A Study of Non-Local Strategies for Zero-Knowledge Proof Systems

Aly Tarek Ibrahim, School of Computer Science
McGill University, Montreal
June, 2020

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of

Master of Computer Science

Abstract

No-signalling (NOSIG) correlations, that are stronger than those allowed by quantum entanglement yet do not violate relativistic causality, are a valuable resource for understanding information processing systems. Such correlations can be achieved between non-communicating players in games when the players use what is called non-local strategies, and can give the players better odds at winning in these games. We propose definitions for non-local strategies in relativistic multi-player non-local games. We prove a conjecture by Crépeau stating that any non-local strategy that can be simultaneously produced by any pi-signalling strategy in a multi-player non-local game, has to be a NOSIG strategy.

Pi-signalling strategies are achieved when 1-way signalling is allowed between players arranged on a line defined by some permutation.

This result gives us a better understanding of how NOSIG strategies fit with the other non-local strategies, and can help in constructing novel NOSIG multi-player strategies and help prove they produce NOSIG correlations. Finally, we extend the definition of zero-knowledge proof systems to the relativistic multi-prover, multi-verifier setting, and propose definitions for what it means for a non-local strategy to have polynomial time complexity.

Résumé

Les corrélations non signalantes (NOSIG), qui sont plus fortes que celles permises par l'intrication quantique, tout en respectant la causalité relativiste, sont des ressources de valeur pour comprendre les systèmes de traitement de l'information. De telles corrélations peuvent être réalisées par des joueurs qui ne se communiquent pas dans les jeux lorsque les joueurs utilisent ce qu'on appelle des stratégies non locales, et ces corrélations permettent aux joueurs de gagner dans ces jeux avec de meilleures probabilités. Nous proposons des définitions de stratégies non locales dans des jeux relativistes non-locaux à joueurs multiples. Nous prouvons la conjecture de Crépeau qui déclare que toute stratégie non locale qui peut être produite simultanément par n'importe quelle stratégie pi-signalante dans un jeu non local multi-joueurs doit être une stratégie NOSIG.

Les stratégies pi-signalantes sont obtenues lorsque la signalisation unidirectionnelle est autorisée entre des joueurs disposés sur une ligne définie par une permutation.

Ce résultat nous permet de mieux comprendre comment les stratégies NOSIG s'intègrent aux autres stratégies non locales, et peut aider à construire de nouvelles stratégies multi-joueurs NOSIG et aider à prouver qu'elles produisent des corrélations NOSIG. Enfin, nous étendons la définition des systèmes à preuve à divulgation nulle de connaissance au cadre relativiste multi-prouveur, multi-vérificateur, et proposons des définitions pour une stratégie non locale d'une complexité polynomiale.

Acknowledgements

First and foremost I would love to thank my advisor Claude Crépeau for introducing me to non-local games and the particular problem this thesis is based on, for his guidance throughout the research process, his meticulous feedback, and his generosity with time and ideas. My conversations with Claude always inspired me to be more curious and through his mentorship this thesis was possible. He was integral to my growth as a computer science researcher, and for that I am eternally grateful.

I would like to thank my thesis examiner, Dave Touchette, for thoroughly reading my work and providing invaluable feedback that enhanced the final version of this document.

I want to thank Nadeem Ward for easing my transition to Montréal and McGill, and showing me the ins and outs of this beautiful city. I wanted to give a big thanks to my labmate, Justin Li, for the fruitful discussions and constantly bouncing ideas off each other which made research more enjoyable and for helping me in translating this thesis's abstract to French on a short notice, I appreciate it brother!

I wish to thank my parents, Samaa and Tarek, for raising me to be the person I am today. I would not be here without your unconditional love and support —I love you. And to my big brother, Omar, for always having my back and being my best friend.

Last but not least, I wanted to thank my loving wife, Hanan—You are my role model and my home.

ربّ أوْزعْني أنْ أشْكر نعْمتك الّتي أنْعمْت عليّ وعلى والديّ وأنْ أعْمل صالحا ترْضاه وأدْخلْني برحْمتك في عبادك الصّالحين

Contribution of Author

- In chapter 2, in the Game theory section, we split actions and strategies into micro actions / strategies and macro ones, which is not how it is defined in any literature we came across, but this distinction was useful throughout this work.
- In chapter 3, our definitions of information theoretic Strategies, T strategies, concrete T strategies are new in this form. Our definition of Local and QPE Strategies is also new.
- Chapter 4 is our work. We developed this chapter to create the appropriate framework to facilitate proving Crépeau's theorem. Discussions with our advisor were helpful for getting the proof correct.
- The generalized zero-knowledge proof system definition in chapter 5 is our work. The problem of needing to generalize the definition came from our advisor and his answers to our questions helped us reach the final form of the definitions in this chapter.
- Appendices *B* and *C* are also our work.

Contents

Chapter 1

Introduction

> In theory, there is no difference
> between theory and practice;
> but in practice there is.
>
> Unknown

Quantum computing poses a direct threat to public-key cryptosystems that are widely used all over the internet [Ber09]. The cryptosystems that are vulnerable to quantum-attacks relied on computational hardness assumptions like the difficulty of factoring large prime numbers or computing the discrete logarithm. However, these assumptions were no longer valid as of 1994, when Peter Shor invented a polynomial time factoring quantum algorithm [Sho97]. Ever since then, cryptographers worked on building post-quantum cryptosystems that are resilient to quantum attacks. The issue with these new algorithms is that they have only been studied theoretically for a few decades and rarely implemented at scale, while the existing cryptosystems have been deployed in the Internet, used by billions of people, were thoroughly tested for the past half-century, and even before that many mathematicians and computer scientists dedicated their lives to try to break them, until this revolutionary idea of harnessing quantum mechanical resources to tackle the underlying hardness problem broke these assumptions. This is troubling to any cryptographer, because quantum computing is a new field and as hardware starts catching up with the theory, and companies start building larger quantum computers, more malicious attackers will work on compromising these new cryptographic algorithms at a rate faster than theorists can invent new protocols.

The work in this thesis is part of a general movement to build cryptosystems that are not only secure against (known) quantum attacks, but rather resilient to attacks from a broader (up till now hypothetical) physical theory known as no-signalling [Bar+05]. Quantum mechanics is a no-signalling theory, but it turns out that there is room for generalizations to quantum mechanics that still obey Einstein's relativistic causality. Meaning that while these stronger no-signalling theories are physically possible, there is no evidence that these model the dynamics of our universe. However, to cryptographers, if we build systems that are secure against general no-signalling attacks, then we might sleep better at night.

Non-Local Games is a class of games that have been reasonably studied in the past four decades since [Bel64] and [Cla+69]. These games can be used to build cryptographic protocols that are as secure as the winning probability of the various players in the game. This winning probability changes based on the type of non-local strategies the players use throughout the game, which enables the players to achieve correlations (no-signalling, quantum or others) without communicating with one another, which many a times helps improve their chances in winning as we will see in chapter 3. We formally define non-local strategies, and the correlations they produce in multi-player non-local games, we do so in a practical manner that is concerned with how to implement such protocols not just how to analyze them theoretically. Furthermore, one of the properties of cryptographic protocols, built using these games, is having zero-knowledge. We make explicit what it means for a protocol or proof to be zero-knowledge under non-local strategies of players, which led us to define what it means for non-local strategies to have polynomial time complexity. In addition, the main theorem we prove in this thesis (chapter 4) helps prove whether a new non-local box is a valid no-signalling box or not. At the time of this writing, the only non-trivial no-signalling box known is for two players only, and is called a PR-box after Popescu and Rohrlich who proposed it in [PR94]. Our work might help in showing new no-signalling boxes for n-players with $n > 2$ that cannot be constructed from PR-boxes. We highlight one way Crépeau's theorem will be used, in our future paper with Claude Crépeau and Nan Yang, at the end of chapter 5 in section 5.3.

The next chapter (Chapter 2) covers a broad range of theoretical computer science and physics background needed. Following that, chapter 3 shows concrete strategies for two player non-local games and surveys three of the canonical non-local games used in the literature. Chapter 4 is our main contribution, where we generalize these games into multi-player non-local games, and prove Crépeau's theorem relating multi-party no-signaling correlations to those that can be implemented by one-way signaling on the line defined by some permutation Π_i. Following that in chapter 5 we extend the classical definition of the zero-knowledge proofs to the relativistic multi-player setting, formally define the time complexity of non-local strategies and put all the pieces together, and then end the thesis with some conclusions and possible future work in chapter 6. In appendix A we cover some applications of non-local games beyond our work for a better understanding of the field as a whole, then in appendix B we cover an attempt to create a quantum PR-box that is stronger than a regular PR-box. We summarize in appendix C some useful equalities for quantum gates.

Main Contributions:

- Proposing a framework for strategies in non-local games, and extending existing definitions of non-local strategies to the multi-player non-local games' setting.
- Proving Crépeau's theorem ($\mathbb{NO}$-$\mathbb{SIG} = \bigcup_{n\in\mathbb{N}^+} \bigcap_{i=1}^{n!} \Pi_i$-$\mathbb{SIG}(\mathrm{n})$).
- Establish the framework where simulators, in zero-knowledge protocols, have access to polynomial time n-player non-local strategies.
- This document serves as an introduction to non-local games and their strategies.

Chapter 2

Background

This area of research lies at the intersection of Theoretical Computer Science, Information Theory, Quantum Mechanics, and Einstein's Special Relativity. Although working in this field is exciting for those interested in interdisciplinary research, there is a steep learning curve to get started. This chapter serves as a quick overview of so many fields, it covers the language used, and the basic definitions from which entire subject matters follow. For the readers already in the field, there is no harm in scanning these quickly as a refresher, and for the researchers newly embarking on this amazing journey, this chapter would serve as a compass to help them quickly ramp up and develop a road map on areas where they need further studying.

We will assume knowledge of asymptotic notation, probability, statistics, linear algebra, and whenever we need any algebra or topology we will explain it at that point. Otherwise, we will try to make this document self-contained and will begin with the basic notions from the theory of computation and complexity theory, introducing proof systems which are the main subject matter. Next we do a quick introduction of quantum mechanics and relativity, followed by covering fundamentals of quantum computation and scratch the surface of information theory both classical and quantum. We will also highlight some notions needed from game theory and cryptography.

2.1 Theory of Computation

Entire courses are dedicated for this subject matter, we will sample here the most essential. For further reading we recommend [Sip96].

Definition 2.1.1 (Turing Machine)**.** *A Turing Machine, $\mathcal{M}$, is defined by $\langle Q, \Gamma, b, \Sigma, \delta, q_0, F\rangle$ together with an infinite one-directional tape s.t.*

- *$Q \neq \emptyset$ is a finite set of states.*
- *$\Gamma \neq \emptyset$ is a finite set of alphabet symbols.*
- *$b \in \Gamma$ denotes a blank/empty symbol.*

- $\Sigma \subseteq (\Gamma - \{b\})$ *are the input symbols, the ones allowed to appear in the initial tape configuration denoting the input to* $\mathcal{M}$.
- $q_0 \in Q$ *is the initial state of* $\mathcal{M}$.
- $F \subseteq Q$ *are the final accepting states of* $\mathcal{M}$.
- $\delta : (Q - F) \times \Gamma \nrightarrow Q \times \Gamma \times \{\text{L,R}\}$ *is a partial function denoting the transition table. Here L orders the tape head to move left, and right is to move right.*

A Turing Machine is mathematical model of computation that defines an abstract machine, which manipulates symbols, $\sigma \in \Sigma$, on a strip of tape according to a table of rules represented as δ. The machine has a tape head that points to some cell on the tape and could read its value and according to the rules in δ move the head (left or right) or write a new value to the current cell. Although this model is simple, a Turing machine is capable of simulating any computer algorithm.

Many variants for Turing Machines (TM) exist. From introducing multiple tapes or two-way infinite tapes, each possibly with read only, write only, or read / write capabilities, some could be read once. What is relevant here is that all these single machine models can simulate one-another with a polynomial time overhead, and variation exist for pure convenience and simplicity (**known as universality of TMs**).

Definition 2.1.2 (Probabilistic Turing Machine)**.** *A probabilistic Turing machine is a TM equipped with an extra tape that is filled with new random symbols from* Σ *with each initialization.*

Definition 2.1.3 (Non-Deterministic Turing Machine)**.** *A non-deterministic Turing machine is a TM with* δ *defined as a transition relation instead of a function*

$$\delta : ((Q - F) \times \Gamma) \times Q \times \Gamma \times \{\text{L,R}\}$$

The change in δ to become a relation means the result/yield of the relation gives a set of possibilities instead of a single outcome. Hence, a non-deterministic TM accepts an input string iff at least one of the possible computational paths starting from that string puts the machine into an accepting state.

Definition 2.1.4 (Reducibility)**.** *A reduction from problem A to problem B is a function* $f : \Sigma_A^* \to \Sigma_B^*$ *s.t.* $\forall a \in \Sigma_A^*$ *we have*

$$a \in A \iff f(w) \in B$$

If f could be implemented in polynomial time then this is a polynomial/Karp reduction (other reductions exist, but we will not care about them in this work.) We say that if A reduces polynomially to B, then B is at least as hard as A and denote it $B \leq_p A$.

A Turing Machine is one of the main (uniform) models of computation that specifies how an output of a function is computed from its input. Another important model of computation which is non-uniform is the Circuit Model, where the output of each input size is computed by a different function or circuit.

Definition 2.1.5 (Circuit)**.** *A circuit, $\mathcal{C}$, is defined by a triple $\langle V, F, G \rangle$, s.t.*

- *V is a finite set of values.*
- *F is a set of functions $f : V^i \to V$, with $i \in \mathbb{N}^+$, denoting gates with i inputs and a single output.*
- *G is a directed acyclic graph with nodes representing gates and edges representing connections from inputs to outputs of these gates.*

While there exists infinitely many sets of gates F that could capture universal computation, we usually restrict ourselves to one of the smallest possible sets that is simple and convenient for analysis. For example, in classical (digital) circuits[1], the universal gate set chosen is often $\{\text{AND}, \text{OR}, \text{NOT}\}$.

Definition 2.1.6 (Polynomial-Time Uniform)**.** *A family of circuits $\{C_n \mid n \in \mathbb{N}\}$ is poly-time uniform if $\exists$ a deterministic polynomial time TM, $\mathcal{M}$, s.t. $\forall\ n \in \mathbb{N}$, $\mathcal{M}$ outputs a circuit description of C_n on input 1^n.*

Here C_n would compute the output of some function on inputs of size n.

2.2 Classical Complexity Theory

A good deeper dive into the topic of complexity theory would be [AB09]. Here we only cover some of the basic definitions, then go through the developments that happened in proof systems in the past decades.

2.2.1 Problems and Languages

Computational problems can be phrased as either a search problem, a counting problem, an optimization problem, or a decision problem. We care about optimization and decision problems in this document, but understanding search and counting problems is needed to define optimization problems.

Definition 2.2.1 (Binary Relation)**.** *A binary relation, $\mathcal{R}$, consists of a domain set A and a codomain set B, and is represented by a subset of $A \times B$.*

Definition 2.2.2 (Search Problem)**.** *A search problem is defined by a binary relation, $\mathcal{R}$, s.t.*

- *If $\forall$ input x, $\exists y$ such that $\mathcal{R}(x, y)$, then a Turing Machine, $\mathcal{T}$, accepts x outputting any of the y's satisfying $\mathcal{R}(x, y)$.*
- *If x is such that there is no y satisfying $\mathcal{R}(x, y)$, then $\mathcal{T}$ rejects x.*

[1] Circuits that could implement any Boolean function.

