G$ which maps \vec{a} to \vec{b} has $\sigma'h = \sigma h$, so $C[\mathcal{A}](h) \neq C[\mathcal{B}](\sigma'h)$ for every $\sigma' \in G$ which respects the pebbles in this sense.

Spoiler then iterates this process, pebbling the support of some child h' of h , and continuing until we reach some input gate $x_{(i,\vec{n})}$. At that point, we have $C[\mathcal{A}](x_{(i,\vec{n})}) \neq C[\mathcal{B}](\sigma x_{(i,\vec{n})})$ for Duplicator's most recently chosen $\sigma \in G$, so either $\vec{n} \in R_i^{\mathcal{A}}$ and $\sigma(\vec{n}) \notin R_i^{\mathcal{B}}$ or $\vec{n} \notin R_i^{\mathcal{A}}$ and $\sigma(\vec{n}) \in R_i^{\mathcal{B}}$. Now we have pebbled the support of $x_{(i,\vec{n})}$ in \mathcal{A} , so $\text{Stab}_G(\vec{a}) \leq \text{Stab}_G(x_{(i,\vec{n})}) = \text{Stab}_G(\vec{n})$ and so \vec{n} is in the r_i -lift of the pebbles \vec{a} , where r_i is the arity of R_i . Hence σ is not a lift-based partial isomorphism from \mathcal{A} to \mathcal{B} with respect to \vec{a} , so Spoiler wins.

The crucial step in this argument is given by the following claim.

Claim 6.9 [DW22, Claim 4.9]. *Suppose that in the current position, the placed pebbles include \vec{a} on \mathcal{A} mapping to pebbles \vec{b} on \mathcal{B} , where $|\vec{a}| = |\vec{b}| \leq k$. Let g be a gate of C with at least one child such that $sp(g) \subseteq \vec{a}$ and for some $\sigma \in G$ that maps \vec{a} to \vec{b} we have $C[\mathcal{A}](g) \neq C[\mathcal{B}](\sigma g)$. There is a strategy for Spoiler such that after at most k rounds, the placed pebbles now include \vec{a}' on \mathcal{A} mapping to pebbles \vec{b}' on \mathcal{B} with $|\vec{a}'| = |\vec{b}'| \leq k$ such that there is some $h \in \text{child}(g)$ with $sp(h) \subseteq \vec{a}'$ and for all $\sigma' \in G$ which map \vec{a}' to \vec{b}' we have $C[\mathcal{A}](h) \neq C[\mathcal{B}](\sigma'h)$.*

Proof. Spoiler maintains the following invariant. Suppose that after $i \geq 0$ rounds, the placed pebbles include \vec{a}, c_1, \dots, c_i on \mathcal{A} mapping to pebbles \vec{b}, d_1, \dots, d_i on \mathcal{B} . Let $S_i = \text{Stab}(\vec{a} \cup \{c_1, \dots, c_i\})$; then $S_0 = \text{Stab}(\vec{a})$. Spoiler will maintain a pointer to a gate $h_i \in \text{child}(g)$ such that $c_1, \dots, c_i \in sp(h_i)$ and

$$|\{h \in \text{Orb}_{S_i}(h_i) : C[\mathcal{A}](h_i) = 1\}| \neq |\{h \in \text{Orb}_{S_i}(h_i) : C[\mathcal{B}](\sigma h_i) = 1\}| \quad (6.3)$$

for all $\sigma \in G$ which map \vec{a}, c_1, \dots, c_i to \vec{b}, d_1, \dots, d_i . Then since $|sp(h_i)| \leq k$, after at most k rounds we have pebbled all of $sp(h_i)$, so $\text{Orb}_{S_i}(h_i) = \{h_i\}$ and the invariant reduces to the claim.

First consider the base case $i = 0$. We have $C[\mathcal{A}](g) \neq C[\mathcal{B}](\sigma g)$. g and σg are labelled by the same function, which is fully symmetric, so its value is determined entirely by the number of 1's in its input. Since σ is an automorphism of C , observe that $\text{child}(\sigma g) = \{\sigma h : h \in \text{child}(g)\}$. So we must have

$$|\{h \in \text{child}(g) : C[\mathcal{A}](h) = 1\}| \neq |\{h \in \text{child}(g) : C[\mathcal{B}](\sigma h) = 1\}|. \quad (6.4)$$

Furthermore, since $sp(g) \subseteq \vec{a}$, we have $S_0 = \text{Stab}(\vec{a}) \leq \text{Stab}(g) \leq \text{SetStab}(\text{child}(g))$, so S_0 partitions $\text{child}(g)$ into orbits. Hence for some $h_0 \in \text{child}(g)$,

$$|\{h \in \text{Orb}_{S_0}(h_0) : C[\mathcal{A}](h) = 1\}| \neq |\{h \in \text{Orb}_{S_0}(h_0) : C[\mathcal{B}](\sigma h) = 1\}|. \quad (6.5)$$

It remains to generalize (6.5) to all $\sigma' \in G$ mapping \vec{a} to \vec{b} . Take any such σ' and let $\rho = \sigma^{-1}\sigma'$. Then $\rho \in S_0 = \text{Stab}(\vec{a})$, so $\text{Orb}_{S_0}(h_0) = \text{Orb}_{S_0}(\rho h_0)$. Hence $\{\sigma h : h \in \text{Orb}_{S_0}(h_0)\} = \{\sigma\rho h : h \in \text{Orb}_{S_0}(h_0)\} = \{\sigma'h : h \in \text{Orb}_{S_0}(h_0)\}$, and so

$$|\{h \in \text{Orb}_{S_0}(h_0) : C[\mathcal{A}](h) = 1\}| \neq |\{h \in \text{Orb}_{S_0}(h_0) : C[\mathcal{B}](\sigma'h) = 1\}|. \quad (6.6)$$

For the inductive step, suppose that the invariant (6.3) holds for i . At the start of round $i+1$, Spoiler picks up a pair of pebbles (a_j, b_j) such that a_j is not in \vec{a} and is not one of c_1, \dots, c_i (that is, a new pair of pebbles or a leftover pair from earlier in the game). Suppose Duplicator plays $\sigma_{i+1} \in G$, which must map \vec{a}, c_1, \dots, c_i to \vec{b}, d_1, \dots, d_i . Then by the induction hypothesis, there is an $h_i \in \text{child}(g)$ such that

$$|\{h \in \text{Orb}_{S_i}(h_i) : C[\mathcal{A}](h) = 1\}| \neq |\{h \in \text{Orb}_{S_i}(h_i) : C[\mathcal{B}](\sigma_{i+1}h) = 1\}| \quad (6.7)$$

and $c_1, \dots, c_i \in sp(h_i)$. Enumerate $sp(h_i) = \{c_1, \dots, c_i, s_{i+1}, \dots, s_u\}$. We can cover $\text{Orb}_{S_i}(h_i)$ by where each element of S_i sends s_{i+1} : define the sets $(O_c)_{c \in [n] \setminus (\vec{a} \cup \{c_1, \dots, c_i\})}$ where $O_c = \{\pi h_i : \pi \in S_i, \pi(s_{i+1}) = c\}$.

Observe that every $h \in \text{Orb}_{S_i}(h_i)$ appears in the same number of sets O_c . Indeed, say $h = \sigma h_i$ for $\sigma \in S_i$. The number of sets O_c in which h appears equals the cardinality of the set $\{\pi(s_{i+1}) : \pi \in S_i, \pi h_i = h\}$. There is a bijection to this set from the fixed set $\{\pi(s_{i+1}) : \pi \in \text{Stab}_{S_i}(h_i)\}$ given by the action of σ .

Then by a double-counting argument, there is some c_{i+1} such that

$$|\{h \in O_{c_{i+1}} : C[\mathcal{A}](h) = 1\}| \neq |\{h \in O_{c_{i+1}} : C[\mathcal{B}](\sigma_{i+1}h) = 1\}|. \quad (6.8)$$

Indeed, if not, suppose every $h \in \text{Orb}_{S_i}(h_i)$ appears in exactly q of the sets O_c : then summing each side of (6.8) over all sets O_c gives q times each side of (6.7), contradicting the invariant.

Spoiler places a_j on c_{i+1} and b_j on $d_{i+1} := \sigma_{i+1}(c_{i+1})$. Let h_{i+1} be any element of $O_{c_{i+1}}$; suppose that $h_{i+1} = \pi h_i$ for $\pi \in S_i$ mapping s_{i+1} to c_{i+1} . To conclude, we prove the following three claims.

- (i) $O_{c_{i+1}} = \text{Orb}_{S_{i+1}}(h_{i+1})$.
- (ii) $c_1, \dots, c_{i+1} \in sp(h_{i+1})$.
- (iii) (6.8) holds with σ_{i+1} substituted for any $\sigma' \in G$ mapping $\vec{a}, c_1, \dots, c_{i+1}$ to $\vec{b}, d_1, \dots, d_{i+1}$.

For (i): Recall that $S_{i+1} = \text{Stab}_G(\vec{a} \cup \{c_1, \dots, c_{i+1}\}) = \text{Stab}_{S_i}(c_{i+1})$. If $\sigma \in S_{i+1}$, then $\sigma h_{i+1} = \sigma \pi h_i \in O_{c_{i+1}}$ since π maps s_{i+1} to c_{i+1} and σ stabilizes c_{i+1} . Conversely, for any $\pi' \in S_i$ mapping s_{i+1} to c_{i+1} , we have $\pi' \pi^{-1} \in S_{i+1}$, so $\pi' h_i = \pi' \pi^{-1} h_{i+1} \in \text{Orb}_{S_{i+1}}(h_{i+1})$. So $O_{c_{i+1}} = \text{Orb}_{S_{i+1}}(h_{i+1})$.

For (ii): $c_1, \dots, c_i, s_{i+1} \in sp(h_i)$ and by the assignment of supports, $sp(h_{i+1}) = sp(\pi h_i) = \pi sp(h_i)$. The claim follows since π stabilizes c_1, \dots, c_i and $\pi(s_{i+1}) = c_{i+1}$.

For (iii): The same argument as in the base case goes through.

By these claims, the invariant is preserved: we have $c_1, \dots, c_{i+1} \in sp(h_{i+1})$, and (6.8) gives

$$|\{h \in \text{Orb}_{S_{i+1}}(h_{i+1}) : C[\mathcal{A}](h) = 1\}| \neq |\{h \in \text{Orb}_{S_{i+1}}(h_{i+1}) : C[\mathcal{B}](\sigma' h) = 1\}| \quad (6.9)$$

for all $\sigma' \in G$ mapping $\vec{a}, c_1, \dots, c_{i+1}$ to $\vec{b}, d_1, \dots, d_{i+1}$, as required. \square

Hence in at most kd rounds, where d is the depth of the circuit C , Spoiler can force a partial isomorphism violation as described above. \square

Observe that in contrast to the support theorem, this proof does not depend on the particular group G . The generalization of the above proof, and particularly that of Claim 6.9, to the quantum pebble games comprises the remaining chapters of Part II.

6.3 Lower bound results

Combining the support theorem and indistinguishability theorem gives us a recipe for proving lower bounds:

Theorem 6.10 [DW22, Thm. 4.13]. *Let $G = \text{Alt}_n$ or Sym_n . Suppose that (\mathcal{A}_n) and (\mathcal{B}_n) are families of τ -structures such that for infinitely many n , Duplicator wins the lift-based (G, k) -pebble game on \mathcal{A}_n and \mathcal{B}_n for $k = \Omega(n)$. Let \mathcal{P} be any τ -property separating (\mathcal{A}_n) and (\mathcal{B}_n) . There is no family of G -symmetric τ -circuits (C_n) which computes \mathcal{P} and has size $s(C_n) = 2^{o(n)}$.*

Proof. From [DW22]. By Lemma 5.7, we may assume without loss of generality that each C_n is rigid. By Theorem 6.8, any rigid G -symmetric τ -circuit C of order n with $\mathbf{max-supp}(C) \leq k/2$ has $C[\mathcal{A}_n] = C[\mathcal{B}_n]$ whenever Duplicator wins the (G, k) -pebble game, so any family of rigid G -symmetric circuits (C_n) computing \mathcal{P} must have $\mathbf{max-supp}(C_n) > k/2$ infinitely often. Hence $\mathbf{max-supp}(C_n)$ is not $o(k)$, so it is also not $o(n)$. Then by the support theorem for G (Theorem 6.3 or 6.4), $\mathbf{max-orbit}(C_n)$ is not $2^{o(n)}$, so C_n does not have size $2^{o(n)}$. \square

In particular, we obtain a concrete lower bound for the CFI property (Section 2.4).

Corollary 6.11. *There is no family of Sym_n -symmetric τ_{graph} -circuits with size $2^{o(n)}$ which computes \mathcal{P}_{CFI} .*

Proof. As observed above, by Proposition 4.13 and the equivalence of the lift-based (G, k) -pebble game and the $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game on classical structures, the CFI graphs fulfill the conditions of Theorem 6.10. \square

This exponential lower bound is remarkable because \mathcal{P}_{CFI} is computable in polynomial time (Theorem 2.23). Hence concretely, symmetry breaking is required to efficiently compute \mathcal{P}_{CFI} .

We also obtain the following result analogous to Corollary 6.11, which is, to the author's knowledge, new.

Corollary 6.12. *There is no family of Alt_n -symmetric τ_{graph} -circuits with size $2^{o(n)}$ which computes $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$.*

Proof. The same proof as Corollary 6.11. As observed above, by Proposition 4.14, the Alt-CFI graphs fulfill the conditions of Theorem 6.10. \square

$\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ is also computable in polynomial time (Corollary 2.28). This result is stronger than Corollary 6.11 in the sense that it shows that breaking Alt_n -symmetry, not just Sym_n -symmetry, is necessary to efficiently compute $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$.

Dawar and Wilsenach use a variant of the above technique to additionally prove lower bounds on symmetric *arithmetic* circuits computing the matrix permanent [DW20] and the determinant [DW22]. Dawar also extends Corollary 6.11 to prove lower bounds for other, more natural properties by means of symmetric circuit reductions [Daw15a]. Generalizations of these extensions to quantum circuits are not explored in this thesis and are left for future work.

Chapter 7

Quantum lower bounds without entanglement

This chapter proves new lower bounds for quantum circuits which do not use entanglement by adapting the technique of Dawar and Wilsenach [DW22] for classical circuits. Except where noted, it contains entirely original material.

In this and the next chapter, we adapt Dawar and Wilsenach’s technique from Chapter 6 to quantum circuits using our partial trace-based quantum pebble game introduced in Chapter 4. We focus on quantum circuits taking classical structures as input, encoded as computational basis states $|\mathcal{A}\rangle$, and thereby obtain lower bounds on the size of quantum circuits solving classical problems. Our technique is heavily dependent on the amount of entanglement used by the circuit in the following sense.

Definition 7.1. Let $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be a state on n qubits. The *entanglement width* of $|\psi\rangle$, denoted $\eta(|\psi\rangle)$, is the smallest integer such that $|\psi\rangle$ admits a decomposition $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$, where each state $|\psi_i\rangle$ is defined over a subset of qubits $S_i \subseteq [n]$ of size $|S_i| \leq \eta(|\psi\rangle)$.

That is, if $\eta(|\psi\rangle) \leq \eta$, then the state $|\psi\rangle$ uses at most η -partite entanglement. Entanglement width was previously defined by Jozsa and Linden [JL03, Def. 4], where it was called being “ p -blocked”.

Definition 7.2. Let C be an output quantum τ -circuit of order n whose layers are represented by unitaries L_1, \dots, L_m . Let $L_{\leq i} = L_i L_{i-1} \cdots L_1$ for each $i \in [m]$. The *entanglement width* of C is defined as

$$\eta(C) := \max_{i \in [m], \mathcal{A} \in \text{fin}_n[\tau]} \eta(L_{\leq i}|\mathcal{A}\rangle|0\rangle^{\otimes a(C)}). \quad (7.1)$$

That is, if $\eta(C) \leq \eta$, then when a classical structure $|\mathcal{A}\rangle$ (i.e., a computational basis state) is given as input, after every layer, the state of the circuit uses at most η -partite entanglement.

States $|\psi\rangle$ with $\eta(|\psi\rangle) = 1$ are product states, and circuits C with $\eta(C) = 1$ operate (between layers) only on product states. This chapter presents lower bounds for such circuits; Chapter 8 then generalizes the technique to the substantially more complex case of circuits with entanglement width bounded by an arbitrary function.

Our results hold for rigid circuits over the following gate set:

Definition 7.3. The *CNOT gate set* $\mathbb{G}_{\text{CNOT}}^Q$ consists of all 1-qubit unitaries and the CNOT gate. More formally, on wires W , $\mathbb{G}_{\text{CNOT}}^Q$ consists of all unitaries $U_w \otimes \mathbb{I}$ which apply a 1-qubit unitary $U \in \text{U}(\mathbb{C}^2)$ to a wire $w \in W$, and the unitaries $\text{CNOT}_{c,t} \otimes \mathbb{I}$ which apply the CNOT gate to control and target wires $c, t \in W$ with $c \neq t$.

This gate set is universal in the strong sense that it can exactly implement any n -qubit unitary [KLM06, Thm. 4.3.3]. Circuits over $\mathbb{G}_{\text{CNOT}}^Q$ have favourable combinatorial properties: in particular, our technique as-is does *not* prove lower bounds for circuits over the threshold gate set $\mathbb{G}_{\text{thr}}^Q$ for reasons explained in Section 7.2.

We work with rigid Γ_G -permutation symmetric circuits C for some $G \leq \text{Sym}_n$: that is, we work only with symmetries and automorphisms which just permute the wires W . We use the classical pebble set $\mathcal{P} = \mathcal{P}_G$, where each pebble $\Gamma_p \leq \Gamma_G$ is the subgroup of unitaries U_σ which stabilize some domain element. We therefore also assume that G has distinct stabilizers, which is the case for Sym_n and Alt_n for $n \geq 4$ (see Section 3.3.1).

By rigidity, for every permutation $\sigma \in G$, the corresponding unitary $U_\sigma \in \Gamma_G$ induces a unique automorphism $U_\pi \in \Gamma_{\text{Sym}_W}$ of C which applies the permutation $\pi \in \text{Sym}_W$ to the wires. Hence G acts on the set of wires W : each $\sigma \in G$ applies the corresponding permutation $\pi \in \text{Sym}_W$ to the wires. In this chapter and Chapter 8, we usually work directly with this action of G on W . Since the pebbles in \mathcal{P}_G are subgroups of Γ_G , which naturally correspond to subgroups of G via the natural embedding $G \rightarrow \Gamma_G$, we often abuse notation and refer to the pebbles in \mathcal{P}_G as if they were the corresponding subgroups of G : for example, if $P \subseteq \mathcal{P}_G$, we might write $\sigma \in \bigcap P$ or $\bigcap P \leq \text{Stab}_G(w)$ for some $w \in W$. We also often do not distinguish between unitaries $U \in \Gamma_G$ and the unique automorphisms of C which they induce: for example, if $U \in \Gamma_G$ and $\rho \in \text{D}(\mathcal{H}_W)$, we might write $U\rho U^\dagger$ where strictly we mean $V\rho V^\dagger$, where V is the unique automorphism of C induced by U .

I emphasize that our results hold only for rigid quantum circuits. Dawar and Wilsenach's technique extends their results from rigid circuits to all circuits by providing an efficient transformation from any circuit to an equivalent rigid circuit. As explained in Section 5.4, we do not yet have such a transformation for quantum circuits, so our results must assume rigidity.

7.1 Support

We define support using the notion of lift from Chapters 4 and 6, originally due to Dawar and Wilsenach [DW22], which we now redefine in a quantum circuit context. Fix a Γ_G -permutation symmetric output quantum circuit C of order n on wires $W = X \sqcup A$. The *lift* of a set of pebbles $P \subseteq \mathcal{P}_G$ to W is

$$W_P := \{w \in W : \bigcap P \leq \text{Stab}_G(w)\} \tag{7.2}$$

where G acts on W as explained above. We say P *supports* a wire $w \in W$ if $w \in W_P$. Let **min-supp**(w) be the size of the smallest set of pebbles $P \subseteq \mathcal{P}_G$ which supports w , and let **max-supp**(C) = $\max_{w \in W} \text{min-supp}(w)$. (Note that for ancilla wires w , **min-supp**(w)

depends on how the symmetries G of the input wires extend to the ancillas, which depends on the topology of C .) Let $\mathbf{max-orbit}(C) = \max_{w \in W} |\text{Orb}_G(w)|$. We are now ready to prove a support theorem for $G = \text{Alt}_n$, which follows by a direct adaptation of the proof of Theorem 6.3.

Theorem 7.4 (Quantum support theorem for Alt_n). *Let (C_n) be a family of rigid Γ_{Alt_n} -permutation symmetric output quantum circuits. If $\mathbf{max-orbit}(C_n) = 2^{o(n)}$ then $\mathbf{max-supp}(C_n) = o(n)$.*

Proof. We follow Theorem 6.3. Let k be the smallest positive integer with $\mathbf{max-orbit}(C_n) < \binom{n}{k}$: then as before, $k = o(n)$, so for large enough n , $k \leq \frac{n}{4}$. By the orbit–stabilizer theorem, for every wire w in C_n , $[\text{Alt}_n : \text{Stab}_{\text{Alt}_n}(w)] < \binom{n}{k}$. Then by Lemma 6.2, there is some $S \subseteq [n]$ with $|S| < k$ such that $\text{Stab}_{\text{Alt}_n}(S) \leq \text{Stab}_{\text{Alt}_n}(w)$. Then, abusing notation as explained above, consider the set of pebbles $P = \{\text{Stab}_{\text{Alt}_n}(s) : s \in S\} \subseteq \mathcal{P}_G$; then $\bigcap P = \text{Stab}_{\text{Alt}_n}(S)$, so $\bigcap P \leq \text{Stab}_{\text{Alt}_n}(w)$ and so P supports w , and we have $|P| < k$. Hence $\mathbf{max-supp}(C_n) < k = o(n)$. \square

We do not have an analogous result for Sym_n because unlike for Alt_n , the classical support theorem for Sym_n (Theorem 6.4) relies on the DAG structure of classical circuits and so cannot be readily adapted to the quantum setting.

7.2 Reconstructibility and partition symmetry

We now introduce several technical properties which are needed to state our indistinguishability theorem. Fix a set of wires $W = X \sqcup A$ and a group $G \leq \text{Sym}_n$ with distinct stabilizers. If $f : S \rightarrow T$ is a function and σ is an element of a group acting on S , define the function $f \circ \sigma$ by $(f \circ \sigma)(s) = f(\sigma s)$ for all $s \in S$. Additionally, observe that for every $\sigma \in \text{Sym}_W$, $w \in W$, and $\rho \in D(\mathcal{H}_W)$, since U_σ just permutes the wires according to σ , we have

$$\text{Tr}_{\overline{\sigma(w)}}(\rho) = \text{Tr}_{\overline{w}}(U_\sigma^\dagger \rho U_\sigma). \quad (7.3)$$

Definition 7.5. For every density matrix $\rho \in D(\mathcal{H}_W)$, define the *part function*

$$\begin{aligned} f_\rho : W &\rightarrow D(\mathbb{C}^2) \\ w &\mapsto \text{Tr}_{\overline{w}}(\rho). \end{aligned} \quad (7.4)$$

For each $S \subseteq W$, let $f_\rho^S : S \rightarrow D(\mathbb{C}^2)$ be the restriction of f_ρ to the domain S .

Lemma 7.6. *For all $\rho \in D(\mathcal{H}_W)$, $S \subseteq W$, and $\sigma \in \text{SetStab}_{\text{Sym}_W}(S)$, we have $f_{U_\sigma^\dagger \rho U_\sigma}^S = f_\rho^S \circ \sigma'$, where $\sigma' \in \text{Sym}_S$ is such that $\sigma'(w) = \sigma(w)$ for all $w \in S$.*

Proof. For all $w \in S$, by equation (7.3), $f_{U_\sigma^\dagger \rho U_\sigma}^S(w) = \text{Tr}_{\overline{w}}(U_\sigma^\dagger \rho U_\sigma) = \text{Tr}_{\overline{\sigma(w)}}(\rho) = \text{Tr}_{\overline{\sigma'(w)}}(\rho) = (f_\rho^S \circ \sigma')(w)$. \square

Definition 7.7. A set of density matrices $\Delta \subseteq \mathcal{H}_W$ is *reconstructible* if the map $\rho \mapsto f_\rho$ is injective on the domain Δ ; that is, every $\rho \in \Delta$ is determined uniquely among elements of Δ by its part function.

Definition 7.8. Let C be a Γ_G -permutation symmetric output quantum τ -circuit of order n whose layers are represented by unitaries L_1, \dots, L_m , and let $L_{\leq i} = L_i L_{i-1} \cdots L_1$. C is *reconstructible* if for every $0 \leq i \leq m$, the set

$$\Delta_i(C) := \{L_{\leq i}(|\mathcal{A}\rangle|0\rangle^{\otimes a(C)}) (\langle \mathcal{A}|0|^{\otimes a(C)}) L_{\leq i}^\dagger : \mathcal{A} \in \text{fin}_n[\tau]\} \quad (7.5)$$

is reconstructible.

That is, we define C to be reconstructible just if the set of states that could appear after each layer when given classical structures as input is reconstructible. Each $\Delta_i(C)$ is closed under conjugation by any $U_\sigma \in \Gamma_G$: indeed, U_σ commutes with $L_{\leq i}$ since U_σ is an automorphism of C , and since U_σ permutes the input and ancilla wires separately, it maps computational basis states $|\mathcal{A}\rangle|0\rangle^{\otimes a(C)}$ to other computational basis states of that form.

Observe that every $\Delta \subseteq D(\mathcal{H}_W)$ consisting only of density matrices of pure product states is reconstructible since product states are uniquely determined by their single-qubit partial traces. Hence every Γ_G -permutation symmetric quantum circuit C with $\eta(C) = 1$ is reconstructible.

Lemma 7.9. $\Delta \subseteq D(\mathcal{H}_W)$ is reconstructible if and only if it has the following property: for every $\rho_1, \rho_2 \in \Delta$ and $\sigma \in \text{Sym}_W$, we have $f_{\rho_1} = f_{\rho_2} \circ \sigma$ iff $U_\sigma \rho_1 U_\sigma^\dagger = \rho_2$.

Proof. (\Leftarrow) Easy. Suppose $\rho_1, \rho_2 \in D(\mathcal{H}_W)$ have $f_{\rho_1} = f_{\rho_2}$. Then $f_{\rho_1} = f_{\rho_2} \circ e$, where $e \in \text{Sym}_W$ is the identity; $U_e = \mathbb{I}$, so by the property, $\mathbb{I} \rho_1 \mathbb{I}^\dagger = \rho_2$, i.e. $\rho_1 = \rho_2$.

(\Rightarrow) Suppose Δ is reconstructible. By Lemma 7.6, $f_{\rho_1} = f_{\rho_2} \circ \sigma$ iff $f_{\rho_1} = f_{U_\sigma^\dagger \rho_2 U_\sigma}$, which by reconstructibility occurs iff $\rho_1 = U_\sigma^\dagger \rho_2 U_\sigma$, i.e. $U_\sigma \rho_1 U_\sigma^\dagger = \rho_2$. \square

Definition 7.10. A unitary $L \in U(\mathcal{H}_W)$ has *partition symmetry* with respect to a pebble set \mathcal{P} if for every $P \subseteq \mathcal{P}$ and every $w \in W_P$, there exists a partition $(E_i)_i$ of W such that $\bigcap P \leq \prod_i \text{Sym}_{E_i}$ and for every $\rho \in D(\mathcal{H}_W)$ and every $\sigma \in \prod_i \text{Sym}_{E_i}$, viewed as a unitary U_σ , we have $\text{Tr}_{\overline{w}}(LU_\sigma \rho U_\sigma^\dagger L^\dagger) = \text{Tr}_{\overline{w}}(L\rho L^\dagger)$.

Here $\prod_i \text{Sym}_{E_i}$ denotes the subgroup of Sym_W consisting of all permutations σ which map elements of each set E_i only to other elements of E_i . To understand this technical property, think of L as a layer in a quantum circuit. The property states that for every wire w and set of pebbles P , there is some partition of the wires which is respected by the pebbles such that every permutation preserving the partition does not affect the output of the layer on w . L might not be formally symmetric against all such permutations, but its output on w must be invariant.

Definition 7.11. Let C be a rigid Γ_G -permutation symmetric output quantum τ -circuit of order n . C has *partition symmetry* with respect to a pebble set \mathcal{P} if for each of its layers \mathcal{L} , the unitary L representing \mathcal{L} has partition symmetry with respect to \mathcal{P} .

Lemma 7.12. Let $G \leq \text{Sym}_n$ with distinct stabilizers. Every rigid Γ_G -permutation symmetric output quantum circuit C over the gate set $\mathbb{G}_{\text{CNOT}}^Q$ has partition symmetry with respect to \mathcal{P}_G .

Proof. Let W be the set of wires in C . Let $P \subseteq \mathcal{P}_G$ and $w \in W_P$. Assume without loss of generality that each layer \mathcal{L} in C consists of exactly one orbit of gates under conjugation by Γ_G . (We can always split up the layers of C to be of this form.) Then \mathcal{L} consists of either 1-qubit unitaries of the same type or CNOT gates. Let L be the unitary representing a layer \mathcal{L} .

First suppose \mathcal{L} applies some 1-qubit unitary U to the wires $S \subseteq W$. Define a partition $(E_i)_i$ of W by $E_1 = \{w\}$, $E_2 = S \setminus \{w\}$ and $E_3 = (W \setminus \{w\}) \setminus S$. Then each $\sigma \in \prod_i \text{Sym}_{E_i}$ just maps wires with the unitary U applied to other wires with U and wires without U to wires without U , so U_σ is an automorphism of the layer \mathcal{L} . Indeed, every automorphism of \mathcal{L} in Γ_G that stabilizes w is of the form U_σ for some $\sigma \in \prod_i \text{Sym}_{E_i}$, so $\bigcap P \leq \prod_i \text{Sym}_{E_i}$ and $L = U_\sigma L U_\sigma^\dagger$ for all $\sigma \in \prod_i \text{Sym}_{E_i}$. Hence, using equation (7.3), $\text{Tr}_{\bar{w}}(LU_\sigma \rho U_\sigma^\dagger L^\dagger) = \text{Tr}_{\bar{w}}(U_\sigma L \rho L^\dagger U_\sigma^\dagger) = \text{Tr}_{\bar{w}}(L \rho L^\dagger)$ for all ρ since σ stabilizes w , so conjugating by U_σ does not affect the partial trace to w .

Next, suppose \mathcal{L} consists of CNOT gates. Since all gates in a layer must commute, no wire can be both a control and target wire for any two CNOT gates in \mathcal{L} . Partition W into four sets: let $E_1 = \{w\}$, $E_2 = \{c \in W \setminus \{w\} : \text{CNOT}_{c,w} \in \mathcal{L}\}$ be the set of control wires of gates with target wire w , $E_3 = \{t \in W \setminus \{w\} : \text{CNOT}_{w,t} \in \mathcal{L}\}$ be the set of target wires of gates with control wire w , and $E_4 = W \setminus (E_1 \cup E_2 \cup E_3)$.

Any automorphism of C which stabilizes w must preserve this partition, so $\bigcap P \leq \prod_i \text{Sym}_{E_i}$. Furthermore, a wire's effect on w is determined only by which set in the partition it lies in. More precisely, since all gates in \mathcal{L} commute, divide \mathcal{L} into the set of gates S_1 which have w as their control or target wire and the gates S_2 which do not, and consider the gates in S_1 to be ordered before those in S_2 . For each $\sigma \in \prod_i \text{Sym}_{E_i}$, U_σ is an automorphism of the gates in S_1 , and since the gates in S_2 act trivially on w , they cannot affect the partial trace to w of the resulting state by the no-communication theorem [PT04]. So, let L_1 and L_2 be the products of the unitaries in S_1 and S_2 respectively: we have $L = L_2 L_1$ and $L_1 = U_\sigma L_1 U_\sigma^\dagger$ for each $\sigma \in \prod_i \text{Sym}_{E_i}$, and $\text{Tr}_{\bar{w}}(L_2 \rho L_2^\dagger) = \text{Tr}_{\bar{w}}(\rho)$ for all ρ , so for each ρ ,

$$\begin{aligned} \text{Tr}_{\bar{w}}(LU_\sigma \rho U_\sigma^\dagger L^\dagger) &= \text{Tr}_{\bar{w}}(L_2 L_1 U_\sigma \rho U_\sigma^\dagger L_1^\dagger L_2^\dagger) = \text{Tr}_{\bar{w}}(U_\sigma L_1 \rho L_1^\dagger U_\sigma^\dagger) \\ &\stackrel{(7.3)}{=} \text{Tr}_{\bar{w}}(L_1 \rho L_1^\dagger) = \text{Tr}_{\bar{w}}(L_2 L_1 \rho L_1^\dagger L_2^\dagger) = \text{Tr}_{\bar{w}}(L \rho L^\dagger). \end{aligned} \quad \square$$

Note that circuits over $\mathbb{G}_{\text{thr}}^Q$ do not necessarily have partition symmetry since their symmetries may generally be too rich to admit a partition as above; hence our results as-is do not apply to circuits over $\mathbb{G}_{\text{thr}}^Q$.