Definition 2.2.3 (Counting Problem)**.** *A counting problem, $\mathcal{C}$, with input x, is a search problem with binary relation $\mathcal{R}$ s.t.*

$$\mathcal{C}_{\mathcal{R}}(x) = |\{y \mid \mathcal{R}(x, y)\}|$$

Definition 2.2.4 (Optimization Problem)**.** *An optimization problem is w.l.o.g. the maximization of a counting problem $\mathcal{C}$.*

$$\operatorname*{argmax}_{x} \Big[\mathcal{C}_{\mathcal{R}}(x)\Big]$$

Definition 2.2.5 (Decision Problem)**.** *A decision problem is a boolean function $f\colon \{0,1\}^n \to \{0,1\}$, that maps the binary encoding of an input to the problem (binary strings of length n) to a YES or NO answer.*

Definition 2.2.6 (Formal Language)**.** *A language is the set of input strings of a decision problem that map to YES or binary 1.*

$$L_f = \{x : f(x) = 1\}$$

Decision problems are central in the study of complexity theory. Computational complexity theory is concerned mainly with deciding, using an algorithm $\mathcal{A}$, whether a given input string is a member of the formal language under consideration. If $\mathcal{A}$ returns YES then it is said to *accept* this input string (instance), *otherwise*, it either (1) stops and *rejects* membership, (2) loops forever, or (3) has undefined behaviour.

Definition 2.2.7 (Turing-Recognizable)**.** *We say a Turing Machine $\mathcal{M}$ recognizes a language L iff*

- *If $x \in L$, $\mathcal{M}$ reaches an accepting state.*
- *If $x \notin L$, $\mathcal{M}$ (1) stops at a rejecting state or (2) loops infinitely (does not HALT).*

We say L is recognizable if $\exists$ TM $\mathcal{M}$ that recognizes L.

Definition 2.2.8 (Turing-Decidable)**.** *We say a Turing Machine $\mathcal{M}$ decides a language L iff*

- *For any valid instance $x \in L$, $\mathcal{M}$ stops at an accepting state.*
- *For any invalid instance $x \notin L$, $\mathcal{M}$ stops at a rejecting state.*

We say L is decidable if $\exists$ TM $\mathcal{M}$ that decides L.

Definition 2.2.9 (Turing-Computable)**.** *It is the same as Turing-Decidable but when applied to optimization problems instead of decision problems. We say problem P is computable if $\exists$ TM $\mathcal{M}$ that computes P.*

It will be useful for the reader to be acquainted with the notion of a hard language and a complete language.

Definition 2.2.10 ($\mathcal{C}$-Hard)**.** *For some complexity class $\mathcal{C}$, we say language L is $\mathcal{C}$-Hard iff $\forall$ languages $L' \in \mathcal{C}$ we have $L' \leq_p L$.*

Definition 2.2.11 ($\mathcal{C}$-Complete)**.** *For some complexity class $\mathcal{C}$, we say language L is $\mathcal{C}$-Complete iff $L \in \mathcal{C}$-Hard, and $L \in \mathcal{C}$.*

2.2.2 Proof Complexity

In computational complexity theory a proof system is introduced to analyze the computational resources needed to prove or disprove statements.

Definition 2.2.12 (Proof System)**.** *A propositional proof system is defined by a proof-verification algorithm, called a verifier, $\mathcal{A}(x,t)$ with two inputs. x is the proposition, and t is the transcript of the alleged proof (provided by some prover(s)[2]). If the verifier accepts (x,t), denoted by $\mathcal{A}(x,t)=1$, then t is a proof of x. $\mathcal{A}$ needs to have a low false rejection rate (completeness) and a low false acceptance rate (soundness). The verifier is required to be "efficient".*

Informally, completeness gauges how powerful the a proof systems is at generating proofs for valid statements, while soundness implies that the statements that have proofs that pass verification are indeed those that are valid.

Definition 2.2.13 (Completeness)**.** *If a statement is true, a prover can write a proof of length $\mathsf{poly}(x)$ that an honest verifier, $\mathcal{V}$, accepts. If the system is probabilistic, then we say a proof system for language L has completeness α, where $0 \leq \alpha \leq 1$, when:*

$$\forall x \in L,\ Pr[\mathcal{V}(x,t)=1] \geq \alpha$$

Perfect Completeness *is when $\alpha = 1$.*

Definition 2.2.14 (Soundness)**.** *No prover can convince an honest verifier, $\mathcal{V}$, that a false statement is true. If the system is probabilistic, then we say a proof system for language L has soundness $1-\beta$, where $0 \leq \beta \leq 1$, when:*

$$\forall x \notin L,\ Pr[\mathcal{V}(x,t)=1] \leq \beta$$

Perfect Soundness *is when $\beta = 0$.*

Let us examine some of the canonical proof systems typically studied in complexity theory. Let $I = \{0,1\}^*$ be the input set of a function, and $I_n = \{x \in I \mid |x| = n\}$

Definition 2.2.15 (The class P)**.** *For a language $L : I \to I$, we say $L \in \mathsf{P}$, if there exists an algorithm, $\mathcal{A}$, computing membership in L and a positive constant c, such that for every n and every $x \in I_n$, $\mathcal{A}$ computes $x \in L$ in $O(n^c)$ time.*

P is considered the most trivial kind of proof system, where the verifier does not need a proof transcript t accompanying the input x for some language $L \in \mathsf{P}$. This is because the verifier can simply do the polynomial time computation on x to check its membership in L.

[2]Here we are keeping the notion of prover(s) purposely vague. We will expound on this in the bulk of this work, for now just imagine a possibly malicious entity providing t to the verifier

Definition 2.2.16 (The class NP)**.** *The language L is in the class* NP*, if $\exists$ a deterministic polynomial-time verifier TM, V_C, and a constant c s.t.*

- *If $x \in L$, then $\exists t$ with $|t| \in O(|x|^c)$ and $V_C(x,t) = 1$*
- *If $x \notin L$, then $\forall t$ $V_C(x,t) = 0$*

NP is also defined by the languages solvable by a non-deterministic TM in polynomial time. Using both definitions we can imagine a proof system, where the prover has access to a non-deterministic TM as a resource (or an exponential deterministic TM), and can solve any language $L \in$ NP. The prover receives an instance x and so does the deterministic polytime verifier. The prover sends the solution/proof t of instance/input x trying to convince the verifier that x is a member of L. Thereafter, the verifier will always confirm membership of $x \in L$. However, for any x whether $x \in L$ or $x \notin L$, if a malicious prover provides an incorrect proof t', and the verifier always rejects, then we say $L \in$ NP.

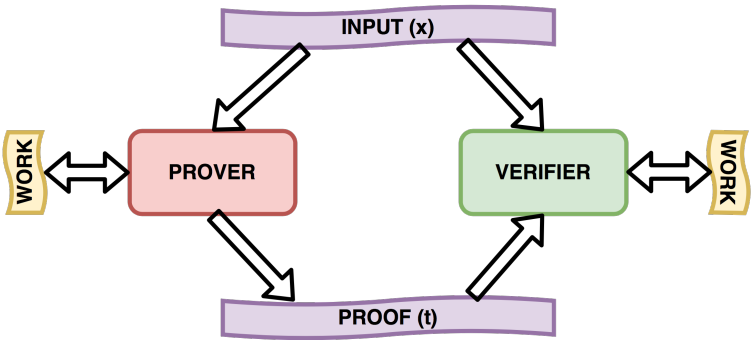


Figure 2.1: Proof System for NP

Next we introduce interaction in proof systems with two definitions published in 1985 independently [Bab85; GMR89]. But before we do that, imagine that the Prover and Verifier have a back-and-forth interaction, but the verifier is a deterministic TM, we will sketch why this is equivalent to NP. To see this, imagine the verifier deterministically decides on a first question and sends it to the prover, the prover provides an answer, then the verifier deterministically generates the next question (whether based on the prover's answer or not), and sends it again to the prover which proceeds to send back an answer. Imagine this happens for a polynomial number of rounds (since our verifier is a polytime machine and cannot go longer by definition). If you were this prover and you were all powerful, you could just simulate the verifier, generate their first question, figure out what they would ask given your answer to the question you generated, then simulate the verifier to generate the next questions and so on till you have a transcript filled with this interaction, and you can just begin by sending the verifier this transcript, which they could verify that it was indeed what they were going to do (pictorially this is seen in Figure 2.2).

So to have hope at identifying a stronger proof system, randomness needs to be added in the mix.

Definition 2.2.17 (Bounded-Error Probabilistic Polynomial Time (BPP)). *The language L is said to be in* BPP *iff* $\exists$ *a probabilistic TM, $\mathcal{M}$, that runs in polynomial time on all inputs with:*

- *(Completeness)* $x \in L \implies Pr[\mathcal{M}(x) = 1] \geq 2/3$
- *(Soundness)* $x \notin L \implies Pr[\mathcal{M}(x) = 1] \leq 1/3$

Let us introduce some important notation before diving in the definitions of interaction.

Notation:

- Up till now the verifiers were deterministic, when considering probabilistic TMs for verifiers, we will call the verifier's machine in calligraphic letters, say $\mathcal{V}$. The set of all such verifier TMs will be denoted by blackboard bold-ing the TM name, so $\mathbb{V}$. We will use V to denote a random variable over the coin tosses of the verifier's probabilistic TM. This extends beyond just the verifiers and the letter V.
- Let $\mathcal{P}$ and $\mathcal{V}$ be the prover and verifier's machines, and k be the number of rounds of interaction between them, then we define $\mathcal{P}(x) \overset{k}{\longleftrightarrow} \mathcal{V}(x)$ to denote the interactions in the k-rounds between the prover and verifier or until the end of the proof. $\langle \mathcal{P}_1, \mathcal{P}_2 \rangle (x) \overset{k}{\longleftrightarrow} \mathcal{V}(x)$ means $\mathcal{V}$'s interaction with $\mathcal{P}_1$ and separately with $\mathcal{P}_2$. $\langle \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a random variable denoting the joint event from $\mathcal{P}_1$ and $\mathcal{P}_2$ over their random coins.
- We define $\text{output}_{\mathcal{X}}(\mathcal{X}(a) \overset{k}{\longleftrightarrow} \mathcal{Y}(a))$ to be a random variable denoting the output of $\mathcal{X}$ when $\mathcal{X}$ interacts with $\mathcal{Y}$ on input a. If $\mathcal{X}$ is a verifier, then output 1 means accept.

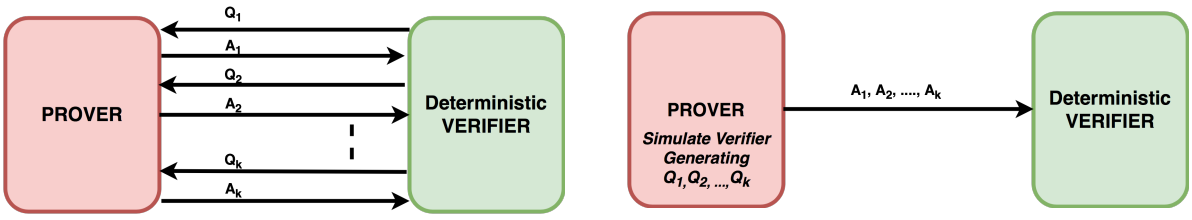
Definition 2.2.18 (Interactive Proofs (IP)). *A language L is said to be in* IP$[k]$ *if* $\exists$ *a deterministic polynomial-time TM $\mathcal{V}$ (the verifier) s.t. given the problem instance x, generated randomness tape r for $\mathcal{V}$, and some prover $\mathcal{P}$ interacting with $\mathcal{V}$ for $k(|x|)$ rounds, for some polynomial time computable function $k : \mathbb{N} \to \mathbb{N}$, $\mathcal{V}$ runs in polynomial time in $|x|$ s.t.*

- *(Completeness)* $\exists \mathcal{P}$ *s.t if* $x \in L \implies Pr[output_{\mathcal{V}}(\mathcal{V}(r, x) \overset{k}{\longleftrightarrow} \mathcal{P}(x)) = 1] \geq 2/3$
- *(Soundness)* $\forall \mathcal{P}$ *s.t. if* $x \notin L \implies Pr[output_{\mathcal{V}}(\mathcal{V}(r, x) \overset{k}{\longleftrightarrow} \mathcal{P}(x)) = 1] \leq 1/3$

where the probabilities are taken over the prover and verifier's coin tosses.

Then we define $\boxed{\text{IP} := \cup_{c \geq 1} \text{IP}[|x|^c]}$.

In figure 2.3, the prover can be thought of as an all-powerful TM, and the verifier is a TM with read-once-access to a randomness tape. Both the prover and the verifier read



(a) Deterministic Interactive Proof

(b) Unrolling of Deterministic Interaction

Figure 2.2: Equivalence of Deterministic Interaction and NP

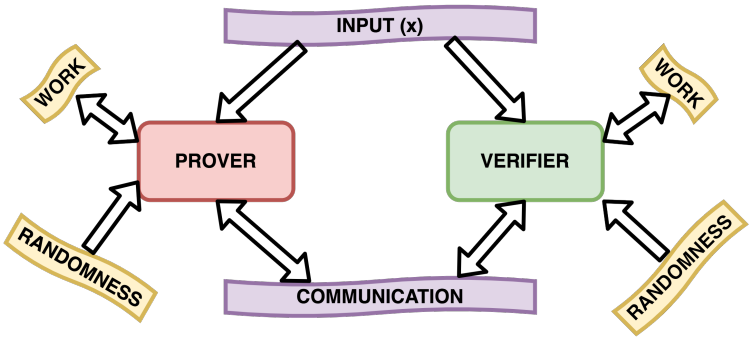


Figure 2.3: Proof System for IP

the input instance, x, from the input tape, then communicate back and forth over a shared communication tape. The verifier typically, but not necessarily, starts this interaction. Each TM has a read-write work tape to use. Many attempts try to restrict the verifier's powers (which up until now, was probabilistic polynomial-time Turing Machine). Restrictions classically included the amount of extra *space* used in verifying the proof, or restricting *time*, or allowing a number of *random bits* to be used by the verifier, or the number of *bits read from the prover's proof.*

Another variant of interactive proof systems was introduced by Babai called Merlin-Arthur (MA) and Arthur-Merlin (AM) systems. MA is similar to NP where you have a single interaction, but different in that Arthur, the verifier, is allowed to use randomness. The main difference between AM and IP, is that the prover (here called Merlin) can see the verifier (Arthur)'s random bits (see figures 2.4 and 2.5).