7.3 A product state indistinguishability theorem

We are ready to prove our adaptation of the indistinguishability theorem. Fix for the moment a group $G \leq \text{Sym}_n$ with distinct stabilizers and a rigid Γ_G -permutation symmetric output quantum circuit C of order n with wires W . We begin by assigning supports $sp(w) \subseteq \mathcal{P}_G$ to each $w \in W$. Below, we treat the pebble groups Γ_p in \mathcal{P}_G as subgroups of G , using the abuse of notation explained earlier.

Lemma 7.13. Suppose $P \subseteq \mathcal{P}_G$ supports $w \in W$ and $\sigma \in G$. Then $\sigma P \sigma^{-1} := \{\sigma \Gamma_p \sigma^{-1} : \Gamma_p \in P\}$ supports σw .

Proof. Observe that $\bigcap(\sigma P \sigma^{-1}) = \{\sigma \pi \sigma^{-1} : \pi \in \bigcap P\}$. P supports w , so $\bigcap P \leq \text{Stab}_G(w)$. Let $\pi \in \bigcap P$: then $\pi w = w$, so $(\sigma \pi \sigma^{-1})(\sigma w) = \sigma w$. Hence $\bigcap(\sigma P \sigma^{-1}) \leq \text{Stab}_G(\sigma w)$ and so $\sigma P \sigma^{-1}$ supports σw . \square

Therefore, to each wire w we assign a support $sp(w) \subseteq \mathcal{P}_G$ such that $sp(\sigma w) = \sigma sp(w) \sigma^{-1}$ for all $\sigma \in G$. Since $|\sigma P \sigma^{-1}| = |P|$ for all $P \subseteq \mathcal{P}_G$, if $\mathbf{max-supp}(C) \leq k$, we may assume $|sp(w)| \leq k$ for all w .

Theorem 7.14 (Indistinguishability theorem for product states). *Let $G \leq \text{Sym}_n$ with distinct stabilizers. Let C be a rigid Γ_G -permutation symmetric output quantum τ -circuit of order n which is reconstructible, has partition symmetry with respect to \mathcal{P}_G , and has $\mathbf{max-supp}(C) \leq k$. Let $\mathcal{A}, \mathcal{B} \in \text{fin}_n[\tau]$. If Duplicator wins the $(\Gamma_G, \mathcal{P}_G, 2k)$ -1-PT quantum pebble game on $|\mathcal{A}\rangle$ and $|\mathcal{B}\rangle$, then $C[|\mathcal{A}\rangle] = C[|\mathcal{B}\rangle]$.*

Proof. Suppose C has wires $W = X \sqcup A$. We again prove the contrapositive. Suppose $C[|\mathcal{A}\rangle] \neq C[|\mathcal{B}\rangle]$: We give a Spoiler strategy for the $(\Gamma_G, \mathcal{P}_G, 2k)$ -1-PT quantum pebble game on $|\mathcal{A}\rangle$ and $|\mathcal{B}\rangle$. Let the layers of C be represented by unitaries L_1, \dots, L_m . For each $0 \leq i \leq m$, let $L_{\leq i} = L_i L_{i-1} \cdots L_1$ and let $\rho_i^{\mathcal{A}} = L_{\leq i}(|\mathcal{A}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{A}| \langle 0|^{\otimes a(C)})L_{\leq i}^\dagger$ and $\rho_i^{\mathcal{B}} = L_{\leq i}(|\mathcal{B}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{B}| \langle 0|^{\otimes a(C)})L_{\leq i}^\dagger$.

We traverse the circuit layer by layer from output to input. Spoiler plays to maintain the invariant that for each i there is a wire $w_i \in W$ supported by the current set of pebbles P such that for the current unitary $U \in \Gamma_G$ we have $\text{Tr}_{\overline{w_i}}(\rho_i^{\mathcal{A}}) \neq \text{Tr}_{\overline{w_i}}(U^\dagger \rho_i^{\mathcal{B}} U)$. (Recall that we do not distinguish between $U \in \Gamma_G$ and the unique automorphism of C in Γ_{Sym_W} induced by U .) Then for $i = 0$, we have $\text{Tr}_{\overline{w_0}}(\rho_0^{\mathcal{A}}) \neq \text{Tr}_{\overline{w_0}}(U^\dagger \rho_0^{\mathcal{B}} U)$ where $\rho_0^{\mathcal{A}} = (|\mathcal{A}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{A}| \langle 0|^{\otimes a(C)})$ and $\rho_0^{\mathcal{B}} = (|\mathcal{B}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{B}| \langle 0|^{\otimes a(C)})$. Since the automorphism U permutes X and A separately, if w_0 is an ancilla, then $\text{Tr}_{\overline{w_0}}(\rho_0^{\mathcal{A}}) = \text{Tr}_{\overline{w_0}}(U^\dagger \rho_0^{\mathcal{B}} U) = |0\rangle\langle 0|$. Since this is not the case, w_0 must be an input wire, so we must have $\text{Tr}_{\overline{w_0}}(|\mathcal{A}\rangle\langle \mathcal{A}|) \neq \text{Tr}_{\overline{w_0}}(U^\dagger |\mathcal{B}\rangle\langle \mathcal{B}| U)$, considering U to act only on the input wires. This is a violation of 1-PT partial isomorphism, so Spoiler wins.

For the base case $i = m$, recall that the output wire w_{out} of C is not moved by any automorphism of C , so it is supported by the empty set of pebbles. Let $w_m = w_{\text{out}}$. Since $C[|\mathcal{A}\rangle] \neq C[|\mathcal{B}\rangle]$, we must have $\text{Tr}_{\overline{w_m}}(\rho_m^{\mathcal{A}}) \neq \text{Tr}_{\overline{w_m}}(\rho_m^{\mathcal{B}})$, as required.

The inductive step follows from the following claim, observing that $\rho_{i+1}^{\mathcal{A}} = L_{i+1} \rho_i^{\mathcal{A}} L_{i+1}^\dagger$ and $\rho_{i+1}^{\mathcal{B}} = L_{i+1} \rho_i^{\mathcal{B}} L_{i+1}^\dagger$.

Claim 7.15. Suppose we are at layer $0 \leq i < m$, and let $L = L_{i+1}$, $\rho_{\mathcal{A}} = \rho_i^{\mathcal{A}}$, and $\rho_{\mathcal{B}} = \rho_i^{\mathcal{B}}$. Suppose we are in a position where the pebbles include $P \subseteq \mathcal{P}_G$ with $|P| \leq k$ and the unitary is $U \in \Gamma_G$, and we have a wire $w = w_{i+1}$ supported by P such that

$$\text{Tr}_{\overline{w}}(L \rho_{\mathcal{A}} L^\dagger) \neq \text{Tr}_{\overline{w}}(U^\dagger L \rho_{\mathcal{B}} L^\dagger U). \quad (7.6)$$

There is a strategy for Spoiler such that after at most k rounds, we are in a position where the pebbles include $P' \subseteq \mathcal{P}_G$ with $|P'| \leq k$ and the unitary is $U' \in \Gamma_G$, and we have a wire w' supported by P' such that

$$\mathrm{Tr}_{\overline{w'}}(\rho_A) \neq \mathrm{Tr}_{\overline{w'}}(U'^\dagger \rho_B U'). \quad (7.7)$$

Proof. Since C has partition symmetry, there is a partition $(E_i)_i$ of W with the properties of Definition 7.10. These properties imply that $\rho_A \neq U_\sigma U^\dagger \rho_B U U_\sigma^\dagger$ for any $\sigma \in \prod_i \mathrm{Sym}_{E_i}$: indeed,

$$\mathrm{Tr}_{\overline{w}}(LU_\sigma U^\dagger \rho_B U U_\sigma^\dagger L^\dagger) = \mathrm{Tr}_{\overline{w}}(LU^\dagger \rho_B U L^\dagger) = \mathrm{Tr}_{\overline{w}}(U^\dagger L \rho_B L^\dagger U) \quad (7.8)$$

where the first equality comes from Definition 7.10 and the second holds since $U \in \Gamma_G$ is an automorphism of C , so L commutes with U (and so with U^\dagger). Hence if $\rho_A = U_\sigma U^\dagger \rho_B U U_\sigma^\dagger$ then $\mathrm{Tr}_{\overline{w}}(L\rho_A L^\dagger) = \mathrm{Tr}_{\overline{w}}(U^\dagger L \rho_B L^\dagger U)$, contradicting (7.6).

The orbits of W under $\bigcap P \leq G$ partition W : let $(O_i)_i$ be those orbits. Since $\bigcap P \leq \prod_i \mathrm{Sym}_{E_i}$ by Definition 7.10, the orbits of W under $\bigcap P$ form a refinement of those under $\prod_i \mathrm{Sym}_{E_i}$ (which are just $(E_i)_i$), so $\prod_i \mathrm{Sym}_{O_i} \leq \prod_i \mathrm{Sym}_{E_i}$. So in particular, $\rho_A \neq U_\sigma U^\dagger \rho_B U U_\sigma^\dagger$ for any $\sigma \in \prod_i \mathrm{Sym}_{O_i}$. Then since C is reconstructible, by Lemma 7.9,

$$f_{\rho_A} \circ \sigma \neq f_{U^\dagger \rho_B U} \quad (7.9)$$

for any $\sigma \in \prod_i \mathrm{Sym}_{O_i}$. The domain of these functions is W , which is partitioned by $(O_i)_i$, so there is some orbit O' of W under $\bigcap P$ such that

$$f_{\rho_A}^{O'} \circ \sigma \neq f_{U^\dagger \rho_B U}^{O'} \quad (7.10)$$

for all $\sigma \in \mathrm{Sym}_{O'} \leq \prod_i \mathrm{Sym}_{O_i}$.

We now place pebbles. Suppose that in the j th round, the pebbles include $P_j = P \cup \{\Gamma_{p_1}, \dots, \Gamma_{p_j}\}$ and the current unitary is U_j . I claim that Spoiler can play to maintain the following invariant: there is some $w_j \in W$ such that $\Gamma_{p_1}, \dots, \Gamma_{p_j} \in sp(w_j)$ and for its orbit $O'_j = \mathrm{Orb}_{\bigcap P_j}(w_j)$ under $\bigcap P_j$ we have

$$f_{\rho_A}^{O'_j} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{O'_j} \quad (7.11)$$

for all $\sigma \in \mathrm{Sym}_{O'_j}$. Then since $|sp(w_j)| \leq k$, after at most k rounds, we have $O'_j = \{w_j\}$ and so the invariant gives us $\mathrm{Tr}_{\overline{w_j}}(\rho_A) \neq \mathrm{Tr}_{\overline{w_j}}(U_j^\dagger \rho_B U_j)$ with w_j supported by $\{\Gamma_{p_1}, \dots, \Gamma_{p_j}\}$, which proves the claim.

The case $j = 0$ is given above: take $O'_0 = O'$, $U_0 = U$, $P_0 = P$, and choose $w_0 \in O'_0$ arbitrarily. In round $j \geq 1$, Spoiler first picks up some pebble not in the support of w or w_{j-1} if necessary. From the invariant, we have

$$f_{\rho_A}^{O'_{j-1}} \circ \sigma \neq f_{U_{j-1}^\dagger \rho_B U_{j-1}}^{O'_{j-1}} \quad (7.12)$$

for all $\sigma \in \text{Sym}_{O'_{j-1}}$. Duplicator chooses some unitary $U_\pi \in \bigcap P_{j-1}$ and sets $U_j := U_{j-1}U_\pi$. Since O'_{j-1} is an orbit of $\bigcap P_{j-1}$, π maps elements of O'_{j-1} to elements of O'_{j-1} : let $\pi' \in \text{Sym}_{O'_{j-1}}$ be the action of π restricted to O'_{j-1} . Now by Lemma 7.6,

$$f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}} = f_{U_\pi^\dagger U_{j-1}^\dagger \rho_B U_{j-1} U_\pi}^{O'_{j-1}} = f_{U_{j-1}^\dagger \rho_B U_{j-1}}^{O'_{j-1}} \circ \pi' \quad (7.13)$$

and so combining with (7.12), we have

$$f_{\rho_A}^{O'_{j-1}} \circ \sigma \pi' \neq f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}} \quad (7.14)$$

for all $\sigma \in \text{Sym}_{O'_{j-1}}$. But $\pi' \in \text{Sym}_{O'_{j-1}}$, so in fact

$$f_{\rho_A}^{O'_{j-1}} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}} \quad (7.15)$$

for all $\sigma \in \text{Sym}_{O'_{j-1}}$. Having defused Duplicator's choice of unitary, we now show how Spoiler can make progress. Let Γ_p be some pebble in $sp(w_{j-1})$ which is not yet in P_{j-1} . For each pebble $\Gamma_q \in \mathcal{P}_G$ which is conjugate to Γ_p by some $\pi \in \bigcap P_{j-1}$ (considered as a subgroup of G), let

$$W_q := \{\pi w_{j-1} : \pi \in \bigcap P_{j-1}, \pi \Gamma_p \pi^{-1} = \Gamma_q\}. \quad (7.16)$$

I make a series of claims about these sets $(W_q)_q$:

- (i) Every $v \in O'_{j-1}$ appears in the same number of sets W_q .
- (ii) There is some Γ_q such that $f_{\rho_A}^{W_q} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{W_q}$ for all $\sigma \in \text{Sym}_{W_q}$.
- (iii) For every Γ_q , we have $W_q = \text{Orb}_{\Gamma_q \cap \bigcap P_{j-1}}(v)$ for all $v \in W_q$.

For (i): Let $v \in O'_{j-1}$; then $v = \sigma w_{j-1}$ for some $\sigma \in \bigcap P_{j-1}$. The set of Γ_q such that v is in W_q is given by $\{\pi \Gamma_p \pi^{-1} : \pi \in \bigcap P_{j-1}, \pi w_{j-1} = v\}$. There is a bijection to this set from the fixed set $\{\pi \Gamma_p \pi^{-1} : \pi \in \text{Stab}_{\bigcap P_{j-1}}(w_{j-1})\}$ given by conjugating by σ .

For (ii): Suppose there is no such Γ_q . Then for each Γ_q there is some $\sigma \in \text{Sym}_{W_q}$ such that $f_{\rho_A}^{W_q} \circ \sigma = f_{U_j^\dagger \rho_B U_j}^{W_q}$. That is, the multisets given by the images of $f_{\rho_A}^{W_q}$ and $f_{U_j^\dagger \rho_B U_j}^{W_q}$ are equal. By claim (i), taking the union of these multisets for all Γ_q gives a multiset in which the image of each $v \in O'_{j-1}$ appears the same number of times (say t times). That is, the resulting multiset consists of t copies of the images of $f_{\rho_A}^{O'_{j-1}}$ and $f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}}$, so those images are equal as multisets and so $f_{\rho_A}^{O'_{j-1}} \circ \sigma = f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}}$ for some $\sigma \in \text{Sym}_{O'_{j-1}}$, contradicting (7.15).

For (iii): For brevity, let $Q = \Gamma_q \cap \bigcap P_{j-1}$ and $w = w_{j-1}$. Let $v \in W_q$: there is some $\pi \in \bigcap P_{j-1}$ such that $v = \pi w$ and $\pi \Gamma_p \pi^{-1} = \Gamma_q$. For every $\sigma \in Q$, we have $\sigma v = \sigma \pi w$ and $(\sigma \pi) \Gamma_p (\sigma \pi)^{-1} = \sigma (\pi \Gamma_p \pi^{-1}) \sigma^{-1} = \sigma \Gamma_q \sigma^{-1} = \Gamma_q$ since $\sigma \in \Gamma_q$, so $\sigma v = \sigma \pi w \in W_q$ and so $\text{Orb}_Q(v) \subseteq W_q$. Conversely, for every $\sigma \in \bigcap P_{j-1}$ such that $\sigma \Gamma_p \sigma^{-1} = \Gamma_q$ (that is, for every $\sigma w \in W_q$), we have $(\sigma \pi^{-1}) \Gamma_q (\sigma \pi^{-1})^{-1} = \sigma (\pi^{-1} \Gamma_q \pi) \sigma^{-1} = \sigma \Gamma_p \sigma^{-1} = \Gamma_q$. But, since G has distinct stabilizers, every pebble is by definition a self-normalizing subgroup (see Section 3.3.1); thus we have $\sigma \pi^{-1} \in \Gamma_q$ and so $\sigma \pi^{-1} \in Q$. Furthermore, $\sigma \pi^{-1} v = \sigma \pi^{-1} \pi w = \sigma w$, so $\sigma w \in \text{Orb}_Q(v)$. Hence $W_q \subseteq \text{Orb}_Q(v)$ as well.

Thus, by claim (ii), let Γ_q be such that $f_{\rho_A}^{W_q} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{W_q}$ for all $\sigma \in W_q$. Spoiler places the pebble Γ_q : let $P_j = P_{j-1} \cup \{\Gamma_q\}$. Choose $w_j \in W_q$ arbitrarily. We have $w_j = \pi w_{j-1}$ for some $\pi \in \bigcap P_{j-1}$ with $\Gamma_q = \pi \Gamma_p \pi^{-1}$, so by our assumption on the assignment of supports, $\Gamma_{p_1}, \dots, \Gamma_{p_{j-1}}, \Gamma_q \in sp(w_j)$. By claim (iii), $W_q = \text{Orb}_{\bigcap P_j}(w_j)$, so let $O'_j = W_q$. This preserves the invariant. \square

Repeatedly applying Claim 7.15 gives a Spoiler strategy which wins in at most km rounds. \square

As in the classical case, unlike the support theorem, the indistinguishability theorem does not depend on the particular group G .

7.4 Lower bound results without entanglement

As in Chapter 6, we may combine the indistinguishability and support theorems into a recipe for proving quantum lower bounds. We use a combinatorial lemma to link lower bounds on $\mathbf{max-orbit}(C_n)$ to lower bounds on size; the lemma is stated more generally than needed in anticipation of the results in Chapter 8.

Lemma 7.16. *Let $G \leq \text{Sym}_n$. Let (C_n) be a family of rigid Γ_G -permutation symmetric output quantum τ -circuits over $\mathbb{G}_{\text{CNOT}}^Q$. For every function $f : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ with $f(n) = \omega(\log n)$, if $s(C_n) = 2^{o(f(n))}$, then $\mathbf{max-orbit}(C_n) = 2^{o(f(n))}$.*

Proof. We prove the contrapositive: suppose $\mathbf{max-orbit}(C_n)$ is not $2^{o(f(n))}$. That is, there is some $c > 0$ such that $\mathbf{max-orbit}(C_n) > 2^{c \cdot f(n)}$ for infinitely many n . Suppose each C_n has wires $W_n = X_n \sqcup A_n$. Clearly $|W_n| \geq \mathbf{max-orbit}(C_n)$, so $|W_n| > 2^{c \cdot f(n)}$ for infinitely many n .

Now $|W_n| = |X_n| + |A_n|$, and since X_n is the set of input wires encoding a τ -structure of size n , $|X_n|$ is polynomial in n : say $|X_n| = p(n)$ for some polynomial p . Then $a(C_n) = |A_n| = |W_n| - p(n) > 2^{c \cdot f(n)} - p(n)$ for infinitely many n . Now since $f(n) = \omega(\log n)$, $2^{c \cdot f(n)} = n^{\omega(1)}$ dominates $p(n)$. It follows that $2^{c \cdot f(n)} - p(n) = \Omega(2^{c \cdot f(n)})$ and so $2^{c \cdot f(n)} - p(n) = 2^{\Omega(f(n))}$ (Lemma A.3), so there is some $d > 0$ such that $2^{c \cdot f(n)} - p(n) \geq 2^{d \cdot f(n)}$ for large enough n . Hence $a(C_n) > 2^{d \cdot f(n)}$ for infinitely many n , so $a(C_n)$ cannot be $2^{o(f(n))}$.

We now prove that $s(C_n)$ also is not $2^{o(f(n))}$. Say that a wire in a circuit is *empty* if no gate acts nontrivially on it. In a rigid circuit, no more than one ancilla wire may be empty, because if $a_1, a_2 \in A_n$ are distinct empty ancillas and $U_\pi \in \Gamma_{\text{Sym}_{W_n}}$ is an automorphism of C_n induced by $U_\sigma \in \Gamma_G$, then $U_{\pi(a_1 a_2)}$ is another automorphism induced by U_σ , contradicting rigidity. So at most one ancilla wire in each C_n is empty. Over $\mathbb{G}_{\text{CNOT}}^Q$, each gate acts nontrivially on at most 2 wires, so $s(C_n) \geq \frac{a(C_n)-1}{2}$ and so $s(C_n)$ also cannot be $2^{o(f(n))}$. \square

The above proof easily generalizes to any gate set whose gates act nontrivially on a bounded number of wires. Note that because we have defined $\mathbf{max-orbit}(C_n)$ in terms of orbits of wires,

the above proof additionally obtains a lower bound on the number of ancilla wires $a(C_n)$ from which the lower bound on size is derived.

Theorem 7.17. *Let $G = \text{Alt}_n$. Suppose that (\mathcal{A}_n) and (\mathcal{B}_n) are families of τ -structures such that for infinitely many n , Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ -1-PT quantum pebble game on $|\mathcal{A}_n\rangle$ and $|\mathcal{B}_n\rangle$ for $k = \Omega(n)$. Let \mathcal{P} be any τ -property separating (\mathcal{A}_n) and (\mathcal{B}_n) . Then there is no family of rigid Γ_G -permutation symmetric output quantum τ -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ with $\eta(C_n) = 1$ computing \mathcal{P} which has size $2^{o(n)}$.*

Proof. Like Theorem 6.10. Let (C_n) be such a family of quantum circuits computing \mathcal{P} . Since $\eta(C_n) = 1$, each C_n is reconstructible, and by Lemma 7.12, C_n has partition symmetry. By Lemma 3.8, Alt_n has distinct stabilizers for every $n \geq 4$. Hence by Theorem 7.14, for each $n \geq 4$, if $\mathbf{max-supp}(C_n) \leq k/2$ and Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ -1-PT quantum pebble game on $|\mathcal{A}_n\rangle$ and $|\mathcal{B}_n\rangle$, then $C_n[|\mathcal{A}_n\rangle] = C_n[|\mathcal{B}_n\rangle]$, contradicting the assumption that (C_n) computes \mathcal{P} . Therefore we must have $\mathbf{max-supp}(C_n) > k/2$ for infinitely many n , so $\mathbf{max-supp}(C_n)$ is not $o(k)$ and so it is not $o(n)$. Then by the support theorem for Alt_n (Theorem 7.4), $\mathbf{max-orbit}(C_n)$ is not $2^{o(n)}$, and so by Lemma 7.16, $s(C_n)$ is not $2^{o(n)}$. \square

In particular, we obtain a concrete lower bound for the Alt-CFI property (Section 2.5.1).

Theorem 7.18. *There is no family of rigid Γ_{Alt_n} -permutation symmetric output quantum τ_{graph} -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ with $\eta(C_n) = 1$ computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ which has size $2^{o(n)}$.*

Proof. Let $G = \text{Alt}_n$. Let (G_n) and (H_n) be the families of Alt-CFI graphs of Corollary 2.28. By Proposition 4.14, Duplicator wins the full $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game on G_n and H_n for some $k = \Omega(n)$, so it also wins the $(\Gamma_G, \mathcal{P}_G, k)$ -1-PT quantum pebble game. The result follows from Theorem 7.17. \square

I again emphasize that this result is limited in that it applies only to *rigid* quantum circuits. As explained in Section 5.4, in the absence of a quantum-circuit analogue of Lemma 5.7 allowing us to efficiently transform symmetric quantum circuits into equivalent rigid such circuits, Theorem 7.18 does not establish a lower bound for all circuits.

The results in this chapter are generalized in Chapter 8, and so we postpone further discussion until Section 8.6.

Chapter 8

General quantum lower bounds

This chapter further generalizes Dawar and Wilsenach’s technique [DW22] to quantum circuits which use entanglement, proving novel lower bounds which are parametrized by the entanglement width of the circuits. Except where noted, this chapter contains entirely original material.

We now generalize the results of Chapter 7 to quantum circuits with entanglement width bounded by an arbitrary function. We apply essentially the same technique abstractly to tuples of distinct wires. We adopt the same notational conventions as Chapter 7. Fix a set of wires W and $\ell \in \mathbb{Z}_{\geq 1}$ and assume $|W| \geq \ell$, and define

$$W_D^\ell = \{(w_1, \dots, w_\ell) \in W^\ell : w_1, \dots, w_\ell \text{ are all distinct}\}. \quad (8.1)$$

Any group G acting on W —in particular, Sym_W —then also acts on W_D^ℓ elementwise.

8.1 Directional partial trace

We define a “directional partial trace” of a density matrix $\rho \in D(\mathcal{H}_W)$ with respect to a tuple $\vec{w} \in W_D^\ell$ which essentially traces out the qubits not in \vec{w} and arranges the remaining qubits in the order specified by \vec{w} . For this to make sense, fix some total order \leq on W and view $\mathcal{H}_W = (\mathbb{C}^2)^{\otimes W}$. For each $S \subseteq W$ with $|S| = \ell$, we view $\text{Tr}_{\bar{S}}$ as a function $D(\mathcal{H}_W) \rightarrow D((\mathbb{C}^2)^{\otimes \ell})$, where for each $\rho \in D(\mathcal{H}_W)$, the qubits of $\text{Tr}_{\bar{S}}(\rho)$ are indexed $1, \dots, \ell$ and correspond to the qubits of ρ indexed by the wires S arranged in ascending order according to \leq .

Definition 8.1. Fix a total order on W . Let $\vec{w} = (w_1, \dots, w_\ell) \in W_D^\ell$ and $\rho \in \mathcal{H}_W$. Let $\sigma \in \text{Sym}_\ell$ be the unique permutation such that $(w_{\sigma(1)}, \dots, w_{\sigma(\ell)})$ is in ascending order. Let $S = \{w_1, \dots, w_\ell\}$. The *directional partial trace* of ρ with respect to \vec{w} is

$$\text{DTr}_{\vec{w}}(\rho) := U_\sigma \text{Tr}_{\bar{S}}(\rho) U_\sigma^\dagger. \quad (8.2)$$

The i th qubit of $\text{DTr}_{\vec{w}}(\rho)$ corresponds to the w_i qubit of ρ , and in particular does not depend on the total order chosen. Observe that if $\pi \in \text{Sym}_W$ acts on W_D^ℓ elementwise, we have

$$\text{DTr}_{\pi(\vec{w})}(\rho) = \text{DTr}_{\vec{w}}(U_\pi^\dagger \rho U_\pi). \quad (8.3)$$

We then redefine the part function of Section 7.2.

Definition 8.2. For every density matrix $\rho \in D(\mathcal{H}_W)$, define the ℓ -part function

$$\begin{aligned} f_\rho : W_D^\ell &\rightarrow D((\mathbb{C}^2)^{\otimes \ell}) \\ \vec{w} &\mapsto D\text{Tr}_{\vec{w}}(\rho). \end{aligned} \tag{8.4}$$

For each $S \subseteq W_D^\ell$, let $f_\rho^S : S \rightarrow D((\mathbb{C}^2)^{\otimes \ell})$ be the restriction of f_ρ to the domain S .

Lemma 8.3. For all $\rho \in D(\mathcal{H}_W)$, $S \subseteq W_D^\ell$, and $\sigma \in \text{SetStab}_{\text{Sym}_{W_D^\ell}}(S)$, we have $f_{U_\sigma^\dagger \rho U_\sigma}^S = f_\rho^S \circ \sigma'$, where $\sigma' \in \text{Sym}_S$ is such that $\sigma'(\vec{w}) = \sigma(\vec{w})$ for all $\vec{w} \in S$.

Proof. For all $\vec{w} \in S$, by equation (8.3), $f_{U_\sigma^\dagger \rho U_\sigma}^S(\vec{w}) = D\text{Tr}_{\vec{w}}(U_\sigma^\dagger \rho U_\sigma) = D\text{Tr}_{\sigma(\vec{w})}(\rho) = D\text{Tr}_{\sigma'(\vec{w})}(\rho) = (f_\rho^S \circ \sigma')(\vec{w})$. \square

8.2 ℓ -partition symmetry and support

We now define generalizations of the notions of partition symmetry and support from Chapter 7. As an abuse of notation, if K is a group acting on a set S and $H \leq \text{Sym}_S$, we write $K \leq H$ to mean that if $\varphi : K \rightarrow \text{Sym}_S$ is the homomorphism induced by the action of K on S , then $\varphi(K) \leq H$.

Definition 8.4. A unitary $L \in U(\mathcal{H}_W)$ has ℓ -partition symmetry with respect to a pebble set \mathcal{P} and some $\Delta \subseteq D(\mathcal{H}_W)$ if for every $P \subseteq \mathcal{P}$ and every $S \subseteq W_P$ with $1 \leq |S| \leq \ell$, there exists a partition $(T_i)_i$ of W_D^ℓ such that $\bigcap P \leq \prod_i \text{Sym}_{T_i}$ (where we consider $\bigcap P$ to act elementwise on W_D^ℓ) and for every $\rho_1, \rho_2 \in \Delta$, if there is some $\sigma \in \prod_i \text{Sym}_{T_i}$ such that $f_{\rho_1} \circ \sigma = f_{\rho_2}$, then $\text{Tr}_{\bar{S}}(L\rho_1 L^\dagger) = \text{Tr}_{\bar{S}}(L\rho_2 L^\dagger)$.

Again, $\prod_i \text{Sym}_{T_i}$ denotes the subgroup of $\text{Sym}_{W_D^\ell}$ consisting of all permutations $\sigma \in \text{Sym}_{W_D^\ell}$ which map elements of each set T_i only to other elements of T_i .

Definition 8.5. Let $G \leq \text{Sym}_n$. A rigid Γ_G -permutation symmetric output quantum τ -circuit C with m layers has ℓ -partition symmetry with respect to a pebble set \mathcal{P} if for every $i \in [m]$, the unitary L_i representing layer i has ℓ -partition symmetry with respect to \mathcal{P} and $\Delta_{i-1}(C)$.

The following theorem links entanglement width to ℓ -partition symmetry:

Theorem 8.6. Let $G \leq \text{Sym}_n$ with distinct stabilizers. Every rigid Γ_G -permutation symmetric output quantum circuit C over $\mathbb{G}_{\text{CNOT}}^Q$ has $\eta(C)$ -partition symmetry with respect to \mathcal{P}_G .

I delay the proof to Section 8.4 as it is quite involved.

We extend the notion of support to ℓ -size sets of wires. Fix a Γ_G -permutation symmetric output quantum circuit C on wires W . We say a set of pebbles $P \subseteq \mathcal{P}_G$ supports a set $S \subseteq W$ if $S \subseteq W_P$. Let **min-supp**(S) be the size of the smallest set of pebbles $P \subseteq \mathcal{P}_G$ which supports S and let **max-supp** $_\ell(C) = \max_{S \subseteq W, |S|=\ell} \text{min-supp}(S)$. Observe that if $sp(w) \subseteq \mathcal{P}_G$ supports the wire w for each $w \in S$, then $\bigcup_{w \in S} sp(w)$ supports S ; hence **min-supp**(S) $\leq \sum_{w \in S} \text{min-supp}(w)$ and so

$$\text{max-supp}_\ell(C) \leq \ell \cdot \text{max-supp}(C). \tag{8.5}$$

By abuse of notation, we also say $P \subseteq \mathcal{P}_G$ supports a tuple $\vec{w} = (w_1, \dots, w_\ell) \in W_D^\ell$ if P supports $\{w_1, \dots, w_\ell\}$.

8.3 A general quantum indistinguishability theorem

We now prove a generalized version of the product state indistinguishability theorem (Theorem 7.14). The proof is very similar to that given in Section 7.3.

Lemma 8.7. *Suppose $P \subseteq \mathcal{P}_G$ supports $S \subseteq W$ and $\sigma \in G$. Then $\sigma P \sigma^{-1} := \{\sigma \Gamma_p \sigma^{-1} : p \in P\}$ supports $\sigma S = \{\sigma w : w \in S\}$.*

Proof. As in Lemma 7.13. Again, $\bigcap(\sigma P \sigma^{-1}) = \{\sigma \pi \sigma^{-1} : \pi \in \bigcap P\}$. P supports S , so $\bigcap P \leq \text{Stab}_G(S)$. Let $\pi \in \bigcap P$: then $\pi w = w$ for each $w \in S$, so $(\sigma \pi \sigma^{-1})(\sigma w) = \sigma w$ for each $\sigma w \in \sigma S$. Hence $\bigcap(\sigma P \sigma^{-1}) \leq \text{Stab}_G(\sigma S)$ and so $\sigma P \sigma^{-1}$ supports σS . \square

Therefore, to each $S \subseteq W$ with $|S| = \ell$ we assign a support $sp(S) \subseteq \mathcal{P}_G$ such that $sp(\sigma S) = \sigma sp(S) \sigma^{-1}$ for each $\sigma \in G$. As before, if $\mathbf{max-supp}_\ell(C) \leq k$, we may assume $|sp(S)| \leq k$. If $\vec{w} = (w_1, \dots, w_\ell) \in W_D^\ell$, we also write $sp(\vec{w}) = sp(\{w_1, \dots, w_\ell\})$.