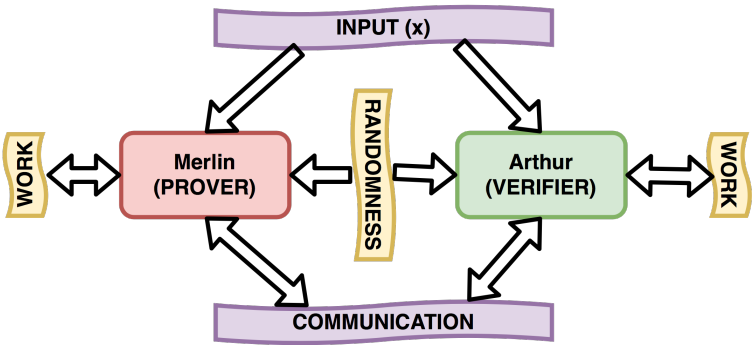
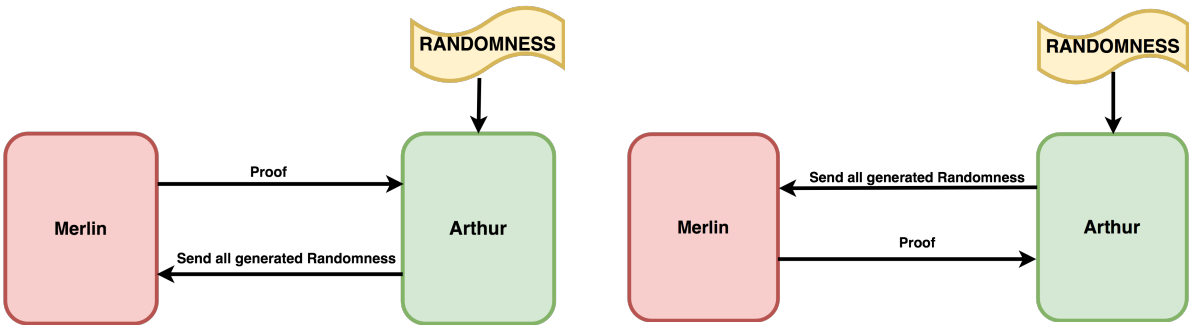


Figure 2.4: Proof System for AM

Definition 2.2.19 (Merlin-Arthur (MA))**.** *A language L is said to be in* MA *if $\exists$ a deterministic polynomial time TM $\mathcal{A}$ representing Arthur (the verifier) and polynomials T (bounding the length of prover Merlin's proof) and R (bounding the number of randomness bits given to Arthur) s.t. $\forall$ inputs x, we have:*

- *(Completeness) If $x \in L$, $\exists$ a proof $t \in \{0,1\}^{T(|x|)}$ s.t. $Pr_{r \in \{0,1\}^{R(|x|)}}[\mathcal{A}(x,t,r) = 1] \geq 2/3$*



(a) Merlin-Arthur Protocol (b) Arthur-Merlin Two Round Protocol

Figure 2.5: MA vs. AM

- *(Soundness) If* $x \notin L$, $\forall$ *proofs* t, $Pr_{r \in \{0,1\}^{R(|x|)}}[\mathcal{A}(x,t,r) = 1] \leq 1/3$

A small note on MA, is that, as in Figure 2.5, we make Arthur send his randomness to Merlin after Merlin sends the proof. This is for rigor and completeness purposes, to seamlessly allow extending the class MA to MA$[k]$ with k-rounds of interaction, however, this is beyond the scope of this document.

Definition 2.2.20 (Arthur-Merlin (AM))**.** *A language* L *is said to be in* AM *if* $\exists$ *a deterministic polynomial time TM* $\mathcal{A}$ *representing Arthur (the verifier) and polynomials* T *(bounding the length of prover Merlin's proof) and* R *(bounding the number of randomness bits given to Arthur) s.t.* $\forall$ *inputs* x*, we have:*

- *(Completeness) If* $x \in L$, $\exists$ *a proof* $t \in \{0,1\}^{T(|x|)}$ *s.t.* $Pr_{r \in \{0,1\}^{R(|x|)}}[\mathcal{A}(x,t,r) = 1] \geq 2/3$
- *(Soundness) If* $x \notin L$, $\forall$ *proofs* t, $Pr_{r \in \{0,1\}^{R(|x|)}}[\mathcal{A}(x,t,r) = 1] \leq 1/3$

Let AM$[k]$ denote the number of rounds of back and forth between Arthur and Merlin, before Arthur decides to accept or reject. Here AM = AM[2], and recalling Figure 2.2, it was shown in [BM88] that AM$[k]$ = AM[2] for any constant k. As to how MA and AM relate to NP and IP, we said that NP $\subseteq$ MA, and

$$\mathsf{AM} \subseteq \mathsf{AM}[\text{polytime}(|x|)] = \mathsf{IP}$$

With most of the community believing that AM $\subsetneq$ IP. However, it is proven in [GS86] that

$$\forall k \geq 1,\ \mathsf{IP}[k] \subseteq \mathsf{AM}[k+2]$$

This gives us the following (which is depicted in Figure 2.19):

$$\mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{AM} \subseteq \mathsf{IP}$$

Recalling the definition of the complexity class PSPACE.

Definition 2.2.21 (Polynomial Space (PSPACE)). *A language L is said to be in* $\mathsf{PSPACE}[S(n)]$ *if* $\exists$ *a deterministic TM that can recognize membership of* $x \in L$ *using a work tape of size* $S(|x|)$ *for some function* $S : \mathbb{N} \to \mathbb{N}$.

Then we have $\mathsf{PSPACE} = \cup_{c \geq 1} \mathsf{PSPACE}[|x|^c]$

We have the seminal result in the field of proof systems stating:

Theorem 2.2.1 ($\mathsf{IP} = \mathsf{PSPACE}$). *[Sha92]*

We are now ready to introduce an extension to IP giving us a more powerful proof system developed in 1999 by [Ben+88]. The extension is to increase the number of provers. It should be obvious that since the single prover was considered all-powerful in IP, increasing provers naively will not help recognizing more languages. The idea here (and this is important) is to make the multiple provers unable to communicate. First we define a multi-prover interactive proof system as in Figure 2.6, here we have $n \in \mathbb{N}$ provers and a single probabilistic polynomial-time TM representing the verifier. Before the interaction starts, the provers can cooperate and communicate to decide on an optimal strategy,[3] that is possibly hidden from the verifier[4], however, once they start interacting with the verifier (this strategy is represented by the common shared read-only infinite tape containing randomly generated bits), the verifier can send various questions to these non-communicating provers and can play the provers against one-another, hence verifying proofs to stronger languages.

Definition 2.2.22 (Multi-Prover Interactive Proofs (MIP)). *Let* $k : \mathbb{N} \to \mathbb{N}$ *be a polynomial time computable function denoting the number of rounds needed for each input size. A language* L *is said to be in* $\mathsf{MIP}[n]$ *if* $\exists$ *a deterministic polynomial-time verifier* $\mathcal{V}$ *s.t. given a problem instance* x*, generated randomness tape* r *for verifier,* n*-non-communicating-provers* $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_n$ *sharing an infinite read-only random tape, and* $\forall i(\ 1 \leq i \leq n)$, $\mathcal{P}_i \overset{k(|x|)}{\longleftrightarrow} \mathcal{V}$, *we have:*

- *(Completeness) If* $x \in L \implies \exists\ \mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_n$,

$$Pr[output_{\mathcal{V}}(\langle \mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_n \rangle (x) \overset{k}{\longleftrightarrow} \mathcal{V}(r, x)) = 1] \geq 2/3$$

- *(Soundness) If* $x \notin L \implies \forall\ \mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_n$,

$$Pr[output_{\mathcal{V}}(\langle \mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_n \rangle (x) \overset{k}{\longleftrightarrow} \mathcal{V}(r, x)) = 1] \leq 1/3$$

We say $\boxed{\mathsf{MIP} = \cup_{n \geq 1} \mathsf{MIP}[n] = \mathsf{MIP}[2]}$

The final equality was established in the original paper stating that having more than two provers in this setting does not help you.

[3] Strategy is defined in the Game Theory section. Informally it refers to the shared randomness / quantum state between the provers. The exact algorithm applied using the shared resources and the input is public.

[4] useful in zero-knowledge proofs

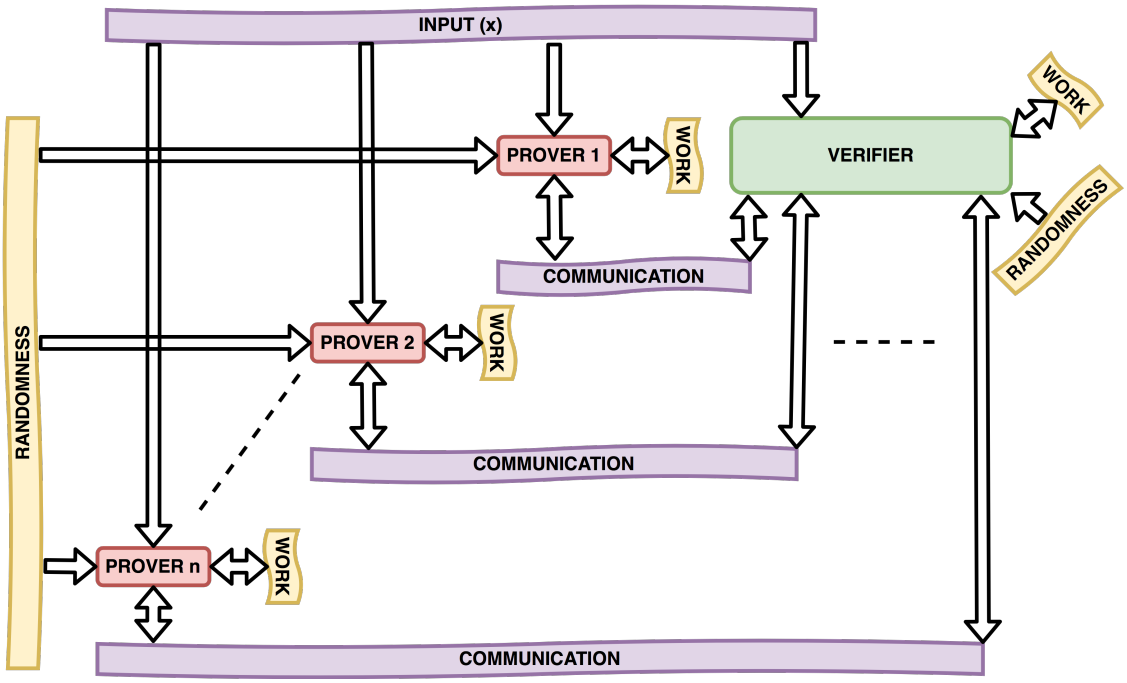


Figure 2.6: Proof System for MIP

Definition 2.2.23 (Exponential Time (EXP))**.** *A language L is said to be in* EXP *if* $\exists$ *a deterministic TM that can recognize membership of* $x \in L$ *in exponential-time* $O(\exp(|x|))$.

Definition 2.2.24 (Non-deterministic Exponential Time (NEXP))**.** *The set C is in the class* NEXP*, if* $\exists$ *a deterministic exponential-time verifier TM*[5]*,* V_C *s.t.*

- *If* $x \in C$*, then* $\exists t$ *with* $|t|{=}O(\exp(|x|))$ *and* $V_C(x,t) = 1$
- *If* $x \notin C$*, then* $\forall t$ $V_C(x,t) = 0$

Recalling the above definitions, we state this other seminal result:

Theorem 2.2.2 (MIP = NEXP)**.** *[BFL91]*

Theorems 6.1 and 6.2 showed that using variations of interaction can actually enable us to prove very complicated languages. Soon after these theorems were proven, scientists tried to restrict the verifier's *powers* in IP systems. Whether limiting the verifier's allotted *space*, *time*, number of *random bits*, or the number of *bits read from the prover's proof*. This led to a series of results culminating in 1998 by introducing *probabilistically checkable proof* systems (PCP's) [AS98] restricting both random bits and number of bits read from the proof, and yielding the amazing PCP-theorem.

Definition 2.2.25. PCP$[r(n), q(n)]$ *is the class of languages having proofs that can be verified in polynomial time by a probabilistic TM in input size n using $O(r(n))$ bits of randomness, querying $O(q(n))$ bits in the proof, and having completeness 1 and soundness 1/2.*

[5] i.e. Recognizing languages in EXP.

Theorem 2.2.3 (PCP Theorem). $\mathsf{NP} \subseteq \mathsf{PCP}[\log n, 1]$, *[Aro+98; Din07]*

Finally, let us define the class of Recursively Enumerable that will be used in later sections.

Definition 2.2.26 (Recursively Enumerable RE). *A language L is said to be in* RE *iff it is Turing-Recognizable.*

Definition 2.2.27 (HALT). *The decision problem of whether a TM, $\mathcal{M}$, terminates on some input x or runs forever.*

Turing famously showed that HALT is not Turing Decidable [36].

Theorem 2.2.4 (HALT is RE-complete).

With this we finish our survey of the main proof systems and classes in classical complexity theory. The main outcome we hope the reader extracts from this survey is two-fold:

1. Choosing the precise definition for a new proof system is important and non-trivial.
2. Seemingly slight modifications to a proof system can make it vastly stronger or weaker.

2.3 Quantum Mechanics

While we would love to give the reader a full walk-through of quantum mechanics (QM), it will easily exceed the page limit of this thesis. Instead, we cover the basic 4 postulates of QM and the immediate definitions needed to understand them, and refer the reader to [NC02] for an overview of all the quantum mechanics needed for the field of quantum information (mainly 2-level systems), and any quantum mechanics textbook for a general understanding of the physics.

Definition 2.3.1 (Hilbert Space). *A complex inner product vector space.*

Most of the time we will only be considering finite dimensional Hilbert spaces. We denote objects in a Hilbert space using Dirac notation.

Definition 2.3.2 (Dirac Notation).

- *A vector in a Hilbert space $\mathcal{H}$ is denoted by the ket $|v\rangle \in \mathcal{H}$ where v is a label for this vector.*
- *The complex conjugate of a ket $|v\rangle$ is called a bra and is written as $\langle v| = |v\rangle^\dagger$, where $\dagger$ is the complex Hermitian conjugate.*
- *The inner product of two kets $|u\rangle, |v\rangle \in \mathcal{H}$ is denoted by the bra-c-ket $\langle u|v\rangle$.*
- *The norm squared of a ket, $|v\rangle$, is $||v||^2 = \langle v|v\rangle$.*
- *An operator A is a linear map $A : \mathcal{H} \to \mathcal{H}$ i.e. $|v\rangle \in \mathcal{H}$ we have $A|v\rangle \in \mathcal{H}$.*
- *The Lie Bracket associated with $\mathcal{H}$ is the commutator of operators A and B s.t. $[A, B] = AB - BA$.*

- *Hermitian operators, A, are operators that obey $A = A^\dagger$.*
- *Projectors are Hermitian operators, P, that further obey $P^2 = P$.*
- *Unitary operators, U, are operators that obey $UU^\dagger = U^\dagger U = I$.*

Postulate 2.3.0.1 (Quantum States)**.** *A closed quantum system is represented by a Hilbert space, $\mathcal{H}$, known as a state space, which is fully described by a state vector, $|\psi\rangle \in \mathcal{H}$ with $||\psi|| = 1$.*

Definition 2.3.3 (Quantum Bits (Qubits))**.** *A qubit is the simplest quantum system and is represented by a 2-dimensional Hilbert space $\mathcal{H}$. A canonical basis spanning $\mathcal{H}$ is $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Hence, any arbitrary state vector $|\psi\rangle \in \mathcal{H}$ can be written as $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ are called probability amplitudes constrained that $|\alpha|^2 + |\beta|^2 = 1$.*

It is important to note here that although the probabilities are the square of the coefficients (called amplitudes), adding qubits to one another or multiplying them, could allow these amplitudes to cancel out since they are complex numbers (destructive interference) or add up increasing their probability (constructive interference).

Throughout this section, we will try to make simple examples to visualize the definitions presented, and because we cannot plot a 2-dimensional complex vector space, we will use the special case where a qubit has real amplitudes (i.e. $\mathbb{R}$ vector space). We start with a qubit, which one could think of as a vector in the x-y plane represented as in Figure 2.8, here $a^2 + b^2 = 1$. However, the realistic picture of a qubit is what is known as a Bloch Sphere (see Figure 2.7), but it is more challenging to use in giving intuition to the novice reader.