Theorem 8.8 (General quantum indistinguishability theorem). *Let $\ell \in \mathbb{Z}_{\geq 1}$ and let $G \leq \text{Sym}_n$ with distinct stabilizers. Let C be a rigid Γ_G -permutation symmetric output quantum τ -circuit of order n with at least ℓ wires which has ℓ -partition symmetry with respect to \mathcal{P}_G and has $\mathbf{max-supp}_\ell(C) \leq k$. Let $\mathcal{A}, \mathcal{B} \in \text{fin}_n[\tau]$. If Duplicator wins the $(\Gamma_G, \mathcal{P}_G, 2k)$ - ℓ -PT quantum pebble game on $|\mathcal{A}\rangle$ and $|\mathcal{B}\rangle$, then $C[|\mathcal{A}\rangle] = C[|\mathcal{B}\rangle]$.*

Proof. Suppose C has wires $W = X \sqcup A$; we assume $|W| \geq \ell$. We again prove the contrapositive. Suppose $C[|\mathcal{A}\rangle] \neq C[|\mathcal{B}\rangle]$: We give a Spoiler strategy. Again, let the layers of C be represented by unitaries L_1, \dots, L_m , let $L_{\leq i} = L_i L_{i-1} \dots L_1$, and let $\rho_i^{\mathcal{A}} = L_{\leq i}(|\mathcal{A}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{A}| \langle 0|^{\otimes a(C)})L_{\leq i}^\dagger$ and $\rho_i^{\mathcal{B}} = L_{\leq i}(|\mathcal{B}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{B}| \langle 0|^{\otimes a(C)})L_{\leq i}^\dagger$ for each $0 \leq i \leq m$.

For each i from m to 0, Spoiler plays to maintain the invariant that there is a set of wires $S_i \subseteq W$ with $|S_i| \leq \ell$ supported by the current set of pebbles P such that for the current unitary $U \in \Gamma_G$ we have $\text{Tr}_{\overline{S_i}}(\rho_i^{\mathcal{A}}) \neq \text{Tr}_{\overline{S_i}}(U^\dagger \rho_i^{\mathcal{B}} U)$. (Again, recall that we do not distinguish between $U \in \Gamma_G$ and the unique automorphism of C in Γ_{Sym_W} induced by U .) Then again, for $i = 0$, we have $\text{Tr}_{\overline{S_0}}(\rho_0^{\mathcal{A}}) \neq \text{Tr}_{\overline{S_0}}(U^\dagger \rho_0^{\mathcal{B}} U)$ where $\rho_0^{\mathcal{A}} = (|\mathcal{A}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{A}| \langle 0|^{\otimes a(C)})$ and $\rho_0^{\mathcal{B}} = (|\mathcal{B}\rangle|0\rangle^{\otimes a(C)})(\langle \mathcal{B}| \langle 0|^{\otimes a(C)})$. Since the automorphism U permutes X and A separately, if $S_0 \subseteq A$, then $\text{Tr}_{\overline{S_0}}(\rho_0^{\mathcal{A}}) = \text{Tr}_{\overline{S_0}}(U^\dagger \rho_0^{\mathcal{B}} U) = (|0\rangle \langle 0|)^{\otimes |S_0|}$; but this is not the case, so $S_0 \not\subseteq A$. Let $S_X = S_0 \cap X$: then $1 \leq |S_X| \leq \ell$, S_X is supported by P , and we have $\text{Tr}_{\overline{S_X}}(|\mathcal{A}\rangle \langle \mathcal{A}|) \neq \text{Tr}_{\overline{S_X}}(|\mathcal{B}\rangle \langle \mathcal{B}|)$, considering U to act only on the input wires. This is a violation of ℓ -PT partial isomorphism, so Spoiler wins.

By the same argument as in Theorem 7.14, the base case $i = m$ holds with $S_m = \{w_{\text{out}}\}$. The inductive step follows from the following claim, again observing that $\rho_{i+1}^{\mathcal{A}} = L_{i+1} \rho_i^{\mathcal{A}} L_{i+1}^\dagger$ and $\rho_{i+1}^{\mathcal{B}} = L_{i+1} \rho_i^{\mathcal{B}} L_{i+1}^\dagger$.

Claim 8.9. Suppose we are at layer $0 \leq i < m$, and let $L = L_{i+1}$, $\rho_A = \rho_i^A$, and $\rho_B = \rho_i^B$. Suppose we are in a position where the pebbles include $P \subseteq \mathcal{P}_G$ with $|P| \leq k$ and the unitary is $U \in \Gamma_G$, and we have some $S = S_{i+1} \subseteq W$ with $|S| \leq \ell$ supported by P such that

$$\mathrm{Tr}_{\bar{S}}(L\rho_A L^\dagger) \neq \mathrm{Tr}_{\bar{S}}(U^\dagger L\rho_B L^\dagger U). \quad (8.6)$$

There is a strategy for Spoiler such that after at most k rounds, we are in a position where the pebbles include $P' \subseteq \mathcal{P}_G$ with $|P'| \leq k$ and the unitary is $U' \in \Gamma_G$, and we have some $S' \subseteq W$ with $|S'| \leq \ell$ supported by P' such that

$$\mathrm{Tr}_{\bar{S}'}(\rho_A) \neq \mathrm{Tr}_{\bar{S}'}(U'^\dagger \rho_B U'). \quad (8.7)$$

Proof. Since C has ℓ -partition symmetry, there is a partition $(T_i)_i$ of W_D^ℓ such that $\bigcap P \leq \prod_i \mathrm{Sym}_{T_i}$ and for every $\rho_1, \rho_2 \in \Delta_i(C)$, if $f_{\rho_1} \circ \sigma = f_{\rho_2}$ for some $\sigma \in \prod_i \mathrm{Sym}_{T_i}$, then $\mathrm{Tr}_{\bar{S}}(L\rho_1 L^\dagger) = \mathrm{Tr}_{\bar{S}}(L\rho_2 L^\dagger)$. Now L commutes with U (and so U^\dagger) since $U \in \Gamma_G$ is an automorphism of C , so (8.6) says $\mathrm{Tr}_{\bar{S}}(L\rho_A L^\dagger) \neq \mathrm{Tr}_{\bar{S}}(LU^\dagger \rho_B UL^\dagger)$. Additionally, $\rho_A, U^\dagger \rho_B U \in \Delta_i(C)$ by definition (since $\Delta_i(C)$ is closed under conjugation by elements of Γ_G), so

$$f_{\rho_A} \circ \sigma \neq f_{U^\dagger \rho_B U} \quad (8.8)$$

for all $\sigma \in \prod_i \mathrm{Sym}_{T_i}$. The domain of these functions is W_D^ℓ , and the orbits of W_D^ℓ under $\bigcap P$ partition W_D^ℓ : let $(O_i)_i$ be those orbits. Since $\bigcap P \leq \prod_i \mathrm{Sym}_{T_i}$, the orbits of W_D^ℓ under $\bigcap P$ form a refinement of those under $\prod_i \mathrm{Sym}_{T_i}$ (which are just $(T_i)_i$), so $\prod_i \mathrm{Sym}_{O_i} \leq \prod_i \mathrm{Sym}_{T_i}$. Hence there is some orbit O' under $\bigcap P$ such that

$$f_{\rho_A}^{O'} \circ \sigma \neq f_{U^\dagger \rho_B U}^{O'} \quad (8.9)$$

for all $\sigma \in \mathrm{Sym}_{O'} \leq \prod_i \mathrm{Sym}_{O_i}$.

We now place pebbles. Suppose that in the j th round, the pebbles include $P_j = P \cup \{\Gamma_{p_1}, \dots, \Gamma_{p_j}\}$ and the current unitary is U_j . I claim that Spoiler can play to maintain the following invariant: there is some $\vec{w}_j \in W_D^\ell$ such that $\Gamma_{p_1}, \dots, \Gamma_{p_j} \in sp(\vec{w}_j)$ and for its orbit $O'_j = \mathrm{Orb}_{\bigcap P_j}(\vec{w}_j)$ under $\bigcap P_j$ we have

$$f_{\rho_A}^{O'_j} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{O'_j} \quad (8.10)$$

for all $\sigma \in \mathrm{Sym}_{O'_j}$. Then since $|sp(\vec{w}_j)| \leq k$, after at most k rounds, we have $O'_j = \{\vec{w}_j\}$; then if S' is the set containing the elements of \vec{w}_j , the invariant gives us $\mathrm{Tr}_{\bar{S}'}(\rho_A) \neq \mathrm{Tr}_{\bar{S}'}(U_j^\dagger \rho_B U_j)$ with $\{\Gamma_{p_1}, \dots, \Gamma_{p_j}\}$ supporting S' , which proves the claim.

The case $j = 0$ is given above: take $O'_0 = O$, $U_0 = U$, $P_0 = P$, and choose $\vec{w}_0 \in O'_0$ arbitrarily. In round $j \geq 1$, Spoiler first picks up some pebble not in the support of S or \vec{w}_{j-1} if necessary. From the invariant, we have

$$f_{\rho_A}^{O'_{j-1}} \circ \sigma \neq f_{U_{j-1}^\dagger \rho_B U_{j-1}}^{O'_{j-1}} \quad (8.11)$$

for all $\sigma \in \text{Sym}_{O'_{j-1}}$. Duplicator chooses $U_\pi \in \bigcap P_{j-1}$ and sets $U_j := U_{j-1}U_\pi$. By the same argument as in the proof of Claim 7.15 (invoking Lemma 8.3),

$$f_{\rho_A}^{O'_{j-1}} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{O'_{j-1}} \quad (8.12)$$

for all $\sigma \in \text{Sym}_{O'_{j-1}}$. Next, we show how Spoiler makes progress. Let Γ_p be some pebble in $sp(\vec{w}_{j-1})$ which is not yet in P_{j-1} . As in Claim 7.15, for each pebble Γ_q conjugate to Γ_p by some $\pi \in \bigcap P_{j-1}$ (considered as a subgroup of G), let

$$W_j := \{\pi \vec{w}_{j-1} : \pi \in \bigcap P_{j-1}, \pi \Gamma_p \pi^{-1} = \Gamma_q\}. \quad (8.13)$$

I make the same claims about $(W_q)_q$ as in Claim 7.15:

- (i) Every $\vec{v} \in O'_{j-1}$ appears in the same number of sets W_q .
- (ii) There is some Γ_q such that $f_{\rho_A}^{W_q} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{W_q}$ for all $\sigma \in \text{Sym}_{W_q}$.
- (iii) For every Γ_q , we have $W_q = \text{Orb}_{\Gamma_q \cap \bigcap P_{j-1}}(\vec{v})$ for all $\vec{v} \in W_q$.

The proofs of these claims are identical to those in Claim 7.15. Thus by claim (ii), Spoiler places some pebble Γ_q such that $f_{\rho_A}^{W_q} \circ \sigma \neq f_{U_j^\dagger \rho_B U_j}^{W_q}$ for all $\sigma \in W_q$; let $P_j = P_{j-1} \cup \{\Gamma_q\}$. Choose $\vec{w}_j \in W_q$ arbitrarily: by the same argument as in Claim 7.15, $\Gamma_{p_1}, \dots, \Gamma_{p_{j-1}}, \Gamma_q \in sp(\vec{w}_j)$. By claim (iii), $W_q = \text{Orb}_{\bigcap P_j}(\vec{w}_j)$, so let $O'_j = W_q$. This preserves the invariant. \square

As before, repeatedly applying Claim 8.9 gives a winning Spoiler strategy taking at most km rounds. \square

8.4 CNOT circuits have $\eta(C)$ -partition symmetry

We now prove Theorem 8.6:

Theorem 8.6. *Let $G \leq \text{Sym}_n$ with distinct stabilizers. Every rigid Γ_G -permutation symmetric output quantum circuit C over $\mathbb{G}_{\text{CNOT}}^Q$ has $\eta(C)$ -partition symmetry with respect to \mathcal{P}_G .*

Proof. Let $\eta = \eta(C)$. Suppose C has wires W , and observe that $\eta \leq |W|$. Let $P \subseteq \mathcal{P}_G$ and $S \subseteq W_P$ with $|S| \leq \eta$. As in Lemma 7.12, assume without loss of generality that each layer \mathcal{L} in C consists of exactly one orbit of gates under conjugation by Γ_G . Let L be the unitary representing some layer \mathcal{L} .

First suppose \mathcal{L} applies some 1-qubit unitary U to the wires $W_{\mathcal{L}} \subseteq W$. Define an equivalence relation \approx on the wires W as follows: Let $w_1, w_2 \in W$. If $w_1 \in S$ or $w_2 \in S$, then $w_1 \approx w_2$ iff $w_1 = w_2$. Otherwise, $w_1, w_2 \notin S$; let $w_1 \approx w_2$ iff w_1 and w_2 agree on membership in $W_{\mathcal{L}}$. Lift \approx to an equivalence relation on W_D^c for every $c \leq |W|$ elementwise: for every $\vec{w}_1 = (w_1^{(1)}, \dots, w_c^{(1)}), \vec{w}_2 = (w_1^{(2)}, \dots, w_c^{(2)}) \in W_D^c$, let

$$\vec{w}_1 \approx \vec{w}_2 \quad \text{iff} \quad w_i^{(1)} \approx w_i^{(2)} \text{ for all } i \in [c]. \quad (8.14)$$

Let $(T_i)_i$ be the equivalence classes of W_D^η under \approx . By construction, every automorphism π of \mathcal{L} which pointwise stabilizes S maps each $w \in W$ to some $\pi w \approx w$, so $\bigcap P \leq \prod_i \text{Sym}_{T_i}$.

Furthermore, let $\vec{w} \in W_D^\eta$ be some η -tuple of wires whose first $|S|$ elements list the wires in S in some order. Since every $w \in S$ is the sole member of its equivalence class under \approx , for every $\sigma \in \prod_i \text{Sym}_{T_i}$, $\sigma \vec{w}$ also begins with the elements of S in the same order. So if $\rho_1, \rho_2 \in D(\mathcal{H}_W)$ have $f_{\rho_1} \circ \sigma = f_{\rho_2}$ for some $\sigma \in \prod_i \text{Sym}_{T_i}$, plugging in \vec{w} gives $D\text{Tr}_{\sigma \vec{w}}(\rho_1) = D\text{Tr}_{\vec{w}}(\rho_2)$, and tracing out all but the first $|S|$ qubits of these density matrices gives $\text{Tr}_{\bar{S}}(\rho_1) = \text{Tr}_{\bar{S}}(\rho_2)$. Since L just applies local unitaries to each qubit, we therefore have $\text{Tr}_{\bar{S}}(L\rho_1 L^\dagger) = \text{Tr}_{\bar{S}}(L\rho_2 L^\dagger)$. So L has ℓ -partition symmetry.

Next, suppose \mathcal{L} consists of CNOT gates. We define another equivalence relation \approx on W as follows. For each $w \in W \setminus S$ and each $s \in S$, let $c_s(w)$ be the number of CNOT gates in \mathcal{L} with control wire w and target wire s and $t_s(w)$ be the number of CNOT gates in \mathcal{L} with control wire s and target wire w . Then for each $w_1, w_2 \in W$, if $w_1 \in S$ or $w_2 \in S$, let $w_1 \approx w_2$ iff $w_1 = w_2$. Otherwise, $w_1, w_2 \notin S$; let $w_1 \approx w_2$ iff $c_s(w_1) = c_s(w_2)$ and $t_s(w_1) = t_s(w_2)$ for all $s \in S$. Intuitively, if $w_1 \approx w_2$, then w_1 and w_2 affect the wires S in the same way. Let $(E_i)_i$ be the equivalence classes of W under \approx .

Lift \approx to an equivalence relation on W_D^c for every $c \leq |W|$ elementwise in the same way as (8.14). Let $(T_i)_i$ be the equivalence classes of W_D^η under \approx . Again, by the construction of \approx , every automorphism π of \mathcal{L} which pointwise stabilizes S maps $w \in W$ to some $\pi w \approx w$, so $\bigcap P \leq \prod_i \text{Sym}_{T_i}$. Next, I make the following claim.

Claim 8.10. Suppose $|\psi\rangle, |\varphi\rangle \in \mathcal{H}_W$ with $\eta(|\psi\rangle), \eta(|\varphi\rangle) \leq \eta$. Let $\rho_1 = |\psi\rangle\langle\psi|$ and $\rho_2 = |\varphi\rangle\langle\varphi|$. If there is some $\sigma \in \prod_i \text{Sym}_{T_i} \leq \text{Sym}_{W_D^\eta}$ such that $f_{\rho_1} \circ \sigma = f_{\rho_2}$, then there is some $\pi \in \prod_i \text{Sym}_{E_i} \leq \text{Sym}_W$ such that $U_\pi \rho_1 U_\pi^\dagger = \rho_2$.