Definition 2.3.4 (Superposition)**.** *If $\alpha \neq 0$ and $\beta \neq 0$ then we say $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is in a superposition of logical zero $|0\rangle$ and logical one $|1\rangle$. (see Figure 2.8)*

Postulate 2.3.0.2 (Quantum Evolution)**.** *A closed quantum system, $|\psi_{t=0}\rangle$, evolves according a unitary operator U (for time T) to reach the (new) state $|\psi_{t=T}\rangle$ written as $|\psi_{t=T}\rangle = U|\psi_{t=0}\rangle$. (see Figure 2.9)*

Postulate 2.3.0.3 (Quantum state composition)**.** *The state space representing a composition of multiple (possibly interacting) closed quantum systems is defined by the tensor product of the state spaces of the individual quantum systems, and is written as the product state $|\psi_1\rangle \otimes |\psi_2\rangle$, where $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ and dimension $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is the product of their dimensions (see figure 2.10).*

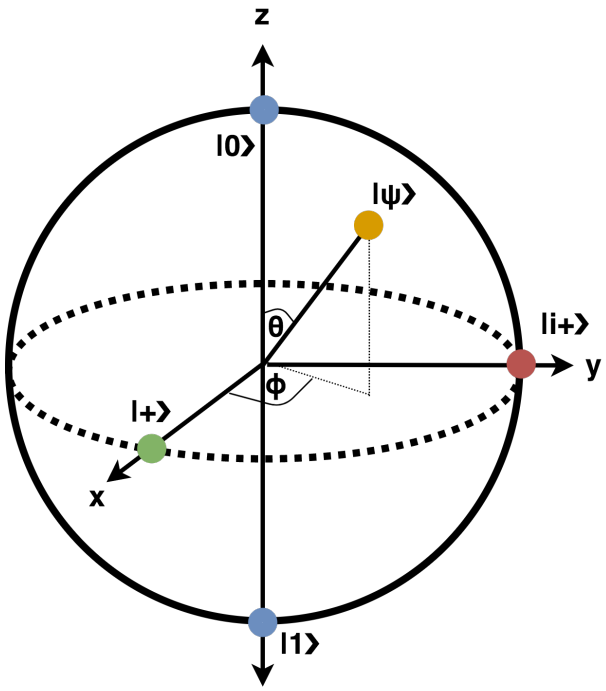


Figure 2.7: A Bloch Sphere showing, the 3 basis typically used when describing a qubit $\{|0\rangle,|1\rangle\}$, $\{|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, and $\{|i\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)\}$, and the generic qubit $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$. Here the positive and negative directions of each axis are orthogonal vector in the 2-dimensional Hilbert space.

Definition 2.3.5 (Quantum Entanglement)**.** *We say a quantum state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is entangled if it cannot be decomposed/factored into a tensor product of constituents of the sub-systems $\mathcal{H}_1$ and $\mathcal{H}_2$, namely $\forall\ |\psi_1\rangle \in \mathcal{H}_1$, $|\psi_2\rangle \in \mathcal{H}_2$*

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$$

There are four famous entangled states (Table 2.1) that together form an orthonormal basis on the Hilbert space of two qubits.

Theorem 2.3.1 (No-Cloning Theorem)**.** *Creating an identical copy of an arbitrary unknown quantum state without destroying the original is impossible.*

We can also consider an statistical ensemble/mixture of quantum states $|\psi_i\rangle$ as follows:

Definition 2.3.6 (Density Matrix)**.** *Let $\{|\psi_i\rangle\}$ be a finite set of quantum (pure) states of size n, and let p_i be a probability distribution over the $|\psi_i\rangle$'s. We define a density matrix representing our statistical mixture of our quantum states (or mixed state) as:*

$$\rho = \sum_{i\in[n]} p_i\,|\psi_i\rangle\,\langle\psi_i|$$

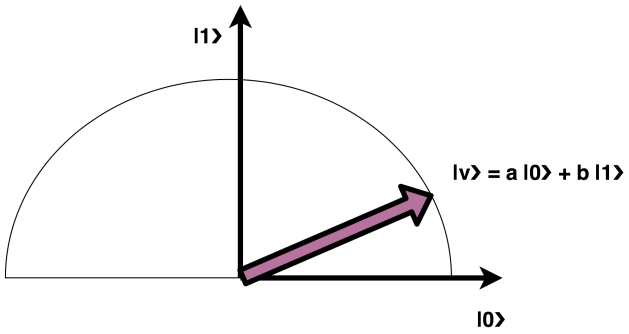


Figure 2.8: A example qubit $|v\rangle$ that is a superposition of $|0\rangle$ and $|1\rangle$ with $a > b$

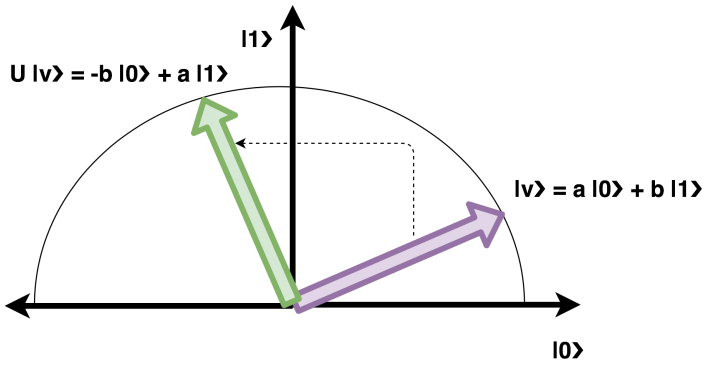


Figure 2.9: Applying the unitary $U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ to the qubit $|v\rangle$ that rotates the qubit by $\pi/2$ CCW making it more likely to collapse to $|1\rangle$ if measured in the $(|0\rangle, |1\rangle)$ basis

Then the density matrix of part of the system is given by the partial trace.

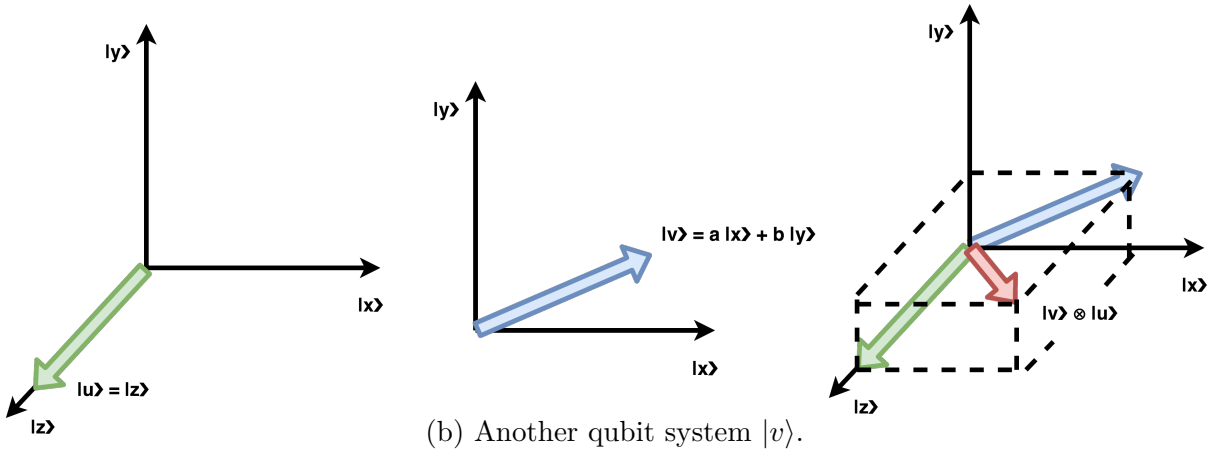
Definition 2.3.7 (Partial Trace)**.** *Let ρ_{AB} be a density matrix on the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, and let $\{|b\rangle\}$ be a set of orthonormal basis for $\mathcal{H}_B$, then we define the partial trace to be:*

$$\mathrm{Tr}_B[\rho_{AB}] = \rho_A = \sum_{\forall b} \langle b| \rho_{AB} |b\rangle$$

Postulate 2.3.0.4 (Quantum Measurement)**.** *An open quantum system, $|\psi_{\mathrm{Pre}}\rangle$, interacts with the rest of the world in non-unitary evolution. Let us model this external system interacting with our quantum system by a collection of measurement operators (for our purposes these will be projectors) $\{M_b\}$ where b represents the measurement outcome and $\sum_b M_b^\dagger M_b = I$. The result of this interaction is the collapse of $|\psi_{\mathrm{Pre}}\rangle$ to*

$$|\psi_{\mathrm{Post}}\rangle = \frac{M_b |\psi_{\mathrm{Pre}}\rangle}{\sqrt{\langle\psi_{\mathrm{Pre}}| M_b^\dagger M_b |\psi_{\mathrm{Pre}}\rangle}}$$

for a specific b, where the probability for any particular b, $Pr[b] = \langle\psi_{\mathrm{Pre}}| M_b^\dagger M_b |\psi_{\mathrm{Pre}}\rangle$



(a) A qubit system $|u\rangle$.

(b) Another qubit system $|v\rangle$.

(c) A composition of both systems $|v\rangle \otimes |u\rangle$.

Figure 2.10: In this example visualizing composition of closed quantum systems, $|u\rangle$ is completely in the direction of the canonical basis $|z\rangle$, while $|v\rangle$ lives in the (x-y) state space. When studying both systems collectively, and only visualizing the relevant 3-dimension subspace, gives the state vector $|v\rangle \otimes |u\rangle$ in the higher dimensional space.

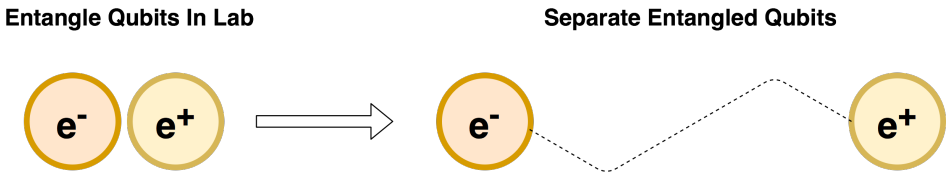


Figure 2.11: On the left we create $|e^-\rangle \otimes |e^+\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$, this state cannot be factored, and as we separate the individual particles, measuring one will result in an instantaneous collapse of the other to the same resultant basis vector!

As mentioned we will be concerned with a special case of measurement represented by projective operators. Here the projectors project the quantum state onto a specific basis for the Hilbert space $\mathcal{H}$. For those familiar with the spectral theory, this basis is the eigenvectors of a Hermitian operator on $\mathcal{H}$ which span $\mathcal{H}$. The b here would be the associated eigen-value. Hence, Hermitian operators are said to be observables, because they measure the quantum state collapsing it to a specific eigenvector, making the state not in a superposition of basis-states since the eigenvectors are the basis that span the Hilbert space. (see figure 2.12).

A common concept introduced at this point is that of *Realism*, which will be needed when discussing Bell's Theorem.

Definition 2.3.8 (Realism)**.** *The idea that nature exists independent of an observer.*

Realism is particularly contested when considering the weird laws quantum measurement and its implications. Quantum mechanics suggests that the measurement outcome of a

Table 2.1: The four Bell Basis states represent the simplest maximally entangled two qubit systems

Symbol	Expansion in Tensor Product of Canonical Basis
$\|\Phi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} + \|11\rangle_{AB}\right)$
$\|\Phi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|00\rangle_{AB} - \|11\rangle_{AB}\right)$
$\|\Psi^+\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} + \|10\rangle_{AB}\right)$
$\|\Psi^-\rangle$	$\frac{1}{\sqrt{2}}\left(\|01\rangle_{AB} - \|10\rangle_{AB}\right)$

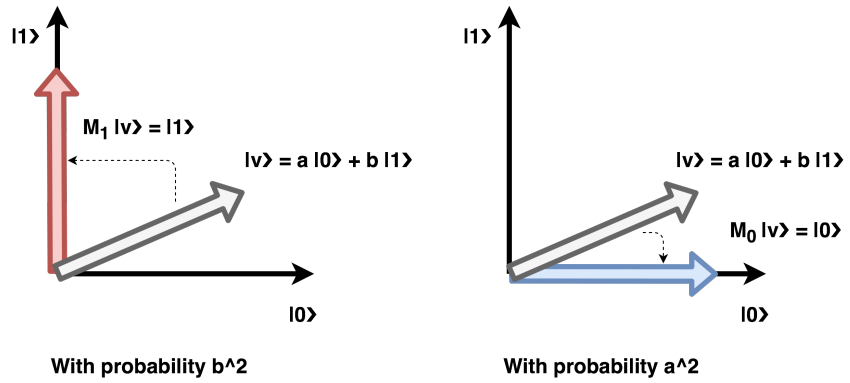


Figure 2.12: When applying the projective measurement ($|0\rangle\langle 0|$, $|1\rangle\langle 1|$) on the qubit in Figure 2.8, it collapses the state to either the left or right figure, and since $a^2 \gg b^2$, measuring a $|0\rangle$ is more probable.

quantum system does not exist prior to observing the system, and it becomes a reality only when observed. That is, if you don't measure the position of an electron then the electron does not actually have a position. Only when the position is measured / observed, does the electron exhibit being in a location. Realism opposes that view, suggesting that the position of an unobserved electron exists all the time.

2.4 Relativity

To understand terms used like signalling or lack thereof, causality, space-time diagrams and a few others, we will need to cover Einstein's special theory of relativity, namely its two main postulates. A cultural classic covering the topic is Einstein's book [Ein19].

Definition 2.4.1 (Frame of Reference)**.** *A frame of reference is a coordinate system, relative to which physical properties are measured.*

Definition 2.4.2 (Inertial Frame of Reference)**.** *An inertial frame of reference is a reference frame (called the observer's inertial reference frame) in which a body at rest remains at rest*

and a body in motion moves at a constant speed, v_{body}, in a straight line unless acted on by an outside force.

This body could equivalently be studied in another inertial frame of reference (denoted by primed variable). This new inertial frame of reference is the coordinate system with the body at the origin at rest and the observer frame is moving with a constant velocity $v'_{\text{frame}} \geq 0$ in the opposite direction $v'_{\text{frame}} = -v_{\text{body}}$.

Postulate 2.4.0.1 (The Principle of Relativity)**.** *The laws of nature are the same for all inertial frames of reference.*

Postulate 2.4.0.2 (Invariance of the Speed of Light c)**.** *The speed of light (or any mass-less particle for this matter) c is a constant, independent of the relative motion of the source.*

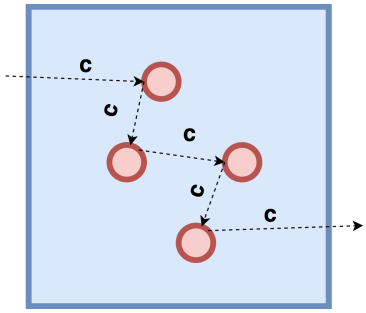


Figure 2.13: Speed of light appears to be slowed down in non-vacuum due to bumping around particles in the medium, but a photon always moves with velocity c.

Definition 2.4.3 (No Faster than Light Signalling)**.** *Also known as the* ***no-communication theorem****, states that information (and even physical effects) cannot travel from one place to another faster than the speed of Light.*

This is particularly relevant in understanding that although effects of measurement of entangled quantum states appear instantaneous, two parties cannot communicate information faster than the speed of light using these correlation effects.

Going back to the MIP complexity class definition 2.2.22 where the provers were not allowed to communicate, and considering how to practically implement a multi-prover interactive proof system, we must ensure that throughout the duration of the provers interaction with the verifier, they were separated by a "distance" that would not be enough for light (information) to travel between them. To understand some of the complications needed to be considered to separate these provers consider these two direct phenomena resulting for the two postulates above.

Definition 2.4.4 (Time Dilation)**.** *Imagine you are in the observer inertial reference frame. A clock, T_{Moving}, in a relatively moving frame (with velocity $v < c$) will be seen to be running slower than a clock in your inertial frame T_0.*

$$\Delta T_{\text{Moving}} = \Delta T_0 / \sqrt{1 - v^2/c^2}$$

Definition 2.4.5 (Length Contraction)**.** *Imagine you are in the observer inertial reference frame. The length of any object, L_{Moving}, in a relatively moving frame (with velocity $v < c$) will be seen to be compressed in the direction of motion $\vec{v}$.*

$$L_{\text{Moving}} = \sqrt{1 - v^2/c^2} \times L_0$$

Definition 2.4.6 (Event)**.** *An instantaneous physical occurrence associated with a point in space-time. For an event A, let A_x be its space coordinate value, and A_t be its time coordinate value in a particular reference frame (x, t).*

Definition 2.4.7 (Time-Like Separation of Events)**.** *Events A and B are time-like separated iff:*

- *$\exists$ a frame[6] of reference s.t. A and B occur at the same spacial location ($A_x = B_x$).*
- *$\forall$ frames of reference, A and B never occur at the same time ($A_t \neq B_t$).*

A direct consequence of the second bullet-point above, is that for time-like events, A and B, if $A_t < B_t$ in reference frame $(x, t) \implies \forall$ reference frames (x', t'), $A_{t'} < B_{t'}$, because in order for them to flip, requires that in some frame they had occurred at the same time.

Definition 2.4.8 (Space-Like Separation of Events)**.** *Events A and B are space-like separated iff:*

- *$\exists$ a frame[7] of reference s.t. A and B occur at the same time ($A_t = B_t$).*
- *$\forall$ frames of reference, A and B never occur at the same place ($A_x \neq B_x$).*

Definition 2.4.9 (Space-Time Diagram)**.** *A 2-dimensional plot representing events happening in 1 space direction x (horizontal axis) as time (vertical axis) progresses relative to an observer O at the origin.*

Definition 2.4.10 (Light Cone)**.** *It is the path that a beam of light emanating from an event E and traveling in all directions would take through space-time.*

Here directions also include the temporal direction, where all events that can be reached from E (called the future light cone), and all those that could've sent a beam of light to E (called the past light cone).

If a space-time diagram included 2-spacial coordinates instead of one (i.e. a horizontal spacial plane) then the light cone would be a double cone with the apex at the origin and its axis being the vertical temporal axis. In regular Space-Time diagrams, the light cone represents the 45^o lines.

Some observations from Figure 2.14:

[6] The frame will have the line connecting A and B as its time-axis

[7] The frame will have the line connecting A and B as its space-axis

- In an inertial reference frame, light beams are the 45^o straight lines.
- Events inside the light cone (with slope larger than 45^o), like the green events A and B, are time-like separated from O.
- Events outside the light cone (with slope smaller than 45^o), like the red event C, are space-like separated from O.
- Time-Separated events obey causality, namely because $A_t < B_t$, we say event B *could have been* caused by event A.
- Event D in the backward cone from our observer O is guaranteed to have happened in the past relative to O in all frames of reference.
- The path $O \to A \to B$ could represents a moving object at a speed slower than c that gets reflected at distance A_x and bounces back to O_x.

Recalling definition 2.3.5 and Figure 2.11, we say this "spooky action at a distance" of entanglement is called *a non-local action.*

Definition 2.4.11 (The Principle of Locality)**.** *For event A to affect time-like separated event B, there has to be a series of local adjacent effects (non-leaping) happening all the way from $A \to B$. Hence, physical influences propagate continuously through space at speed $\leq c$.*

Entanglement is non-local because its effect is time-independent, however from definition 2.4.3 we know this effect cannot transmit information faster than light, it just allows correlations between distant space-like separated parties using entanglement.

Definition 2.4.12 (Causality)**.** *If two events are causally connected (aka the time between them is smaller than (*the distance between them$/c$*)), then their precedence order is preserved. Causality occurs between an effect and an event, if the event is in the back-light-cone of the effect, or if the effect is in the front-light-cone of the event.*

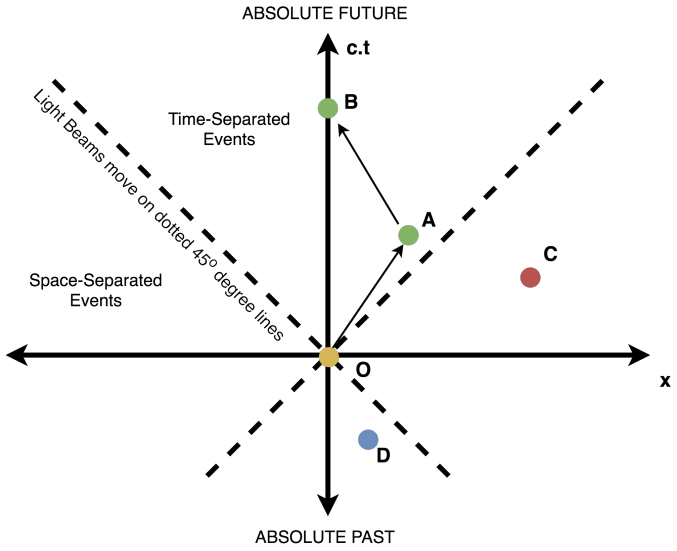


Figure 2.14: Space-Time Diagram Illustrative Example

2.5 Information Theory

For information theory, we recommend reading Shannon's seminal 1948 paper [Sha01] to understand almost the entire field. Here we will understand, without proofs, what a channel is and how different channels transfer a classical or quantum bit of information. For further reading, we found [Wit20] and Preskil's lecture notes helpful.

Definition 2.5.1 (A Communication System)**.** *A Communication System is defined loosely by the triple* ⟨Information Source, Channel, Information Destination⟩ *where:*

- ***Information Source:*** *produces a message to be communicated to the receiving party. This message could be analogue or digital, it could be a (sequence of) qubit(s) or classical bit(s). A transmitter possibly converts / compresses / encodes this message to be more suitable to transfer over a medium.*
- ***Communication Channel:*** *It is the medium which carries the information. This could include a cable / fiber wire or a beam of quantum particles (ions / photons / electrons / etc). This medium is possibly noisy, which means that our signal sent through it could be damaged or completely destroyed.*
- ***Information Destination:*** *receives the possibly damaged / destroyed message / signal, and tries to figure out the original message with a possibility of failure / misunderstanding.*

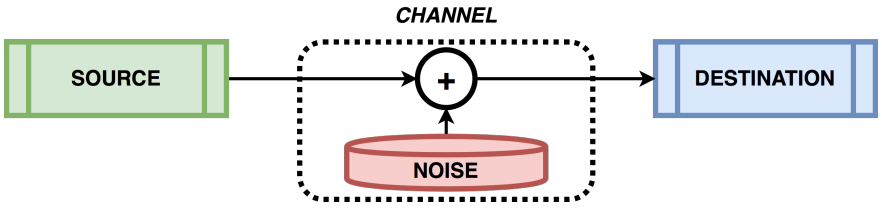


Figure 2.15: A Schematic of a simple Communication System

Notice that if a communication channel was noiseless then whatever message was to be transmitted would be received as is with no issue. The rate of information transfer would be obviously limited by the speed of light, but also by the encoding of the message. For example, instead of encoding each symbol with the same number of (qu)bits, we could label the most frequently used letters by fewer bits and the less used symbols by a longer bit string, this would lead to more information content received per same number of bits sent on average. Formally characterizing possible encodings and noise is done by introducing the notion of the Entropy of an information source.

2.5.1 Shannon Information Theory

Definition 2.5.2 (Noisy Channel (Mathematical))**.** *Let X be a random variable denoting the message sent through the channel, and let Y be a random variable denoting the message*

received on the other end. Then the classical (noisy) communication channel is modelled by a conditional probability.

$$Pr[Y \mid X = x]$$

$Pr[Y \mid X = x]$ means "if the message sent was x, then the message received follows a probability distribution based on the noise." Moreover, it is possible to increase the size of the message through an encoding scheme to allow detection and correction of errors made by the channel due to the noise.

Definition 2.5.3 (Shannon Entropy)**.** *For a random variable X over possible values, x_i and $i = 1, .., n$[8], with an associated probability distribution $p(x_i)$, then we denote by the entropy $H(X)$ the expected uncertainty with any given outcome or the expected number of incompressible bits of information carried per x_i.*

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2(p(x_i))$$

The Shannon entropy is non-negative.

$$\forall\ X,\ H(X) \geq 0$$

For two random variables X and Y (for our purposes we can think of them representing the source messages and the received messages respectively) with joint probability distribution $p(x_i, y_i)$ and the conditional probability $p(y_i \mid x_i)$, we can define ***the joint entropy*** $H(X, Y)$ (signifying the amount of uncertainty of both messages) and ***the conditional entropy*** $H(Y \mid X)$ (signifying the remaining uncertainty in Y after knowing what X was). A simple derivation shows that:

$$H(Y \mid X) = H(X, Y) - H(X)$$

and because entropy is non-negative, we get

$$H(X, Y) \geq H(X)$$

Definition 2.5.4 (Mutual Information)**.** *For two random variables X and Y, the mutual information $I(Y; X)$ is the amount of information gained (or uncertainty lost) about Y by observing X.*

$$\begin{aligned} I(Y; X) &= H(Y) - H(Y \mid X) \\ &= H(Y) + H(X) - H(X, Y) \end{aligned}$$

Clearly $I(Y; X) \geq 0$ (this is called the subadditivity of Shannon Entropy). Less obviously, this next inequality (called strong subadditivity) also holds:

$$H(X, Y) + H(Y, Z) \geq H(Y) + H(X, Y, Z)$$

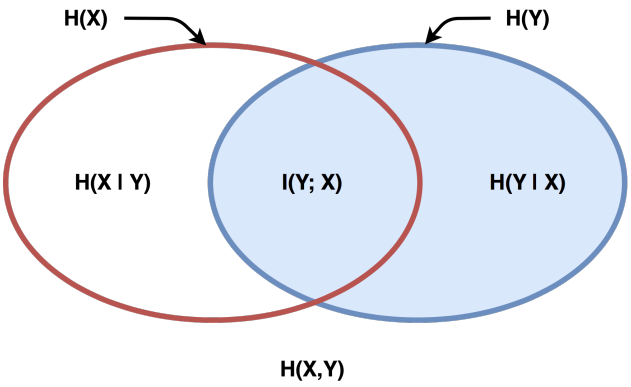


Figure 2.16: Venn Diagram visualizing the various Entropies introduced and their relation to mutual information for illustration purposes only.

Definition 2.5.5 (Channel Capacity)**.** *Let the random variables X and Y describe the information source and received messages respectively for a (noisy) communication channel. We denote by the upper bound on the rate of transfer of information through this channel by its capacity C s.t.*

$$C = \sup_X \ I(Y;X)$$

Hence we can never transfer information at a rate $R > C$. Moreover, if $C = 0$ then no information can transfer between source and destination and we say they cannot signal (communicate with) one another. However, if the capacity is $C > 0$, then it could be **amplified** by repetition (sending message multiple times), or more generally error detecting / correcting codes.

Definition 2.5.6 (Classical Communication Channel (practical))**.** *Le A and B label the two endpoints of a channel, and X_i be a random variable over the possible messages sent by the party at $i \in \{A, B\}$, and let Y_j be a random variable over the messages that could be received by party $j \in \{A, B\}$. Then a classical communication channel is defined by*

$$Pr[Y_A \mid X_B = x] \text{ and } Pr[Y_B \mid X_A = x]$$

and if both distributions are identical we say it is a symmetric channel.

What is important here is that communication channels cannot forbid one party from communicating to the other, unless the channel capacity in one direction is zero, hence a communication channel by definition is bi-directional for all practical purposes.

Finally we introduce *Relative Entropy* (sometimes called *Divergence*), which is important in comparing two probability distributions. Imagine a statistical experiment where we model

[8]For the rest of the Information Theory section, we will assume the random variable X is over outcomes in the set $\{x_i\}_{i=1,..,n}$ and random variable Y is over outcomes in the set $\{y_j\}_{j=1,..,m}$.

our source X with a probability distribution $q(x_i)$, however, we might be wrong, and the actual probability distribution modelling X was indeed $p(x_i)$. The question relative entropy answers is: how sure could we be that our initial hypothesis, $q(.)$, is wrong after observing N samples from the source X. In this experiment, the expected number of any x_i will be $p(x_i) \cdot N$, but since we believe $q(.)$ to be the actual probability, we know the number of sequences with $p(x_i) \cdot N$ occurrences of x_i is $\frac{N!}{\Pi_j (p(x_j) \cdot N)!} \approx |X|^{N \cdot H(X)}$, but we believe this sequence happens with probability $q(x_i)^{p(x_i) \cdot N}$. Hence the total probability of the outcome of our experiment will be:

$$\Pi_{i=1}^{n} q(x_i)^{p(x_i) \cdot N} |X|^{N \cdot H(X)} = |X|^{-N \sum_{i=1}^{n} p(x_i)(\log p(x_i) - \log q(x_i))}$$

Definition 2.5.7 (Relative Entropy / Kullback-Liebler (KL) Divergence)**.** *Given two probability distributions Q and P for the random variable X to take over a value x_i, then the relative entropy is defined as*

$$H(P_X || Q_X) = \sum_i p(x_i)(\log p(x_i) - \log q(x_i))$$

where $H(P_X || Q_X) \geq 0$ and equality when P is statistically equivalent to Q, and $H(P_X || Q_X)$ gets larger the more the initial hypothesis Q was far from the correct probability P.

2.5.2 Quantum Information Theory

Next we can extend these definitions to include quantum communication channels, each definition above has a quantum counterpart. To help the reader understand the difference, the key idea is quantum mechanics extends probability to a non-commutative setting, in which the notion of a joint / conditional probability distribution between events doesn't always have meaning, because this probability depends on the order and way in which these events are measured (see Table 2.2 for a complete description).

Definition 2.5.8 (Von Neumann Entropy)**.** *The analogy of Shannon Entropy extended to the quantum realm. For a quantum system represented by the density matrix ρ (which acts as a random variable among the pure quantum states of the system), we define the entropy $S(\rho)$ to be:*

$$S(\rho) = -\text{tr}[\rho \log(\rho)]$$

Shannon and Von Neumann Entropies are similar in many ways, but differ in a significant few. Table 2.3 contrasts the two. Note that conditional quantum entropy is misleading, because there is no good notion of conditional quantum probability as mentioned above.

A quantum channel in the simple case is modeled by a Unitary U, but more generally, we extend the sender's system ρ by the noise/environment system $\hat{\rho}_A \otimes |0\rangle \langle 0|$, where the environment is a Hilbert space of dimension k. This system evolves under U again, but the

received state

$$\hat{\rho}_B = U\hat{\rho}_A U^{-1} = \sum_i^k \sum_j^k E_i \hat{\rho}_A E_j^\dagger \otimes |i\rangle \langle j|$$

And the receiver then traces out the environment getting:

$$\rho_B = \mathrm{Tr}_{\text{Environment}}[\sum_i^k \sum_j^k E_i \hat{\rho}_A E_j^\dagger \otimes |i\rangle \langle j|] = \sum_i^k E_i \hat{\rho}_A E_i^\dagger$$

Definition 2.5.9 (Quantum Channel)**.** *A quantum channel maps an input state to an output state via the evolution*

$$\rho \to \sum_{i=1}^k E_i \hat{\rho} E_i^\dagger$$

where E_i is called a Kraus operator and $\sum_{i=1}^k E_i^\dagger E_i = I$. Obviously if $k = 1$ this reduces to unitary evolution.

2.6 Relationship between Quantum and Classical Channels

Theorem 2.6.1 (Quantum Channel $\implies$ Classical Channel)**.** *Any quantum channel $\mathcal{E}$ whatsoever can be used to transmit classical information, provided the channel is not simply a constant ($\forall\rho\ \exists\rho_{output}$ s.t. $\mathcal{E}(\rho) = \rho_{output}$).*

We will not prove theorem 2.6.1, it follows directly from the Holevo–Schumacher–Westmoreland (HSW) theorem and the proof could be found in [NC02].

We will now define the notion of entanglement distillation, then highlight how it can be used to create a quantum channel with positive capacity using two zero-capacity quantum channels.