That is, I claim that if f_{ρ_1} and f_{ρ_2} are related by a suitable permutation of the *set of tuples* W_D^η , then ρ_1 and ρ_2 are related by a suitable permutation of the *wires*. This claim gives us ℓ -partition symmetry as follows. Let $\rho_1, \rho_2 \in \Delta_i(C)$: we know ρ_1 and ρ_2 are pure states with entanglement width at most η . If $f_{\rho_1} \circ \sigma = f_{\rho_2}$ for some $\sigma \in \prod_i \text{Sym}_{T_i}$, then by the claim, $U_\pi \rho_1 U_\pi^\dagger = \rho_2$ for some $\pi \in \prod_i \text{Sym}_{E_i}$. Now by the same argument as at the end of the proof of Lemma 7.12, $\text{Tr}_{\bar{S}}(LU_\pi \rho_1 U_\pi^\dagger L^\dagger) = \text{Tr}_{\bar{S}}(L\rho_1 L^\dagger)$, so $\text{Tr}_{\bar{S}}(L\rho_1 L^\dagger) = \text{Tr}_{\bar{S}}(L\rho_2 L^\dagger)$, as required.

Proof of Claim 8.10. Let $n = |W|$. Since $\eta(|\psi\rangle) \leq \eta$, let $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_r\rangle$ be a decomposition of $|\psi\rangle$ such that each $|\psi_i\rangle$ is defined over a disjoint set of wires $S_i \subseteq W$ with $|S_i| \leq \eta$ which is maximal in the sense that each $|\psi_i\rangle$ is not separable, i.e., it cannot be written as a tensor product of two or more states. The sets $(S_i)_i$ partition W . Let $|\varphi\rangle = |\varphi_1\rangle \otimes \cdots \otimes |\varphi_{r'}\rangle$ be a maximal decomposition in the same sense. We argue that a condition analogous to that of Hall's theorem holds.

Suppose that $\vec{w}_1, \dots, \vec{w}_k$ are pairwise disjoint c -tuples in W_D^c for some $c \leq \eta$ such that $\vec{w}_1 \approx \cdots \approx \vec{w}_k$ and $D\text{Tr}_{\vec{w}_1}(\rho_1) = \cdots = D\text{Tr}_{\vec{w}_k}(\rho_1) = |\chi\rangle\langle\chi|$ for some $|\chi\rangle \in (\mathbb{C}^2)^{\otimes c}$, where $|\chi\rangle$ is not separable. (Then $|\chi\rangle$ is a permutation of one of $|\psi_1\rangle, \dots, |\psi_r\rangle$.) I claim that there are at

least k pairwise disjoint c -tuples $\vec{v}_i \in W_D^c$ in the same equivalence class under \approx as $\vec{w}_1, \dots, \vec{w}_k$ such that $D\text{Tr}_{\vec{v}_i}(\rho_2) = |\chi\rangle\langle\chi|$.

We have $c \leq \eta$. Let $e \geq 1$ be the largest integer such that $ec \leq \eta$. If $e \geq k$, then $kc \leq \eta$, so there is some $\vec{w} \in W_D^\eta$ starting with $\vec{w}_1 \oplus \dots \oplus \vec{w}_k$, where \oplus denotes tuple concatenation. Then since $f_{\rho_1} \circ \sigma = f_{\rho_2}$, we have $f_{\rho_1} = f_{\rho_2} \circ \sigma^{-1}$, so $f_{\rho_1}(\vec{w}) = f_{\rho_2}(\sigma^{-1}\vec{w})$; hence $D\text{Tr}_{\vec{w}}(\rho_1) = D\text{Tr}_{\sigma^{-1}\vec{w}}(\rho_2)$ and so $\sigma^{-1}\vec{w}$ starts with $\vec{v}_1 \oplus \dots \oplus \vec{v}_k$ where $\vec{v}_1, \dots, \vec{v}_k$ are pairwise disjoint c -tuples such that $D\text{Tr}_{\vec{v}_1}(\rho_2) = \dots = D\text{Tr}_{\vec{v}_k}(\rho_2) = |\chi\rangle\langle\chi|$. Furthermore, since $\sigma \in \prod_i \text{Sym}_{T_i}$, we have $\vec{w} \approx \sigma^{-1}\vec{w}$, so by the elementwise definition of \approx , $\vec{v}_i \approx \vec{w}_i$ for all $i \in [k]$. So each \vec{v}_i is in the same equivalence class as $\vec{w}_1, \dots, \vec{w}_k$, and so at least k such tuples \vec{v}_i exist.

Otherwise, $e < k$. Let $\text{Aut}(|\chi\rangle) = \{\pi \in \text{Sym}_c : U_\pi|\chi\rangle = |\chi\rangle, (\vec{w}_1)^\pi \approx \vec{w}_1\}$ be the group of symmetries of $|\chi\rangle$ with respect to permutations of its c qubits (the *automorphisms* of $|\chi\rangle$) which preserve the equivalence class under \approx to which $\vec{w}_1, \dots, \vec{w}_k$ belong. Here $(\vec{a})^\pi$ refers to the tuple obtained by applying the permutation π to the *indices* of \vec{a} : if $\vec{a} = (w_1, \dots, w_c)$ then $(\vec{a})^\pi = (w'_1, \dots, w'_c)$ where $w'_{\pi(i)} = w_i$ for each $i \in [c]$. There are exactly

$$e! \binom{k}{e} \cdot |\text{Aut}(|\chi\rangle)|^e \cdot (\eta - ec)! \binom{n - ec}{\eta - ec} \quad (8.15)$$

η -tuples $\vec{w} \in W_D^\eta$ which start with $(\vec{w}_{i_1})^{\pi_1} \oplus \dots \oplus (\vec{w}_{i_e})^{\pi_e}$ for some distinct $\vec{w}_{i_1}, \dots, \vec{w}_{i_e} \in \{\vec{w}_1, \dots, \vec{w}_k\}$ and some automorphisms $\pi_1, \dots, \pi_k \in \text{Aut}(|\chi\rangle)$ preserving the equivalence class: there are $e! \binom{k}{e}$ ways to choose $\vec{w}_{i_1}, \dots, \vec{w}_{i_e}$ from $\vec{w}_1, \dots, \vec{w}_k$, $|\text{Aut}(|\chi\rangle)|^e$ ways to choose π_1, \dots, π_k , and $(\eta - ec)! \binom{n - ec}{\eta - ec}$ ways to choose the $\eta - ec$ other elements of \vec{w} . This formula is exact because $(e + 1)c > \eta$, so there are no tuples $\vec{w} \in W_D^\eta$ containing $e + 1$ of the c -tuples \vec{w}_i .

Since $f_{\rho_1} = f_{\rho_2} \circ \sigma^{-1}$, $\sigma^{-1} \in \prod_i \text{Sym}_{T_i}$ bijectively maps each of these η -tuples \vec{w} to a distinct $\vec{v} \in W_D^\eta$ which starts with $\vec{v}_1 \oplus \dots \oplus \vec{v}_e$, where $\vec{v}_1, \dots, \vec{v}_e \in W_D^c$ are pairwise disjoint c -tuples with $D\text{Tr}_{\vec{v}_1}(\rho_2) = \dots = D\text{Tr}_{\vec{v}_e}(\rho_2) = |\chi\rangle\langle\chi|$. As before, by the definition of \approx , each \vec{v}_i lies in the same equivalence class as $\vec{w}_1, \dots, \vec{w}_k$.

Now since $|\chi\rangle$ is a non-separable pure state, if \vec{u}_1 and \vec{u}_2 are two such c -tuples in W_D^c both in the same equivalence class as $\vec{w}_1, \dots, \vec{w}_k$ with $D\text{Tr}_{\vec{u}_1}(\rho_2) = D\text{Tr}_{\vec{u}_2}(\rho_2) = |\chi\rangle\langle\chi|$, then either \vec{u}_1 and \vec{u}_2 are disjoint or $\vec{u}_1 = (\vec{u}_2)^\pi$ for some automorphism $\pi \in \text{Aut}(|\chi\rangle)$. Indeed, suppose \vec{u}_1 and \vec{u}_2 are not disjoint, and let S' be the set of wires in both \vec{u}_1 and \vec{u}_2 . If S' does not contain all the wires in \vec{u}_1 and \vec{u}_2 (i.e., \vec{u}_1 and \vec{u}_2 do not fully overlap), then since $D\text{Tr}_{\vec{u}_1}(\rho_2)$ and $D\text{Tr}_{\vec{u}_2}(\rho_2)$ are pure states, by Lemma A.6, $\text{Tr}_{\overline{S'}}(\rho_2)$ is a pure state, which (by Lemmas A.4 and A.5) violates the non-separability of $|\chi\rangle$. Hence \vec{u}_1 and \vec{u}_2 fully overlap, so since $D\text{Tr}_{\vec{u}_1}(\rho_2) = D\text{Tr}_{\vec{u}_2}(\rho_2) = |\chi\rangle\langle\chi|$ and $\vec{u}_1 \approx \vec{u}_2 \approx \vec{w}_1$, we must have $\vec{u}_1 = (\vec{u}_2)^\pi$ for some $\pi \in \text{Aut}(|\chi\rangle)$.

Hence each pair of the c -tuples \vec{v}_i are either disjoint or are related by an automorphism. Thus, if there are only at most $k - 1$ disjoint c -tuples $\vec{v}_i \in W_D^c$ such that $D\text{Tr}_{\vec{v}_i}(\rho_2) = |\chi\rangle\langle\chi|$, then by the same calculation as above, there are only at most

$$e! \binom{k - 1}{e} \cdot |\text{Aut}(|\chi\rangle)|^e \cdot (\eta - ec)! \binom{n - ec}{\eta - ec} \quad (8.16)$$

possible η -tuples \vec{v} as defined above. Since the \vec{v} are mapped bijectively by σ to the η -tuples \vec{w} , whose count is given by (8.15), this is not enough! So there are at least k such disjoint c -tuples \vec{v}_i in the same equivalence class as $\vec{w}_1, \dots, \vec{w}_k$.

By symmetry, it also holds that if $\vec{v}_1, \dots, \vec{v}_k$ is a set of disjoint c -tuples in W_D^c for some $c \leq \eta$ such that $\vec{v}_1 \approx \dots \approx \vec{v}_k$ and $\mathrm{DTr}_{\vec{v}_1}(\rho_2) = \dots = \mathrm{DTr}_{\vec{v}_k}(\rho_2) = |\chi\rangle\langle\chi|$ for some non-separable pure state $|\chi\rangle$ (i.e., a permutation of one of $|\varphi_1\rangle, \dots, |\varphi_{r'}\rangle$), then there are at least k disjoint c -tuples $\vec{w}_i \in W_D^c$ in the same equivalence class under \approx as $\vec{v}_1, \dots, \vec{v}_k$ such that $\mathrm{DTr}_{\vec{w}_i}(\rho_1) = |\chi\rangle\langle\chi|$.

Therefore there is a bijection $g : [r] \rightarrow [r']$ (and so $r = r'$) between the components $(|\psi_i\rangle)_i$ of $|\psi\rangle$ and $(|\varphi_i\rangle)_i$ of $|\varphi\rangle$ with the following property: For every $i \in [r]$, let \vec{w}_i be an ordering of S_i , the set of wires underlying $|\psi_i\rangle$. There is an ordering $\vec{v}_{g(i)}$ of the set of wires underlying $|\varphi_{g(i)}\rangle$ such that:

- (a) The states $|\psi_i\rangle$ and $|\varphi_{g(i)}\rangle$ are equal up to a reordering of the wires of $|\psi_i\rangle$ to \vec{w}_i and of $|\varphi_{g(i)}\rangle$ to $\vec{v}_{g(i)}$: i.e., $\mathrm{DTr}_{\vec{w}_i}(\rho_1) = \mathrm{DTr}_{\vec{v}_{g(i)}}(\rho_2)$; and
- (b) $\vec{w}_i \approx \vec{v}_{g(i)}$.

Let $\vec{w} = \vec{w}_1 \oplus \dots \oplus \vec{w}_r$ and $\vec{v} = \vec{v}_{g(1)} \oplus \dots \oplus \vec{v}_{g(r)}$. Since g is a bijection, both $\{\vec{w}_1, \dots, \vec{w}_r\}$ and $\{\vec{v}_{g(1)}, \dots, \vec{v}_{g(r)}\}$ partition the set of wires W , so both \vec{w} and \vec{v} are orderings of all of W . Hence $\vec{v} = \pi\vec{w}$ for some $\pi \in \mathrm{Sym}_W$. Furthermore, by property (b), $\vec{w} \approx \vec{v}$. Let $\vec{w} = (w_1, \dots, w_n)$ and $\vec{v} = (v_1, \dots, v_n)$: we have $v_j = \pi w_j$ and $v_j \approx w_j$ for each $j \in [n]$, so since w_1, \dots, w_n and v_1, \dots, v_n enumerate W , π maps members of each equivalence class of W under \approx only to members of the same equivalence class. Hence in fact $\pi \in \prod_i \mathrm{Sym}_{E_i}$. Finally, by property (a),

$$\mathrm{DTr}_{\vec{w}}(\rho_1) = \mathrm{DTr}_{\vec{v}}(\rho_2) = \mathrm{DTr}_{\pi\vec{w}}(\rho_2) = \mathrm{DTr}_{\vec{w}}(U_\pi^\dagger \rho_2 U_\pi) \quad (8.17)$$

where the last equality is from (8.3). Hence $\rho_1 = U_\pi^\dagger \rho_2 U_\pi$. \square

8.5 Quantum lower bound results

Like in Section 7.4, our efforts culminate in a recipe for proving quantum lower bounds. For a more general result, we prove a generalization of the quantum support theorem for Alt_n (Theorem 7.4).

Theorem 8.11 (Generalized quantum support theorem for Alt_n). *Let (C_n) be a family of rigid Γ_{Alt_n} -permutation symmetric output quantum τ -circuits. Let $f : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ with $f(n) = \omega(1)$ such that $f(n) \leq n$ for sufficiently large n . If $\mathbf{max-orbit}(C_n) = 2^{o(f(n))}$ then $\mathbf{max-supp}(C_n) = o(f(n))$.*

Proof. We again follow Theorem 6.3, originally due to [DW22]. Let k be the smallest positive integer with $\mathbf{max-orbit}(C_n) < \binom{f(n)}{k}$. By a simple modification of the argument of Theorem 6.3, then $k = o(f(n))$. Since $f(n) = O(n)$, we have $k = o(n)$, so for large enough n , $k \leq \frac{n}{4}$. Furthermore, $\mathbf{max-orbit}(C_n) < \binom{f(n)}{k} \leq \binom{n}{k}$ for large enough n . Then by the same argument as for Theorem 7.4, $\mathbf{max-supp}(C_n) < k = o(f(n))$. \square

Entanglement width $\eta(C_n)$	Excluded sizes $s(C_n)$
$O(1)$	$2^{o(n)}$
$O(\sqrt{n})$	$2^{o(\sqrt{n})}$
$O(n^{1-\varepsilon}), 0 < \varepsilon \leq 1$	$2^{o(n^\varepsilon)}$
$O(n/\log^c n), c > 1$	$2^{o(\log^c n)} = n^{o(\log^{c-1} n)}$
$o(n/\log n)$	$n^{O(1)}$

Table 8.1: Lower bounds on sizes of families of rigid Γ_{Alt_n} -permutation symmetric quantum circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$. The right-hand column gives values of $s(C_n)$ which are impossible for any such family of circuits with entanglement width $\eta(C_n)$ given by the left-hand column.