Definition 2.6.1 (Entanglement Distillation)**.** *Let ρ be the density matrix representing a bi-partite quantum system belonging to Alice and Bob. They are supplied with a large number, m, of copies of these states. Entanglement distillation is the process of converting these states to the largest possible number, $n \leq m$, of Bell states with high fidelity using local operations and a (bi-directional) classical communication.*

Entanglement is considered a physical resource that can help with computation as we will see in 2.7. As such, entanglement distillation provides a way to determine the amount of entanglement in any state ρ thereby assigning it a measure of how valuable a resource it is. Showing a distillation protocol is beyond the scope of this document.

Let us demonstrate how to use entanglement distillation in sending quantum information over a noisy quantum channel, together with a noisy classical channel. Alice prepares m Bell

states $\frac{1}{\sqrt{2}}\big(|00\rangle_{AB} + |11\rangle_{AB}\big)$ and sends the second qubit to Bob over the noisy quantum channel. The resulting joint state between Alice and Bob could be distorted due to the noise and become m copies of ρ instead of the m Bell states (assuming the noise acts the same way on all states). Now, Alice and Bob use local operations on their m copies of ρ together with the classical communication channel to create n Bell states. Alice can use her half of a Bell state together with sending classical bits to Bob to teleport any quantum state $|\psi\rangle$ to Bob using Quantum Teleportation [Ben+93].

Definition 2.6.2 (Quantum Teleportation (informal))**.** *Given a classical channel, a shared Bell pair, $|\Phi^+\rangle_{AB}$, between sender Alice, and receiver Bob, a qubit $|\psi\rangle$ owned by Alice which she wishes to send to Bob. Alice measures her part of $|\Phi^+\rangle_A \otimes |\psi\rangle$ in the Bell basis and records the two classical bits produced by this measurement. She sends these classical bits to Bob over the classical channel. Bob uses these two bits to decide on a quantum operation to apply on $|\Phi^+\rangle_B$ to transform it to be $|\psi\rangle$.*

By theorem 2.6.1, as long as the quantum channel is not a constant channel (i.e. could have zero quantum capacity!), then having two such channels one from Alice to Bob and the other from Bob to Alice, they can send each other classical information through these quantum channels without needing any classical channel. Now using the quantum distillation and quantum teleportation as described above, we have all the ingredients to transfer a quantum state over two quantum channels, both with zero capacity!! This implies that with enough quantum channels parties can amplify zero quantum capacity to allow quantum transmission of information. **This is the only known way to amplify a zero capacity channel.**

Table 2.2: Probability Comparison

Classical Probability	**Quantum Probability**
Sample space (Ω)	Hilbert space ($\mathcal{H}$)
Joint of two sample spaces ($\Omega_1 \times \Omega_2$)	Tensor product of Hilbert spaces ($\mathcal{H}_1 \otimes \mathcal{H}_2$)
Union of two sample spaces ($\Omega_1 \cup \Omega_2$)	Direct sum of Hilbert spaces ($\mathcal{H}_1 \oplus \mathcal{H}_2$)
An random variable (X)	A Hermitian matrix (A)
An event (ω)	A density matrix (ρ)
The probability of event ω_k: $P(\omega_k)$	Trace of ρ on the k^{th} projector[9] of A: $\mathrm{Tr}(\rho P_k)$
Marginal $P(X \mid Y) = \sum_{y \in Y} P(X, Y)$	Partial trace $\mathrm{Tr}_B(\rho_{A,B})$
$\mathbb{E}[X] = \sum_k X(\omega_k) P(\omega_k)$	$\langle A \rangle_\rho = \mathrm{Tr}[\rho A]$[10]
$\mathrm{VAR}(X) =$ [11]$\mathbb{E}[X^2] - (\mathbb{E}[X])^2$	$\langle \Delta A \rangle_\rho =$ [12]$\mathrm{Tr}[(\rho A^2) - \langle A \rangle_\rho^2]$

Table 2.3: Entropy Comparison

Shannon Entropy	**Von Neumann Entropy**
$H(X) = 0$ with (certain events): $\exists i,\ p_i = 1$	$S(\rho) = 0$ with (pure states): $\forall \rho = \lvert\psi\rangle \langle\psi\rvert$
$H_n(p_1, .., p_n) \leq H_n\left(\frac{1}{n}, .., \frac{1}{n}\right) = \log_2(n)$	$S(\rho) \leq \log_2 n$ with n=# unique E.V.s
$H(X, Y) \geq H(X),\ H(Y)$	$H(\rho_{A,B}) \geq \lvert H(\rho_A) - H(\rho_B)\rvert$
	e.g. (Entangled Bipartite $\rho_{A,B} = \lvert\psi\rangle \langle\psi\rvert$): $H(\rho_A) = H(\rho_B) = 1$ and $H(\rho_{A,B}) = 0$
$H(X \mid Y) = H(X, Y) - H(Y) \geq 0$	$H(\rho_A \mid \rho_B) = -H(\rho_A) < 0$
$I(X; Y) \geq 0$	$I(\rho_{A,B}) \geq 0$, equal iff $\rho_{A,B} = \rho_A \otimes \rho_B$
$H(XY) + H(YZ) \geq H(Y) + H(XYZ)$	$S(CD) + S(BC) \geq S(B) + S(D)$[13]

[9] Notice that: The Hermitian matrix (A), which acts as the random variable, equals $\sum_k \lambda_k P_k$ by the spectral decomposition where λ_k is the outcome (equivalent to ω_k) and P_k is a projector onto the event representing this outcome; the probability to observe this outcome on your specific system ρ is thus $tr(\rho P_k)$.

[10] aka the expected value of A on state ρ. If $\rho = \lvert\psi\rangle \langle\psi\rvert$, then $\langle A \rangle_\rho = \langle\psi\rvert A \lvert\psi\rangle$.

[11] because $\mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$

[12] because $\mathrm{Tr}[\rho(A - \langle A \rangle_\rho \mathbb{1})^2] = \mathrm{Tr}[\rho A^2] - \langle A \rangle_\rho^2$.

[13] Since the terms $S(CD) - S(D)$ and $S(BC) - S(B)$ could be negative, but their sum is non-negative, a qubit in C can be entangled with D, reducing $S(CD)$, or with B reducing $S(BC)$, but not both! (this is called monogamy of entanglement.)

2.7 Quantum Computation

It will be useful to understand the basics of how a quantum computer performs computation differently from our everyday classical computers. While a classical computer can be modelled by a Turing Machine $\mathcal{M}$, it can also be described by a (digital) circuit[14]. We will start this section by defining a Quantum Turing Maching (QTM) first introduced in [Deu85] and later refined in [BV97], and explain some of the complication with this model of computation, then we will introduce the Quantum Circuit Model which is predominantly used nowadays. We find [YM08] to be a soft introduction to the subject of quantum computation, while [NC02] covers most topics of interest in greater detail and rigor, but might be intense for a first take on the topic.

Definition 2.7.1 (Quantum Turing Machine)**.** *A Quantum Turing Machine, $\mathcal{M}$, is defined by $\langle Q, \Gamma, \perp, \Sigma, \delta, q_0, F\rangle$ together with an infinite one-directional tape similar to a TM with the exception*

- *$C := Q \times \Gamma^* \times \mathbb{Z}$ is the set of configurations of $\mathcal{M}$ denoting the current state $\times$ symbols on the tape $\times$ the position of the head (with 0 being the initial location).*
- *$\delta : c_u \mapsto c_v$ is a quantum channel mapping configuration $c_u \in C$ to configuration $c_v \in C$.*

A few notes on the dynamics of QTMs:

- If we take the simple case of a quantum channel which is unitary evolution, then $|c_n\rangle = \delta^n |c_{\text{initial}}\rangle = \delta^n |q_0\rangle |x\rangle |0\rangle$, with x being the input to $\mathcal{M}$. This allows $|c_n\rangle$ can be in a superposition of multiple configurations.
- If we take the simple case of a quantum channel which is unitary evolution, the probability of accepting after n steps is $\sum_{q\in F} |\langle c_{\text{q}}| \delta^n |c_{\text{initial}}\rangle|^2$.
- Some works suggested that adding a Halt qubit/cell on the tape that can be measured without affecting the final output statistics.
- Once the machine halts, the configuration of $\mathcal{M}$ needs to be measured to determine the symbols on the tape.

A few notes on QTM conceptual problems:

- **Universality of QTMs.** It is difficult to define what it means for on QTM to simulate another. If you want a QTM $\mathcal{M}$ to simulate two machines one after the other (combining algorithms), how can you give a classical input in the middle and erase the contents of the tape, and reset the internal state back to q_0 without $\mathcal{M}$ being measured?
- **Reversibility of QTMs.** Evolution of quantum systems is unitary, hence reversible. Making a QTM reversible required many to restrict the machine to transition from $q_f \in F \to q_0$. Furthermore, it required that each state $q \in Q$ has to be entered while the machine's head steps in a certain direction, say always left for q_1, while right for q_{18} for example.

[14] see earlier section on Theory of Computation.

- **Parallelism of QTMs** might violate the principle of locality if δ is not constrained. [BV97] restricted δ to preserve unit length of any particular configuration. Observe that two configurations (1) whose tape values differ in a cell not under either of their heads, or (2) whose tape heads are not either in the same cell or exactly two cells apart, cannot result in the same next configuration. Therefore, δ is restricted to result in orthogonal configurations for these cases.
- **Termination.** If the QTM is in a superposition of states (branches of computation), and one of the states $q \in F$, while the others are not, should we say this QTM has halted or not? Furthermore, a QTM, $\mathcal{M}$, never stops except when measured, so even if $\mathcal{M}$ reaches a final state, it could move away from it before we get to measure the tape.

Due to these complications, the community sought better luck with an equivalent of Circuits that would allow harnessing superpositions, interference and entanglement. The question to ask is what would be the smallest possible universal quantum gate set? To answer this we define quantum gates and mention some of the most important ones, then extend the definition of classical circuits seen in 2.1.5 to quantum circuits.

Definition 2.7.2 (Quantum Gate)**.** *Any unitary operator U is a valid quantum gate. While we can pick a unitary on a composite complicated multi-qubit Hilbert space, we only focus on Single, Double and Triple qubit gates because they are simple and suffice to perform any unitary evolution on composite systems (see Table 2.7 and Figure 2.17).*

Notice, that a unitary operator is reversible by definition $UU^\dagger = U^\dagger U = I$, implying that the number of input qubits to a gate will be equal to the number of output qubits to preserve information.

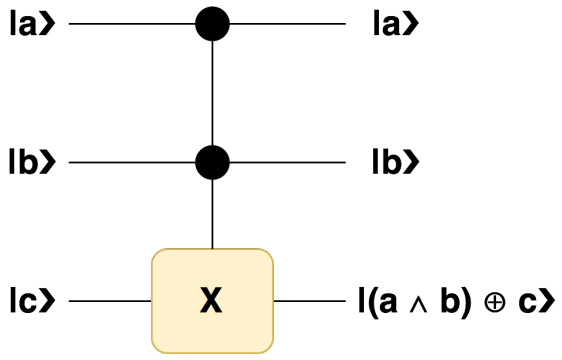


Figure 2.17: The Toffoli gate is a convenient 3-qubit gate that acts as a controlled-CNOT.

Possible universal quantum gate sets:

- CNOT and all single qubit gates [Bar+95].

Gate \ Representation	Matrix	Effect
Pauli-X / NOT	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
Pauli-Y / Rotation by π around y-axis	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto i \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}$
Pauli-Z / Rotation by π around z-axis	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$
Hadamard H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$
$S = \sqrt{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ i\beta \end{pmatrix}$
$T = \sqrt{S}$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ e^{i\pi/4}\beta \end{pmatrix}$
Controlled-NOT (CNOT)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \eta \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ \beta \\ \eta \\ \gamma \end{pmatrix}$

- Toffoli[15], Hadamard, and S gates [Kit97].
- CNOT, Hadamard, and T gates [Boy+00].

Any arbitrary unitary operator can be efficiently approximated[16] from any of these universal quantum gate sets. (recall that there is an infinite number of unitary matrices on a Hilbert space, we informally say this universal set is *dense* in that Hilbert space to enable us to get close to the effect of any unitary we desire.)

Definition 2.7.3 (Quantum Circuit)**.** *A quantum circuit is composed of a fixed number of qubits (called the width of the circuit) and a sequence of gates or measurements applied to combinations of these qubits (where the length of the longest path from the input to the output is called the depth of the circuit). Input qubits move from left to right with each vertical column of gates applied at each timestep and the output is the final state of the qubits on the right (see Figure 2.18).*

The size of the circuit (width $\times$ depth) roughly corresponds to the time complexity of said circuit.

We can now introduce three quantum complexity classes seem to that extend their classical counter-parts introduced above.

[15] See Figure 2.17.
[16] We expound on this in chapter 5.

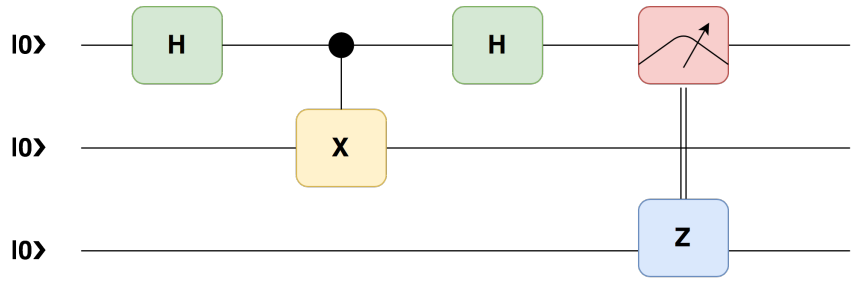


Figure 2.18: An example quantum circuit with 3 qubits, a Hadamard gate applied to the first qubit/wire, followed by a controlled-not gate acting on the top two qubits, then another Hadamard on the top wire, and at the end, the first qubit is measured in the canonical basis, and the classical output of this measurement (0 or 1) is used to classically control (denoted by two vertical lines) a Pauli-Z-gate.

Definition 2.7.4 (Bounded-Error Quantum Polynomial Time BQP)**.** *A language L is said to be in* BQP *iff* $\exists$ *a polynomial-time uniform family*[17] *of quantum circuits* $\{Q_n \mid n \in \mathbb{N}\}$ *that take* n *input qubits and outputs* 1 *output bit s.t.*

- *(Completeness) If* $x \in L$, $Pr[Q_{|x|}(x) = 1] \geq 2/3$
- *(Soundness) If* $x \notin L$, $Pr[Q_{|x|}(x) = 1] \leq 1/3$

Definition 2.7.5 (Quantum Interactive Proofs (QIP))**.** *Same as* IP *but with the verifier being a* BQP *circuit, and the communication between verifier and prover is qubits.*

Theorem 2.7.1 (QIP = IP)**.** *[Jai+09]*

Definition 2.7.6 (Quantum Merlin Arthur (QMA))**.** *Same as* MA *but with the verifier being a* BQP *TM, and the communication between verifier and prover is qubits.*

Definition 2.7.7 (MIP with Quantum Provers (MIP^*))**.** *Same as* MIP*, except that the provers are quantum circuits that can share arbitrarily many entangled qubits before starting interaction with verifier. The verifier is still classical, as are all messages between the provers and verifier.*

Theorem 2.7.2 ($\mathsf{MIP}^* = \mathsf{RE}$)**.** *[Ji+20]*

2.7.1 Bell Inequalities

It is useful to take a deeper look at correlations between distant parties sharing randomness versus sharing quantum entanglement following John Bell's seminal paper [Bel64]. This shared resource (also called a hidden variable[18]) is denoted by λ sampled from a probability

[17] recall definition 2.1.6.