Theorem 8.12. *Let $G = \text{Alt}_n$. Let $f : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ with $f(n) = \omega(\log n)$ such that $f(n) \leq n$ for sufficiently large n , and let $(\ell_n)_n$ be a sequence of positive integers with $\ell_n = O(n/f(n))$. Suppose that (\mathcal{A}_n) and (\mathcal{B}_n) are families of τ -structures such that for infinitely many n , Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ - ℓ_n -PT quantum pebble game on $|\mathcal{A}_n\rangle$ and $|\mathcal{B}_n\rangle$ for $k = \Omega(n)$. Let \mathcal{P} be any τ -property separating (\mathcal{A}_n) and (\mathcal{B}_n) . Then there is no family of rigid Γ_G -permutation symmetric output quantum τ -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ with $\eta(C_n) = \ell_n$ computing \mathcal{P} which has size $2^{o(f(n))}$.*

Proof. Following Theorem 7.17. Let (C_n) be a family of such quantum circuits computing \mathcal{P} . By Theorem 8.6, each C_n has $\eta(C_n)$ -partition symmetry. By Lemma 3.8, Alt_n has distinct stabilizers for $n \geq 4$. Then by Theorem 8.8, for $n \geq 4$, if $\mathbf{max-supp}_{\eta(C_n)}(C_n) \leq k/2$ and Duplicator wins the $(\Gamma_G, \mathcal{P}_G, k)$ - $\eta(C_n)$ -PT quantum pebble game on $|\mathcal{A}_n\rangle$ and $|\mathcal{B}_n\rangle$, then $C_n[|\mathcal{A}_n\rangle] = C_n[|\mathcal{B}_n\rangle]$, contradicting the assumption that (C_n) computes \mathcal{P} . Therefore we must have $\mathbf{max-supp}_{\eta(C_n)}(C_n) > k/2$ for infinitely many n ; hence $\mathbf{max-supp}_{\eta(C_n)}(C_n)$ is not $o(k)$, so it is not $o(n)$.

By (8.5), $\mathbf{max-supp}(C_n) \geq \mathbf{max-supp}_{\eta(C_n)}(C_n)/\eta(C_n)$, so $\mathbf{max-supp}(C_n)$ is not $o(f(n))$ since $\eta(C_n) = \ell_n = O(n/f(n))$. Hence by Theorem 8.11, $\mathbf{max-orbit}(C_n)$ is not $2^{o(f(n))}$, and so by Lemma 7.16, $s(C_n)$ is not $2^{o(f(n))}$. \square

We again obtain concrete lower bounds for the Alt-CFI property.

Theorem 8.13. *Let $f : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ with $f(n) = \omega(\log n)$ such that $f(n) \leq n$ for sufficiently large n . There is no family of rigid Γ_{Alt_n} -permutation symmetric output quantum τ_{graph} -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ with $\eta(C_n) = O(n/f(n))$ computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ which has size $2^{o(f(n))}$.*

Proof. Let $G = \text{Alt}_n$. As in Theorem 7.18, by Proposition 4.14, Duplicator wins the full $(\Gamma_G, \mathcal{P}_G, k)$ -PT quantum pebble game on the pairs of Alt-CFI graphs of Corollary 2.28, so it also wins the $(\Gamma_G, \mathcal{P}_G, k)$ - ℓ -PT quantum pebble game for every $\ell \in \mathbb{Z}_{\geq 1}$. The result follows from Theorem 8.12. \square

Table 8.1 shows several concrete lower bounds on rigid Γ_{Alt_n} -permutation symmetric circuits computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ with various entanglement widths $\eta(C_n)$ obtained by substituting various functions f . In particular, by taking $f(n) = \lfloor n^\varepsilon \rfloor$, where $\lfloor \cdot \rfloor$ denotes the floor function, we obtain:

Corollary 8.14. *Let $0 < \varepsilon \leq 1$. There is no family of rigid Γ_{Alt_n} -permutation symmetric output quantum τ_{graph} -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ with entanglement width $\eta(C_n) = O(n^{1-\varepsilon})$ computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ which has size $2^{o(n^\varepsilon)}$.*

Finally, the following corollary may informally be obtained by substituting $f(n) = \omega(\log n)$ into Theorem 8.13. We give a rigorous proof below.

Corollary 8.15. *There is no polynomial-size family of rigid Γ_{Alt_n} -permutation symmetric output quantum τ_{graph} -circuits (C_n) over $\mathbb{G}_{\text{CNOT}}^Q$ computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ with entanglement width $\eta(C_n) = o(n/\log n)$.*

Proof. Suppose that (C_n) is such a family of circuits with $\eta(C_n) = o(n/\log n)$. Let $f(n) = \lfloor n/\eta(C_n) \rfloor$: we have $f(n) = \omega(\log n)$ and, since entanglement width is always at least 1, $f(n) \leq n$ for all n . We have $\eta(C_n) = O(n/f(n))$, so by Theorem 8.13, (C_n) does not have size $2^{o(f(n))}$. But since $f(n) = \omega(\log n)$, every polynomial is $n^{O(1)} = 2^{O(\log n)} = 2^{o(f(n))}$, so (C_n) cannot have polynomial size. \square

These corollaries constitute the primary results of this thesis.

8.6 Discussion

Corollary 8.15 states that there is no polynomial-size family of rigid Γ_{Alt_n} -permutation symmetric CNOT quantum circuits computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ using $o(n/\log n)$ -partite entanglement. Furthermore, by Corollary 8.14, there is no such family using $O(n^{1-\varepsilon})$ -partite entanglement with subexponential size $2^{o(n^\varepsilon)}$. This is remarkable because by Corollary 2.28, $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ can be classically computed in polynomial time! Hence, efficiently computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$ with rigid CNOT circuits requires either breaking Alt_n -symmetry or entangling many qubits together. These results complement (although do not strictly generalize) Corollary 6.12, which gives an exponential lower bound on any family of classical Alt_n -symmetric circuits computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$.

Our results also complement those of Jozsa and Linden [JL03], who show that any polynomial-size uniform family of quantum circuits over 2-qubit gates with $O(1)$ entanglement width can be efficiently classically simulated, and so unbounded entanglement width is necessary for exponential quantum speedup. Our results provide an example of a property for which, when a symmetry requirement is imposed, we can show that even $o(n/\log n)$ entanglement width does not suffice for efficient computation by rigid CNOT quantum circuits, which is a much stronger lower bound.

Note that since every rigid Γ_{Sym_n} -permutation symmetric quantum circuit is also rigid Γ_{Alt_n} -permutation symmetric, our results imply the corresponding lower bounds for families of rigid Γ_{Sym_n} -permutation symmetric quantum circuits computing $\mathcal{P}_{\text{CFI}}^{\text{Alt}}$.

I again emphasize that in their current state, our results apply only to *rigid* quantum circuits. As explained in Section 5.4, a quantum circuit analogue of Lemma 5.7, giving an efficient transformation of symmetric quantum circuits to equivalent rigid circuits, would be required to extend our results to non-rigid circuits. Since our results are sensitive to the entanglement width, we would need such a transformation to cause only a constant-factor blowup in entanglement width to preserve the strength of our results.

We have stated our results for circuits over the CNOT gate set $\mathbb{G}_{\text{CNOT}}^Q$ because we can prove the ℓ -partition symmetry property for such circuits (Theorem 8.6). This gate set is simple and universal [KLM06, Thm. 4.3.3], and so is a natural gate set to consider. Our technique can be extended to gate sets containing other 2-qubit gates with similar asymmetry properties to CNOT such that the proof of Theorem 8.6 still holds. However, the partition symmetry property does not always hold for circuits over other gate sets such as $\mathbb{G}_{\text{thr}}^Q$, and so our technique as-is does not prove lower bounds for such circuits.

Chapter 9

Conclusion and future directions

This thesis has explored quantum generalizations of pebble games and Dawar and Wilsenach’s [DW22] associated technique for proving lower bounds for symmetric circuits. In Part I, we introduced a general framework for formulating quantum pebble games which generalizes Dawar and Wilsenach’s classical (G, k) -pebble game in several directions and which can serve as a starting point for any investigation of quantum pebble games. From our framework, we then derived the partial trace-based quantum pebble game, which is easier to interpret and apply.

In Part II, we proceeded to apply the partial trace-based quantum pebble game to derive novel lower bounds for rigid symmetric quantum circuits, greatly generalizing the technique of Dawar and Wilsenach. After presenting their original technique for classical circuits, we gave successive generalizations first to the case of quantum circuits operating only on product states, then to quantum circuits with entanglement width bounded by an arbitrary function. As a result, we obtained an almost-linear lower bound on the entanglement width of any polynomial-size family of rigid CNOT circuits with Alt_n symmetry computing the Alt-CFI property—showing that any such family cannot have $o(n/\log n)$ entanglement width (Corollary 8.15)—and we gave an exponential lower bound on the size of any such family of circuits with $O(n^{1-\varepsilon})$ entanglement width (Corollary 8.14).

To conclude, we suggest several possibilities for extensions of this work and for future research directions.

Rigidity. The most immediate open question left by our work is whether there exists a quantum analogue of Lemma 5.7 which would allow us to transform any symmetric quantum circuit into an equivalent rigid such circuit with limited blowup. Such a transformation would allow us to extend our results to all symmetric quantum circuits. To preserve the strength of our results, we would need this transformation to induce only a constant-factor blowup in the entanglement width.

Beyond CNOT and entanglement width. Can our lower bound results be extended to quantum circuits over more general gate sets, such as the threshold gate set $\mathbb{G}_{\text{thr}}^Q$? Furthermore, bounded entanglement width is a sufficient condition to be able to prove the ℓ -partition symmetry property (Theorem 8.6) and hence the quantum indistinguishability theorem (Theorem 8.8); are there weaker properties which suffice to prove these theorems, leading to a stronger result?

Lower bounds on quantum properties. Part II of this thesis focuses on lower bounds for symmetric quantum circuits computing classical properties; that is, we assume the circuits take classical structures as inputs. This is convenient because on classical structures, our quantum pebble games reduce to the classical (G, k) -pebble game (Lemma 3.14, Corollary 4.12). It would be interesting to find *quantum properties*—sets of quantum structures—on which Duplicator wins one of our quantum pebble games, and to adapt our technique to prove lower bounds on symmetric circuits computing them.

More general quantum symmetries. Similarly, it would be interesting to adapt our technique to prove lower bounds on Γ -symmetric circuits for more general unitary groups $\Gamma \leq U(\mathcal{H}_n^\tau)$ which do not necessarily just permute the wires.

Reductions. Dawar [Daw15a] extends his lower bounds on symmetric classical circuits computing the CFI property to other more natural properties using a symmetric version of AC^0 reductions. Can the same be done for our technique?

Symmetric ZX-diagrams. The *ZX-calculus* [CD08; CD11] is an alternative graphical language for quantum computation which is in many respects simpler than the standard quantum circuit notation; a good introduction is [Wet20]. Linear maps are represented by *ZX-diagrams*, which are networks of nodes called *spiders*. Can our technique be adapted to prove lower bounds on the sizes of suitably-defined families of symmetric ZX-diagrams?

Quantum logic. Pebble games are tightly connected to finite variable logics: the classical pebble games of Section 2.3 characterize equivalence in \mathcal{L}_k and \mathcal{C}_k . Are there natural logics which are similarly characterized by the quantum pebble games introduced in this thesis—perhaps a finite variable fragment of linear logic [Gir87], which has been proposed as a logic of quantum information [BS11; RS20; Pra92]?

Pebbling comonads. Abramsky, Dawar, and Wang [ADW17] have introduced a categorical formulation of pebble games using so-called *pebbling comonads*, part of a more general theory of *game comonads* [AR24]. Quantum theory also has a well-developed categorical formulation [AC04; HV19]. Can our quantum pebble games be understood in terms of the framework of pebbling comonads?

Appendix A

Additional lemmas

A.1 Lemmas used in Chapter 4

To prove equation (4.2), the following lemma suffices.

Lemma A.1. *Let $\mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite Hilbert space, ρ be a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$, and A be an operator on \mathcal{H}_A . Then*

$$\mathrm{Tr}_B((A \otimes \mathbb{I})\rho) = A \mathrm{Tr}_B(\rho). \quad (\text{A.1})$$

Proof. Let $\{|a_i\rangle\}_i$ and $\{|b_j\rangle\}_j$ be orthonormal bases for \mathcal{H}_A and \mathcal{H}_B respectively. Then $\{|a_i\rangle \otimes |b_j\rangle\}_{ij}$ is an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$. We may decompose ρ as

$$\rho = \sum_{ij} \alpha_{ij} (|a_i\rangle \otimes |b_j\rangle)(\langle a_i| \otimes \langle b_j|) = \sum_{ij} \alpha_{ij} |a_i\rangle \langle a_i| \otimes |b_j\rangle \langle b_j|. \quad (\text{A.2})$$

Then $\mathrm{Tr}_B(\rho) = \sum_{ij} \alpha_{ij} |a_i\rangle \langle a_i|$, and

$$\mathrm{Tr}_B((A \otimes \mathbb{I})\rho) = \sum_{ij} \alpha_{ij} \mathrm{Tr}_B((A \otimes \mathbb{I})(|a_i\rangle \langle a_i| \otimes |b_j\rangle \langle b_j|)) \quad (\text{A.3})$$

$$= \sum_{ij} \alpha_{ij} \mathrm{Tr}_B(A|a_i\rangle \langle a_i| \otimes |b_j\rangle \langle b_j|) \quad (\text{A.4})$$

$$= \sum_{ij} \alpha_{ij} A |a_i\rangle \langle a_i| = A \mathrm{Tr}_B(\rho). \quad \square$$

Lemma A.2. *Let A and B be Hermitian operators on a Hilbert space \mathcal{H} . If $\langle \psi | A | \psi \rangle = \langle \psi | B | \psi \rangle$ for all $|\psi\rangle \in \mathcal{H}$, then $A = B$.*

Proof. By linearity, $\langle \psi | A | \psi \rangle = \langle \psi | B | \psi \rangle$ iff $\langle \psi | (A - B) | \psi \rangle = 0$, and $A - B$ is Hermitian if A and B are Hermitian. Thus it suffices to show that if $\langle \psi | A | \psi \rangle = 0$ for all $|\psi\rangle \in \mathcal{H}$ then $A = 0$. Since A is Hermitian, we may diagonalize it [KLM06, Thm. 2.4.2], writing $A = \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i|$ for some orthonormal eigenbasis $\{|\lambda_i\rangle\}$. But then for each i , we have $\langle \lambda_i | A | \lambda_i \rangle = \lambda_i = 0$ by assumption, so in fact $A = 0$. \square

A.2 Lemmas used in Chapter 7

All logarithms in the following lemma are base 2.

Lemma A.3. *Let $f, g : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ with $f(n) = \omega(1)$. If $g(n) = \Omega(2^{f(n)})$, then $g(n) = 2^{\Omega(f(n))}$.*

Proof. Since $g(n) = \Omega(2^{f(n)})$, there is some $c > 0$ such that for large enough n , $g(n) \geq c \cdot 2^{f(n)} = 2^{f(n)+\log c}$. Now $f(n) + \log c = \Omega(f(n))$, so there some $d > 0$ such that for large enough n , $\log g(n) \geq f(n) + \log c \geq d \cdot f(n)$. Hence $g(n) = 2^{\Omega(f(n))}$. \square

A.3 Lemmas used in Chapter 8

Lemma A.4. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite Hilbert space. Let $\rho \in D(\mathcal{H})$. If $\text{Tr}_B(\rho) = |\psi\rangle\langle\psi|$ is a pure state, then $\rho = |\psi\rangle\langle\psi| \otimes \rho'$, where $\rho' = \text{Tr}_A(\rho)$.

Proof. Let $\{|a_i\rangle\}_i$ and $\{|b_i\rangle\}_i$ be orthonormal bases for \mathcal{H}_A and \mathcal{H}_B respectively, chosen such that $|\psi\rangle = |a_1\rangle$. Write $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for some positive real numbers $\{p_i\}_i$ with $\sum_i p_i = 1$, and further write each $|\psi_i\rangle$ as $|\psi_i\rangle = \sum_{jk} \alpha_{ijk} |a_j\rangle |b_k\rangle$ for some complex numbers $\{\alpha_{ijk}\}_{jk}$ where $\sum_{jk} |\alpha_{ijk}|^2 = 1$. We obtain

$$\rho = \sum_i p_i \left(\sum_{jk} \alpha_{ijk} |a_j\rangle |b_k\rangle \right) \left(\sum_{jk} \alpha_{ijk}^* \langle a_j | \langle b_k | \right) \quad (\text{A.5})$$

$$= \sum_{i,j,k,j',k'} p_i \alpha_{ijk} \alpha_{ij'k'}^* |a_j\rangle \langle a_{j'}| \otimes |b_k\rangle \langle b_{k'}| \quad (\text{A.6})$$

where α^* denotes the complex conjugate of α . Hence,

$$\text{Tr}_B(\rho) = |\psi\rangle\langle\psi| = \sum_{i,j,j',k} p_i \alpha_{ijk} \alpha_{ij'k}^* |a_j\rangle \langle a_{j'}|. \quad (\text{A.7})$$

Since we chose $|\psi\rangle = |a_1\rangle$, we therefore have

$$\sum_{ik} p_i \alpha_{i1k} \alpha_{i1k}^* = \sum_{ik} p_i |\alpha_{i1k}|^2 = 1 \quad (\text{A.8})$$

and since $\sum_i p_i = 1$, we must have $\sum_k |\alpha_{i1k}|^2 = 1$ for each i . Since $\sum_{jk} |\alpha_{ijk}|^2 = 1$ for each i , we therefore have $\alpha_{ijk} = 0$ whenever $j \neq 1$. Hence,

$$\rho = \sum_{i,k,k'} p_i \alpha_{i1k} \alpha_{i1k}^* |\psi\rangle\langle\psi| \otimes |b_k\rangle\langle b_{k'}| = |\psi\rangle\langle\psi| \otimes \sum_{i,k,k'} p_i \alpha_{i1k} \alpha_{i1k}^* |b_k\rangle\langle b_{k'}| \quad (\text{A.9})$$

and so $\rho = |\psi\rangle\langle\psi| \otimes \text{Tr}_A(\rho)$. □

Lemma A.5. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite Hilbert space. Let $\rho_1 \in D(\mathcal{H}_A)$ and $\rho_2 \in D(\mathcal{H}_B)$. Then $\rho_1 \otimes \rho_2$ is a pure state if and only if both ρ_1 and ρ_2 are pure states.

Proof. For any density matrix ρ we have $\text{Tr}(\rho^2) \leq 1$, with equality if and only if ρ is a pure state [NC10]. We have $\text{Tr}((\rho_1 \otimes \rho_2)^2) = \text{Tr}(\rho_1^2 \otimes \rho_2^2) = \text{Tr}(\rho_1^2) \text{Tr}(\rho_2^2)$, so $\text{Tr}((\rho_1 \otimes \rho_2)^2) = 1$ iff $\text{Tr}(\rho_1^2) = \text{Tr}(\rho_2^2) = 1$. □

Lemma A.6. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be a tripartite Hilbert space. Let $\rho^{ABC} \in D(\mathcal{H})$. If $\rho^{AB} = \text{Tr}_C(\rho^{ABC})$ and $\rho^{AC} = \text{Tr}_B(\rho^{ABC})$ are pure states, then $\rho^A = \text{Tr}_{BC}(\rho^{ABC})$ is a pure state.

Proof. Let $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}_D$ be a purification of ρ^{ABC} , i.e. a state $|\psi\rangle$ such that $\text{Tr}_D(|\psi\rangle\langle\psi|) = \rho^{ABC}$ for some Hilbert space \mathcal{H}_D [NC10]. Since ρ^{AB} is a pure state, by Lemma A.4,

$$|\psi\rangle\langle\psi| = \rho^{AB} \otimes \text{Tr}_{AB}(|\psi\rangle\langle\psi|). \quad (\text{A.10})$$

Furthermore, $\rho^{AC} = \text{Tr}_{BD}(|\psi\rangle\langle\psi|)$, so

$$\rho^{AC} = \text{Tr}_B(\rho^{AB}) \otimes \text{Tr}_D(\text{Tr}_{AB}(|\psi\rangle\langle\psi|)) = \rho^A \otimes \text{Tr}_{ABD}(|\psi\rangle\langle\psi|). \quad (\text{A.11})$$

By Lemma A.5, since ρ^{AC} is a pure state, ρ^A is a pure state. \square

References

- [AC04] Samson Abramsky and Bob Coecke. “A categorical semantics of quantum protocols”. In: *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*. Turku, Finland, 2004, pp. 415–425. DOI: [10.1109/LICS.2004.1319636](https://doi.org/10.1109/LICS.2004.1319636).
- [AD17] Matthew Anderson and Anuj Dawar. “On Symmetric Circuits and Fixed-Point Logics”. In: *Theory of Computing Systems* 60 (Apr. 2017), pp. 521–551. DOI: [10.1007/s00224-016-9692-2](https://doi.org/10.1007/s00224-016-9692-2).
- [ADW17] Samson Abramsky, Anuj Dawar, and Pengming Wang. “The pebbling comonad in finite model theory”. In: *32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. Reykjavik, Iceland, 2017, pp. 1–12. DOI: [10.1109/LICS.2017.8005129](https://doi.org/10.1109/LICS.2017.8005129).
- [AKS12] Andris Ambainis, Julia Kempe, and Or Sattath. “A Quantum Lovász Local Lemma”. In: *Journal of the ACM* 59.5 (Oct. 2012), pp. 1–24. DOI: [10.1145/2371656.2371659](https://doi.org/10.1145/2371656.2371659).
- [AR24] Samson Abramsky and Luca Reggio. “An Invitation to Game Comonads”. In: *ACM SIGLOG News* 11.3 (Aug. 2024), pp. 5–48. DOI: [10.1145/3687256.3687260](https://doi.org/10.1145/3687256.3687260).
- [BGS02] Andreas Blass, Yuri Gurevich, and Saharon Shelah. “On polynomial time computation over unordered structures”. In: *Journal of Symbolic Logic* 67.3 (2002), pp. 1093–1125. DOI: [10.2178/jsl/1190150152](https://doi.org/10.2178/jsl/1190150152).
- [BGS99] Andreas Blass, Yuri Gurevich, and Saharon Shelah. “Choiceless polynomial time”. In: *Annals of Pure and Applied Logic* 100.1–3 (1999), pp. 141–187. DOI: [10.1016/S0168-0072\(99\)00005-6](https://doi.org/10.1016/S0168-0072(99)00005-6).
- [BS11] John Baez and Mike Stay. “Physics, Topology, Logic and Computation: A Rosetta Stone”. In: *New Structures for Physics*. Ed. by Bob Coecke. Berlin, Heidelberg: Springer, 2011, pp. 95–172. DOI: [10.1007/978-3-642-12821-9_2](https://doi.org/10.1007/978-3-642-12821-9_2).
- [BV97] Ethan Bernstein and Umesh Vazirani. “Quantum Complexity Theory”. In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1411–1473. DOI: [10.1137/S0097539796300921](https://doi.org/10.1137/S0097539796300921). First appeared in ACM STOC 1993.
- [CD08] Bob Coecke and Ross Duncan. “Interacting Quantum Observables”. In: *35th International Colloquium on Automata, Languages and Programming (ICALP)*. Ed. by Luca Aceto et al. Lecture Notes in Computer Science. Springer, 2008, pp. 298–310. DOI: [10.1007/978-3-540-70583-3_25](https://doi.org/10.1007/978-3-540-70583-3_25).
- [CD11] Bob Coecke and Ross Duncan. “Interacting quantum observables: categorical algebra and diagrammatics”. In: *New Journal of Physics* 13.043016 (Apr. 2011). DOI: [10.1088/1367-2630/13/4/043016](https://doi.org/10.1088/1367-2630/13/4/043016).
- [CFI92] Jin-Yi Cai, Martin Fürer, and Neil Immernan. “An optimal lower bound on the number of variables for graph identification”. In: *Combinatorica* 12.4 (Dec. 1992), pp. 389–410. DOI: [10.1007/BF01305232](https://doi.org/10.1007/BF01305232).
- [CGS25] Davi Castro-Silva, Tom Gur, and Sergii Strelchuk. *Symmetric quantum computation*. Jan. 2, 2025. DOI: [10.48550/arXiv.2501.01214](https://doi.org/10.48550/arXiv.2501.01214). arXiv: [2501.01214 \[quant-ph\]](https://arxiv.org/abs/2501.01214).
- [Cor+22] Thomas H. Cormen et al. *Introduction to algorithms*. Fourth edition. Cambridge, Massachusetts: The MIT Press, 2022.

- [Czé22] Gábor Czédli. “Cyclic congruences of slim semimodular lattices and non-finite axiomatizability of some finite structures”. In: *Archivum Mathematicum* 58.1 (2022), pp. 15–33. DOI: 10.5817/AM2022-1-15.
- [Daw15a] Anuj Dawar. “On Symmetric and Choiceless Computation”. In: *Topics in Theoretical Computer Science (TTCS)*. Ed. by Mohammed Taghi Hajiaghayi and Mohammad Reza Mousavi. Tehran, Iran, Aug. 2015, pp. 23–29. DOI: 10.1007/978-3-319-28678-5_2.
- [Daw15b] Anuj Dawar. “The nature and power of fixed-point logic with counting”. In: *ACM SIGLOG News* 2.1 (Jan. 2015), pp. 8–21. DOI: 10.1145/2728816.2728820.
- [DM96] John D. Dixon and Brian Mortimer. *Permutation groups*. Graduate Texts in Mathematics. New York: Springer, 1996.
- [DRR08] Anuj Dawar, David Richerby, and Benjamin Rossman. “Choiceless polynomial time, counting and the Cai–Fürer–Immerman graphs”. In: *Annals of Pure and Applied Logic* 152.1 (Mar. 2008), pp. 31–50. DOI: 10.1016/j.apal.2007.11.011.
- [DW20] Anuj Dawar and Gregory Wilsenach. “Symmetric Arithmetic Circuits”. In: *47th International Colloquium on Automata, Languages, and Programming (ICALP)*. Ed. by Artur Czumaj, Anuj Dawar, and Emanuela Merelli. Vol. 168. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020, 36:1–36:18. DOI: 10.4230/LIPIcs.ICALP.2020.36. Full version at arXiv:2002.06451v3.
- [DW21] Anuj Dawar and Gregory Wilsenach. “Symmetric Circuits for Rank Logic”. In: *ACM Transactions on Computational Logic* 23.1 (Nov. 2021), 6:1–35. DOI: 10.1145/3476227.
- [DW22] Anuj Dawar and Gregory Wilsenach. “Lower Bounds for Symmetric Circuits for the Determinant”. In: *13th Innovations in Theoretical Computer Science Conference (ITCS)*. Ed. by Mark Braverman. Vol. 215. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 52:1–52:22. DOI: 10.4230/LIPIcs.ITCS.2022.52. Full version at arXiv:2107.10986v3.
- [EF99] Heinz-Dieter Ebbinghaus and Jörg Flum. *Finite Model Theory*. Second edition. Springer Monographs in Mathematics. Berlin: Springer, 1999. DOI: 10.1007/3-540-28788-4.
- [Ehr61] Andrzej Ehrenfeucht. “An application of games to the completeness problem for formalized theories”. In: *Fundamenta Mathematicae* 49.2 (1961), pp. 129–141.
- [Fag74] Ronald Fagin. “Generalized first-order spectra and polynomial-time recognizable sets”. In: *Complexity of computation*. Ed. by Richard M. Karp. Vol. VII. SIAM–AMS Proceedings. American Mathematical Society, 1974, pp. 43–73.
- [FLS06] Michael Freedman, László Lovász, and Alexander Schrijver. “Reflection positivity, rank connectivity, and homomorphism of graphs”. In: *Journal of the American Mathematical Society* 20.1 (Apr. 2006), pp. 37–51. DOI: 10.1090/s0894-0347-06-00529-7.
- [Fra54] Roland Fraïssé. “Sur quelques classifications des systèmes de relations”. In: *Université d’Alger, Publications Scientifiques, Série A* 1 (1954), pp. 35–182.
- [Gir87] Jean-Yves Girard. “Linear logic”. In: *Theoretical Computer Science* 50.1 (1987), pp. 1–101. DOI: [https://doi.org/10.1016/0304-3975\(87\)90045-4](https://doi.org/10.1016/0304-3975(87)90045-4).
- [GS86] Yuri Gurevich and Saharon Shelah. “Fixed-point extensions of first-order logic”. In: *Annals of Pure and Applied Logic* 32 (Jan. 1986), pp. 265–280. DOI: 10.1016/0168-0072(86)90055-2.

- [Gur83] Yuri Gurevich. “Toward logic tailored for computational complexity”. In: *Computation and Proof Theory*. Ed. by Egon Börger et al. Lecture Notes in Mathematics. Aachen, July 1983, pp. 175–216.
- [Hal35] P. Hall. “On Representatives of Subsets”. In: *Journal of the London Mathematical Society* s1-10.1 (1935), pp. 26–30. DOI: 10.1112/jlms/s1-10.37.26.
- [Hel96] Lauri Hella. “Logical Hierarchies in PTIME”. In: *Information and Computation* 129.1 (Aug. 1996), pp. 1–19. DOI: 10.1006/inco.1996.0070.
- [HV19] Chris Heunen and Jamie Vicary. *Categories for Quantum Theory: An Introduction*. Oxford University Press, Nov. 2019. DOI: 10.1093/oso/9780198739623.001.0001.
- [IL90] Neil Immerman and Eric Lander. “Describing Graphs: A First-Order Approach to Graph Canonization”. In: *Complexity Theory Retrospective*. Ed. by Alan L. Selman. New York, NY: Springer, 1990, pp. 59–81. DOI: 10.1007/978-1-4612-4478-3_5.
- [Imm82a] Neil Immerman. “Relational queries computable in polynomial time (Extended Abstract)”. In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*. STOC ’82. New York, NY, USA: Association for Computing Machinery, May 1982, pp. 147–152. DOI: 10.1145/800070.802187.
- [Imm82b] Neil Immerman. “Upper and lower bounds for first order expressibility”. In: *Journal of Computer and System Sciences* 25.1 (Aug. 1982), pp. 76–98. DOI: 10.1016/0022-0000(82)90011-3.
- [Imm86] Neil Immerman. “Relational queries computable in polynomial time”. In: *Information and Control* 68.1 (Jan. 1986), pp. 86–104. DOI: 10.1016/s0019-9958(86)80029-8.
- [Imm99] Neil Immerman. *Descriptive complexity*. Graduate texts in computer science. New York: Springer, 1999. DOI: 10.1007/978-1-4612-.
- [JL03] Richard Jozsa and Noah Linden. “On the role of entanglement in quantum computational speed-up”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 459.2036 (Aug. 2003), pp. 2011–2032. DOI: 10.1098/rspa.2002.1097.
- [KLM06] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Nov. 2006. DOI: 10.1093/oso/9780198570004.001.0001.
- [Kos24] Roman Kossak. *Mathematical Logic: On Numbers, Sets, Structures, and Symmetry*. Second edition. Springer International Publishing, Apr. 2024. DOI: 10.1007/978-3-031-56215-0.
- [KZ21] Jochen Koenigsmann and Boris Zilber. *C1.1: Model Theory*. Lecture notes. Oct. 2021. URL: https://courses.maths.ox.ac.uk/pluginfile.php/27019/mod_resource/content/1/MT.pdf.
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Dec. 2010. DOI: 10.1017/CBO9780511976667.
- [Pag23] Benedikt Pago. “Lower Bounds for Choiceless Polynomial Time via Symmetric XOR-Circuits”. In: *48th International Symposium on Mathematical Foundations of Computer Science (MFCS)*. Ed. by Jérôme Leroux, Sylvain Lombardy, and David Peleg. Vol. 272. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 73:1–73:15. DOI: 10.4230/LIPIcs.MFCS.2023.73.

- [Pra92] Vaughan R. Pratt. “Linear Logic for Generalized Quantum Mechanics”. In: *Workshop on Physics and Computation*. Dallas, Texas, USA: IEEE, 1992, pp. 166–180.
- [PT04] Asher Peres and Daniel R. Terno. “Quantum information and relativity theory”. In: *Reviews of Modern Physics* 76.1 (Jan. 2004), pp. 93–123. DOI: [10.1103/RevModPhys.76.93](https://doi.org/10.1103/RevModPhys.76.93).
- [RS20] Mathys Rennela and Sam Staton. “Classical Control, Quantum Circuits and Linear Logic in Enriched Category Theory”. In: *Logical Methods in Computer Science* 16.1 (Mar. 2020). DOI: [10.23638/LMCS-16\(1:30\)2020](https://doi.org/10.23638/LMCS-16(1:30)2020).
- [Val79] L. G. Valiant. “Completeness classes in algebra”. In: *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*. STOC ’79. Atlanta, Georgia, USA: Association for Computing Machinery, 1979, pp. 249–261. DOI: [10.1145/800135.804419](https://doi.org/10.1145/800135.804419).
- [Var82] Moshe Y. Vardi. “The complexity of relational query languages (Extended Abstract)”. In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*. STOC ’82. New York, NY, USA: Association for Computing Machinery, May 1982, pp. 137–146. DOI: [10.1145/800070.802186](https://doi.org/10.1145/800070.802186).
- [Wei76] Boris Weisfeiler. *On Construction and Identification of Graphs*. Springer, 1976. DOI: [10.1007/bfb0089374](https://doi.org/10.1007/bfb0089374).
- [Wet20] John van de Wetering. *ZX-calculus for the working quantum computer scientist*. Dec. 2020. DOI: [10.48550/arXiv.2012.13966](https://doi.org/10.48550/arXiv.2012.13966). arXiv: 2012.13966 [quant-ph].
- [WL68] Boris Weisfeiler and A. A. Lehman. “A Reduction of a Graph to a Canonical Form and an Algebra Arising During This Reduction”. In: *Nauchno-Technicheskaya Informatsia* Ser. 2.N9 (1968), pp. 12–16. In Russian.