[18] In 1935, Einstein, Podolsky, and Rosen argued that measurement in quantum mechanics could be explained by a hidden variable (that might be inherently inaccessible) that makes quantum mechanics be a local and realism theory. This was proven incorrect by Bell by exploiting quantum entanglement that violates his inequalities.

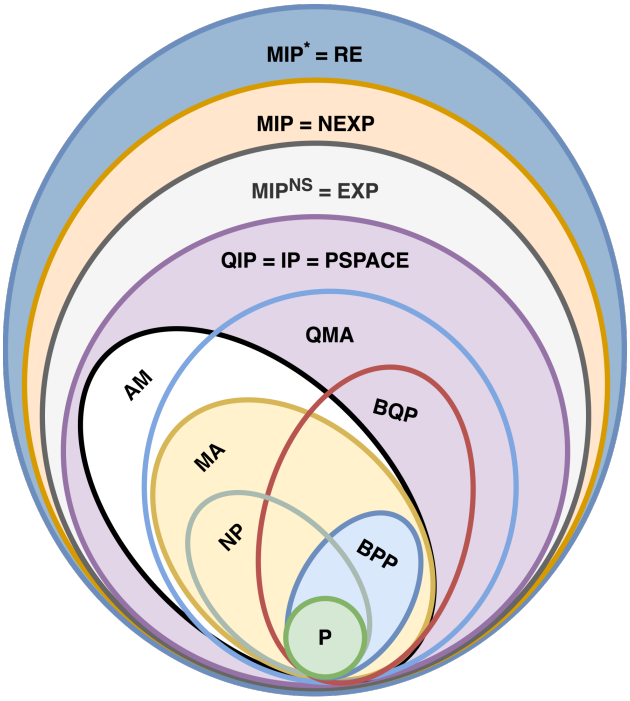


Figure 2.19: Venn-Diagram of Introduced Complexity Classes

distribution $\mathbb{p}(.)$ from a set Λ. If you have two parties that meet and then separate and you believe that quantum mechanics follows *local realism*, then once they separate, their individual actions on the part they have of the joint system cannot affect the other party's part of the system after separation. Note, λ can evolve in general as they separate, but the outcome the first party sees is assumed, in local realism, to only depend on λ not on actions performed by the second party. The setup is two parties, Alice and Bob, able to perform one of two operations, a_0 or a_1 for Alice and b_0 or b_1 for Bob, on their part of the system after separating. As an example, a_0 *could* be a measurement in the canonical basis $|0\rangle, |1\rangle$, and a_1 *could* be a measurement in the $|+\rangle, |-\rangle$ basis for Alice's qubit or some other basis measurement, similarly for Bob. Let A and B be functions mapping the chosen measurement and the hidden variable to the the observed value from these measurements. Formally we write A as

$$A : \{a_0, a_1\} \times \lambda \to \{+1, -1\}$$

and similarly for B. In reality, the outcome could be any discrete set with values in the interval $[-1, 1]$. Let $\bar{A}(a_i, \lambda)$ denote the average of value of the outcome A given multiple measurements of the system with measurement type a, similarly for $\bar{B}(b_i, \lambda)$.

Definition 2.7.8 (Bell's Inequality)**.** *Let $C(a_i, b_i)$ be the expected quantum correlation between the outcome of measurement of Alice and Bob's parts of the quantum system after*

separation. Due to independence of the parts for any specific hidden variable λ, we get

$$C(a_i, b_i) = \int_\Lambda \bar{A}(a_i, \lambda)\bar{B}(b_i, \lambda)\mathbb{p}(\lambda)d\lambda$$

Using the triangle inequality on $C(a_i, b_i) - C(a_i, b_j)$, Bell showed that: $i, j \in \{0, 1\}$ and $i \neq j$:

$$|C(a_i, b_i) + C(a_i, b_j) + C(a_j, b_i) - C(a_j, b_j)| \leq 2$$

The correlation is defined as the expected value over the outcomes that Alice and Bob get after measuring their part of the system. Recalling that the expectation of a random variable X is $\int_\Omega X(\omega)\mathbb{p}(\omega)d\omega$, we replace X with the averages $\overline{A}$ and $\overline{B}$, so it is as if it is a double expectation[19].

Definition 2.7.9 (The Bell Operator)**.** *The left hand side of Bell's Inequality can be rewritten in the language of quantum mechanics in terms of Alice and Bob's Hermitian operators A_0, A_1, B_0, B_1 by defining the Bell operator S as*

$$S = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$$

making Bell's Inequality written as the expected value of S, namely $\langle\Psi| S |\Psi\rangle \leq 2$, where $|\Psi\rangle$ could be a product state (representing classical correlations) or entangled state (representing quantum correlations).

This bound is always satisfied if Alice and Bob share randomness (or a quantum product state, aka not entangled). However, if quantum entanglement is shared among them, there exists a choice of measurements a_0, a_1, b_0, b_1 and shared quantum state that violate this inequality.

$$\langle\Psi| S |\Psi\rangle = 2\sqrt{2} \not\leq 2$$

Experimental violation of Bell's inequality was indeed performed, which directly implies that either realism or locality or both are violated.

Violation of Bell's inequality is achieved with:

- Shared Entangled Quantum State $|\Phi^-\rangle$
- $a_0 = \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}$, or A_0 is the Pauli Z gate.
- $a_1 = \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \right\}$, or A_1 is the Pauli X gate.
- $b_0 = \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1-\sqrt{2}\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1+\sqrt{2}\\1\end{pmatrix} \right\}$, or B_0 is the Hadamard H gate.
- $b_1 = \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}-1+\sqrt{2}\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}-1-\sqrt{2}\\1\end{pmatrix} \right\}$, or B_1 is $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\-1 & -1\end{pmatrix}$

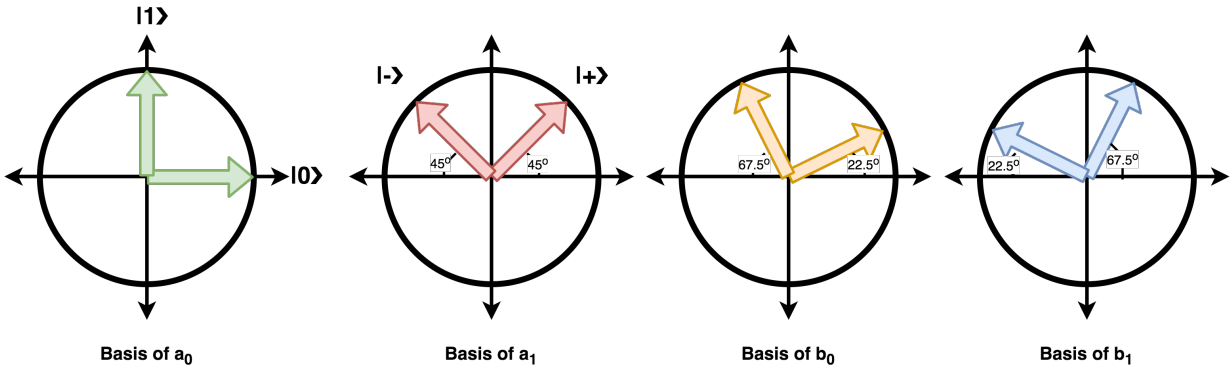


Figure 2.20: Measurement Basis Choices for Alice and Bob to violate Bell's Inequality

Definition 2.7.10 (Tsirelson's bound)**.** *[Cir80] The upper limit to the value of the expected value of the Bell operator, $\langle\Psi| S |\Psi\rangle$, using quantum mechanical shared resources (quantum strategies) is $2\sqrt{2}$.*

$$\langle\Psi| S |\Psi\rangle \leq 2\sqrt{2}$$

Proof. This is a rough sketch of the proof. We start by squaring the Bell Operator S.

$$S^2 = 4 \cdot (I \otimes I) - [A_0, A_1] \otimes [B_0, B_1]$$

Recalling that the eigenvalues of A_i and B_i are ± 1, we get the infinity norm (the maximum value) of

$$||[A_0, A_1]||_\infty \leq 2 \text{ and } ||[B_0, B_1]||_\infty \leq 2$$

$$\implies ||S^2||_\infty \leq 8$$
$$\implies ||S||_\infty \leq 2\sqrt{2}$$

Saturating these inequalities requires both commutators to equal 2, meaning A_0 and A_1 must anti-commute ($A_0A_1 = -A_0A_1$) and similarly for B_0 with B_1. This was indeed what we saw in the above choices to violate Bell's Inequality. □

2.8 Game Theory

Definition 2.8.1 (Game)**.** *A game is defined by a collection of*

- ***Rules:*** *a collection of constraints on what each player can do, and a specification of how / what each player will win.*
- ***Actions:*** *The allowed operations to be performed by agents participating in the game (players).*

[19] see law of total expectation.

- ***Players:*** *(a subset of) these players could be* ***collaborating****, not all players need to have the same set of actions or constraints (****asymmetric*** *games), and the game could be simultaneous where all players have to take actions synchronously, or could be* ***sequential*** *where each (collection's) action(s) depends on another (group of) player(s).*

Definition 2.8.2 (Strategy)**.** *A player's (pure) strategy $\mathcal{S}_{\mathcal{G}}$ is a algorithm, modelled as a Turing Machine, for playing a game providing a deterministic action to perform for every possible situation throughout the game. On the other hand, if a player has a probability distribution over all the possible pure strategies, then we call this a mixed strategy.*

Let us use the Rock-Paper-Scissors game throughout this section as an example to picture what we mean by the previous and upcoming definitions. This game is a two-player, non-collaborating, synchronous, and symmetrical game. Each round a player has 3 actions to choose from; either the player picks rock, paper, or scissors. The rules are simple. Rock beats scissors, scissors beat paper, and paper beats rock. One example of a pure strategy could be to play paper in the first round, play rock in the second round, play scissors in the third round, then in the following round, pick paper again, and so on. A mixed strategy could be to pick one of the three actions uniformly at random (this is a uniform distribution over the three pure strategies that always pick one of the three actions).

We will focus on a class of games modeling the complexity class introduced in Definition 2.2.22 coined Non-Local Games [Cle+04]. These games are asymmetric, partially collaborative (between provers), and with imperfect information (verifier(s) don't necessarily know the provers' strategy, and provers don't know the sampled questions for other players in a given round.)

Definition 2.8.3 (Two Player Non-Local Games)**.** *A two-player non-local one-round game $\mathcal{G}$ is specified by a tuple $\langle \mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, \Xi, W \rangle$ where:*

1. *$\mathcal{A}$ and $\mathcal{B}$ are at most countable question alphabet sets.*
2. *$\mathcal{X}$ and $\mathcal{Y}$ are at most countable answer alphabet sets.*
3. *Ξ is the question probability distribution over $\mathcal{A} \times \mathcal{B}$*
4. *$W : \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ is the winning function.*

We explain below the possible actions for a Prover in a non-local game, to do so we will need to split their actions into macro and micro actions. Making this distinction is critically important because the game-theoretic definition of a strategy is concerned with the action or move the player makes that the other players can see, but is mostly agnostic to the computation required to be performed by the player to finally decide on this action. Here we are very much interested in how the provers harness their input and shared resources, to increase the odds of satisfying the verifiers' winning function.

Before diving into the definitions, let us explain these concepts using the Rock-Paper-Scissors game mentioned above. We relabel the actions we had before (i.e. rock, paper, and scissors) as macro-actions. The pure and mixed strategy examples we had above are now called pure and mixed macro-strategies respectively. However, imagine now the player checks

the temperature using a thermostat and if the temperature is below 19 degrees Celsius, they play scissors, but if it was between 19-22 degrees, they play paper, otherwise they play rock. The player here performed *an action* to measure the temperature and got a number back, $t \in \mathbb{R}$, but it does not concern the other players or the game directly. We label measuring the temperature and getting a reading a micro-action type, if you use a Celsius thermostat then it is a (concrete) micro-action of the temperature measurement micro-action type. Now imagine the player checks their email inbox, and if they don't have any unread email they play rock, if they had one unread email they play scissors, otherwise they play paper. Then the act of checking their inbox and returning a number $n \geq 0$ is again called a micro-action. An example of a pure micro-strategy, let's call it **PURE**, could be that in the even rounds, check the temperature and in the odd rounds check your inbox. A mixed micro-strategy, call it **MIX**, could uniformly at random either pick the micro-action to measure the temperature or to check the inbox. Now a possible pure macro-strategy could be in any round r, invoke the micro-strategy **PURE**, this gives us a number a, then invoke **MIX** this gives us another number b, if the $a \leq b$, perform the macro-action: paper. Otherwise perform the macro-action rock, and never use scissors. This is just some examples to elucidate the meaning of these definitions, but the definitions are generic.

Definition 2.8.4 (Macro-Action)**.** *A macro-action is the final action that a player performs that (a subset of) the players could see and is used in deciding on the outcome of (a round of) the game for this player.*

The macro-action in non-local games is the answer provided back to the verifier(s), and is the action that is commonly used in strategy definition in the game theory literature.

Definition 2.8.5 (Micro-Action)**.** *A micro-action is any intermediate subroutine call that the player performs before deciding on their macro-action.*

Definition 2.8.6 (Micro-Action Type)**.** *A micro-action could be one of the following types:*

1. *Use (a specific part) of their shared randomness.*
2. *Do a specific unitary or measurement on (part of) their quantum state.*
3. *Use a no-signalling blackbox.*
4. *Use a (left / right-)signalling blackbox.*

Notice that: the details of which part of the player's shared resources will be used in a micro-action, and how that part will be accessed is decided by the micro-strategy.

Definition 2.8.7 (Micro-Strategy)**.** *A micro-strategy provides a micro-action based on knowledge of (1) the input they received, (2) any preceding micro-actions, and (3) any previous rounds in the game.*

A pure micro-strategy provides a deterministic micro-action. Notice that the output of some micro-actions is probabilistic or quantum[20], but the decision to pick this micro action is

[20]Refer to Table 2.2 for a comparison between classical and quantum probabilities.

deterministic, while a mixed micro-strategy provides a probability distribution over possible micro-actions.

Definition 2.8.8 (Macro-Strategy)**.** *A macro strategy (1) provides a macro-action based on previous micro-actions performed or (2) decides to invoke another micro-strategy.*

Pure and mixed macro-strategies are as previously explained but over options (1) and (2) in the definition above. We summarize these definitions in Figure 2.21.

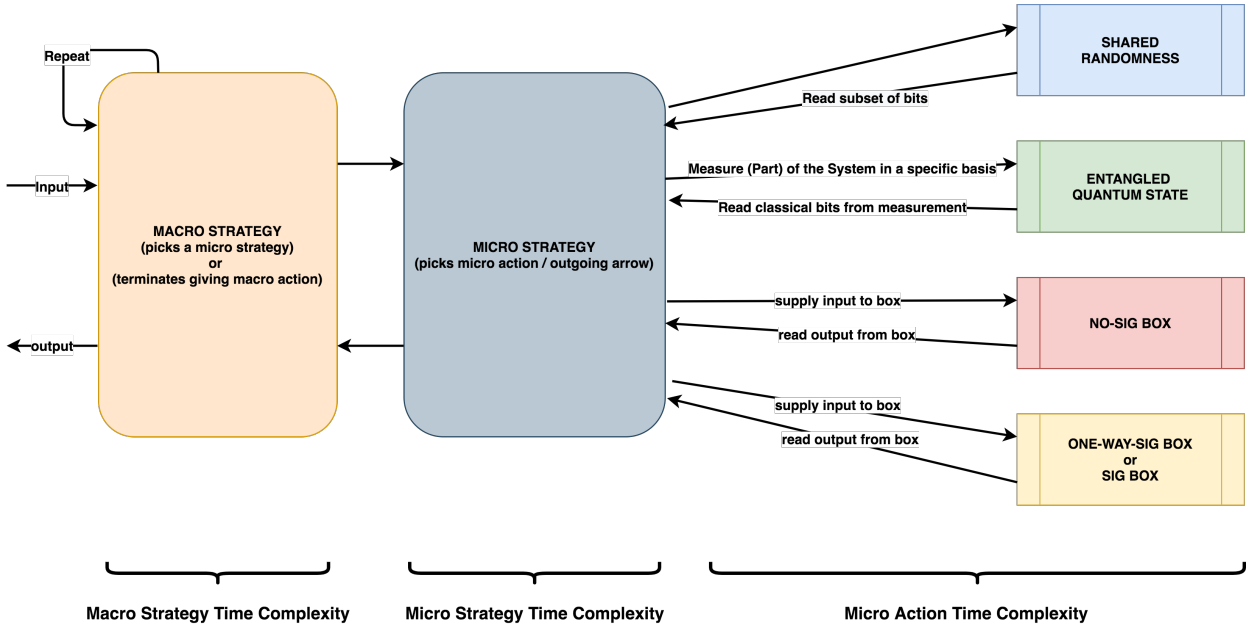
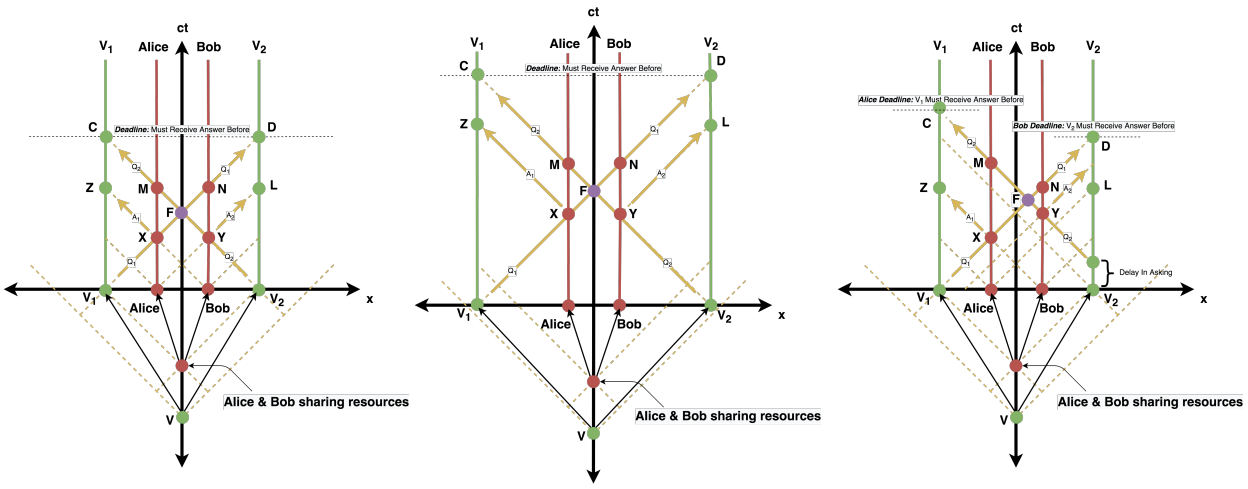


Figure 2.21: Schematic Diagram for a Player's Strategy

Figure 2.22 showcases three possible space-time diagrams for an actual possible implementation of a non-local game (often called **relativistic non-local game** [Kil90] [Ken99] [Lun+15] [Ver+16] [Cré+19]). As will be seen below, to implement non-local games under relativistic constraints, we can no longer always rely on a single verifier. Sometimes we would associate with each prover a verifier that makes sure they reply in a timely manner, so as the provers can never cheat under the rules of information theory and special relativity. The diagrams on the next page are from the frame of reference of the verifiers $V = \langle V_1, V_2 \rangle$. The story starts at the bottom of the time-axis when the verifiers, V_1 and V_2, agree on the questions to ask then move to space-like separated locations to ask the questions to Alice and Bob. Alice and Bob decide on their strategy for this round and then proceed to move at a speed slower than the speed of light to points labelled Alice and Bob thus separating. Verifier V_1 must receive a response from Alice *strictly* before time C_t (similarly V_2 must receive Bob's response before D_t). For practical implementation reasons, we are not concerned with the location of Alice and Bob at any time during the round. However, we want to ensure that they answer before they could ever see each other's questions. Since the verifiers trust each other, then the moment V_1 could've received Q_2 if it were traveling at the speed of



(a) Small Distance between Verifiers

(b) Large Distance between Verifiers

(c) Verifiers ask at Different Times

Figure 2.22: Space-Time Diagrams of Two Player Relativistic Non-Local Games—Showcasing the Effect of Increasing the Gap between Verifiers on the leeway for Alice and Bob to respond. Plots are drawn on the same scale.

light, it should no longer accept an answer from Alice (similarly for V_2, Q_1 and Bob). This is because the point of intersection of V_1 and V_2's light beams carrying their questions, F, is the first event where a player can read both questions.[21]

Comparing Plot (a) and (b) on the next page, we notice that as the verifiers get further away from each other, the players get more time to reply, which might entail the verifier sending multiple questions to a player and the player replying to all questions before the deadline of the first question (aka. Alice could reply to all questions in the time interval $[Z_t, C_t]$). In Plot (c), V_2 send Bob's question later, this shifts event F to the right, which makes Alice have more time to answer, while Bob has a tighter deadline. **If Bob is allowed to reply before C_t instead of D_t, then this is a one-way communication channel where Alice can only see her input, while Bob sees both his input and Alice's.**

What if the Verifiers are malicious? This is typically the case when considering Zero-Knowledge proofs [GMR89][22]. In this case, we look at the non-local game from a complexity theory perspective. We include the verifiers as players, and the game becomes asymmetric, in that the verifiers wish to not only verify that the provers have solved a difficult decision problem and be tricked by the provers, but would also want to know such a solution. For the remainder of this document, we will assume honest verifier(s) and expound on the malicious-

[21] Note there is no clever way for Alice to send a quantum (answer) state entangled with her system before F for example, then apply some measurement to her part of the entanglement after seeing Q_2 to change the answer V_1 receives. This would be in violation of information theory and special relativity.

[22] Will be introduced in the Cryptography section in the Background chapter.

verifier-case only when we need to.

Definition 2.8.9 (Game Value)**.** *We say the players win game $\mathcal{G}$ with probability value* $\text{val}^*(\mathcal{G}, \mathcal{S}_\mathcal{G})$ *using pre-agreed upon strategy $\mathcal{S}_\mathcal{G}$. Then we define the maximum possible winning probability for $\mathcal{G}$ for any possible strategy $\mathcal{S}'_\mathcal{G}$ as the Game Value:*

$$\text{val}^*(\mathcal{G}) = \sup_{\mathcal{S}'_\mathcal{G}} \text{val}^*(\mathcal{G}, \mathcal{S}'_\mathcal{G})$$

Let $\mathbb{S}$ be some subset of all possible strategies $S'_\mathcal{G}$. Then we define the maximum possible winning probability for $\mathcal{G}$ for any strategy belonging to $\mathbb{S}$ as the $\mathbb{S}$-Game Value:

$$\text{val}^*_\mathbb{S}(\mathcal{G}) = \sup_{\mathcal{S}'_\mathcal{G} \in \mathbb{S}} \text{val}^*(\mathcal{G}, \mathcal{S}'_\mathcal{G})$$

2.9 Cryptography

We will only be covering zero knowledge proof systems which were first introduced by [GMR89].

Definition 2.9.1 (Probability Ensemble)**.** *A probability ensemble is a family of random variables $X = \{X_i\}_{i \in I}$ where I is an at most countable index set, and X_i is a random variable.*

Typically the set I is related to the input size, which in turn is a function of some security parameter for a cryptography scheme. We typically drop the subscript $i \in I$ and write X as $\{X_i\}_i$.

Definition 2.9.2 (Comparing Probability Ensembles)**.** *Let $A = \{A_i\}_i$ and $B = \{B_i\}_i$ be two probability ensembles, then we say A and B are*

- *(Perfectly Equal ($=$)) if $\forall$ i, A_i and B_i are identically distributed.*
- *(Statistically Close ($=_s$)) if $\forall$ i, A_i and B_i have the same finite domain set $\mathcal{X}$, and*

$$\frac{1}{2} \sum_{x \in \mathcal{X}} |Pr[A_i = x] - Pr[A_i = x]| \leq negl(i)$$

  where $\forall$ polynomials $p(.)$, $negl\,(i) < p\,(i)$.
- *(Computationally Indistinguishable ($=_c$)) if $\forall$ i, and $\forall$ PPT TMs, $\mathcal{D}$, denoting a distinguisher, we have*

$$|Pr_{a \leftarrow A_i}[\mathcal{D}(a) = 1] - Pr_{b \leftarrow B_i}[\mathcal{D}(b) = 1]| \leq negl\,(i)$$

  where $negl\,(.)$ is some negligible function, $a \leftarrow A_i$ means $\mathcal{D}$ samples element a from the probability distribution that the random variable A_i follows.

An interactive proof-system for language L is zero-knowledge if $\forall x \in L$ whatever the verifier can compute after participating in the interaction with the prover, could have been computed in polynomial time in the input size $|x|$ alone by a probabilistic polynomial time Turing machine called the simulator[23]. Here the simulator is substituting the role of the prover(s) but of course without the special knowledge the prover(s) have to actually make the proof. The simulator interacts with the verifier and tries to output an ensemble resembling the verifier's view. We write this formally below for the one prover, one verifier case that is typically discussed in the literature, but first let us cover some important definitions.

Definition 2.9.3 (Auxiliary Input)**.** *In zero-knowledge proofs, it is important that the verifier does not acquire any knowledge more that what they already had. An auxiliary input to the verifier, models all possible prior knowledge the verifier could have about the problem. For a language to have a zero-knowledge proof, the verifier must leave the interactive proof with the same knowledge (the auxiliary input) as they had prior to engaging with the prover(s), although the auxiliary input could change due to usage by the verifier. The simulator is also given this auxiliary input.*

Auxiliary inputs are also critical to allow composition of zero-knowledge proof systems [GK90].

Definition 2.9.4 (Oracle Access)**.** *When considering malicious verifiers in zero-knowledge proofs, the simulator is given oracle access to the verifier $\mathcal{V}$. Oracle access in standard complexity theory means that $\mathcal{V}$ is a black box that the simulator can query, however, we will need a stronger requirement here. Namely, Let $\mathcal{V}$ be a deterministic TM, let r be a random tape that the verifier uses (hence becomes a probabilistic TM), and let aux be the auxiliary input, let x be the problem's input, and let the sequence of strings $\langle m_0, m_1, ...\rangle$ be an ordered list of the messages $\mathcal{V}$ receives during their interaction with a prover. Then the simulator queries $\mathcal{V}$ with the query $(r, x, \langle m_0, m_1, ..., m_k\rangle)$ and receives its next message to the prover or its output if it would've replied with an answer after any of the m_i's in the query.*

$$V_{aux}(r, x, m_0, m_1, ..., m_k)$$

Notice that although both the simulator and the verifier are provided the aux input, we are not allowing the simulator to provide the aux input to the verifier. That is why we denoted the verifier above by V_{aux} signifying that it is not part of the simulator's query. However, the simulator could control the verifier's randomness r.

Definition 2.9.5 (Rewinding)**.** *If the simulator queries $\mathcal{V}$ with $V_{aux}(r, x, m_0, m_1, ..., m_k)$, then queries it with $V_{aux}(r, x, m_0, m_1, ..., m'_k)$, we say the simulator rewound $\mathcal{V}$ before the last message m_k and changed their message to m'_k. The simulator can rewind to right before any message m_i $\forall$ $0 \leq i \leq k$.*

[23]This is an informal definition to convey the idea, in reality the verifier could compute something that doesn't depend on x at all, and that is okay in our formal definition below.

We give a concrete example of these concepts after defining zero-knowledge proofs below.

Notation: We define $\text{view}_{\mathcal{V}}(\mathcal{P}(x) \overset{k}{\longleftrightarrow} \mathcal{V}(x))$ to be a random variable over $\mathcal{P}$ and $\mathcal{V}$'s coin tosses, denoting $\mathcal{V}$'s view during the protocol on input x, namely the messages exchanged and the private coin tosses that $\mathcal{V}$ used.

Definition 2.9.6 (Zero-Knowledge Interactive Proof System (Complexity))**.** *A language L has a zero-knowledge proof system if*

- *(IP) $\exists$ an interactive proof system $\mathcal{P}, \mathcal{V}$ for L.*
- *(Zero Knowledge) $\exists$ a simulator PPT TM, $\mathcal{S}$, where S is a random variable over its output s.t. $\forall\ x \in L, \forall\ \mathcal{V}^* \in \mathbb{V}, \forall\ aux \in \{0,1\}^{\mathsf{poly}(|x|)}$*

$$view_{\mathcal{V}^*}(\mathcal{P}(x) \leftrightarrow \mathcal{V}^*(x, aux)) = S^{\mathcal{V}^*}(x, aux)$$

where $S^{\mathcal{V}^*}(x, aux)$ is the random variable over the output of simulator $\mathcal{S}$'s PPT TM with oracle access to the verifier $\mathcal{V}^*$'s machine. Recall from the Complexity Theory background 2.2, that $\mathbb{V}$ denotes all possible PPT verifier TMs.

Notice the $\text{view}_{\mathcal{V}^*}(\mathcal{P}(x) \leftrightarrow \mathcal{V}^*(x, \text{aux})) = S^{\mathcal{V}^*}(x, \text{aux})$ in the definition above is a comparison between two probability ensembles[24], where the equal sign means perfectly equal, and this makes it a Perfect Zero-Knowledge Proof (PZK). If we were to replace the equal with $=_s$ or $=_c$ this would imply Statistical/Computational Zero-Knowledge Proof (SZK/CZK) respectively.

Notice that because the provers have knowledge enabling them to prove that $x \in L$, providing the simulator with oracle access to the verifier gives it an advantage above the prover(s). The verifier could now be tricked into thinking it is interacting with a prover, when it is actually interacting with a simulator. However, because the simulator does not interact at all with the provers, and simply rewinds the verifier, it does not possess the knowledge to prove $x \in L$, so if the simulator was able to produce the view of the verifier, then the verifier must have not gain any knowledge about the prover's proof.

We will now cover the canonical example of a zero-knowledge proof with a possible malicious verifier (aka a verifier that is trying to acquire knowledge of the proof that would enable them to impersonate the prover with other verifying entities.)

Theorem 2.9.1 (GRAPH-ISOMORPHISIM $\in \mathsf{PZK}$)**.** *The language Graph-Isomorphism, defined as $\{(G_0, G_1) \mid \exists\ \pi \text{ s.t. } G_0 = \pi(G_1)\}$ where π is a permutation of vertices and G_i's are graph, has a zero-knowledge proof.*

Proof. Let us define the interactive proof first. The input to both the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ is G_0 and G_1, $\mathcal{V}$ flips one coin uniformly at random and denotes it b. An honest $\mathcal{P}$ will be able to compute the isomorphism permutation π s.t $G_0 = \pi(G_1)$. $\mathcal{P}$ using their

[24]The view is a random variable over the coin tosses of $\mathcal{P}$ and $\mathcal{V}$, while S is a random variable over $\mathcal{S}$'s random coin tosses.

private random coins, randomly permutes G_0 resulting in graph $G = \phi(G_0)$, where ϕ is a random permutation of the vertices. $\mathcal{P}$ sends G to $\mathcal{V}$, $\mathcal{V}$ only then sends back b. $\mathcal{P}$ now has to provide $\mathcal{V}$ a permutation that is not the isomorphism (so as to not leak any knowledge), but that maps $G_b \to G$ for whichever b the verifier sampled, so that $\mathcal{V}$ can apply it and check that it indeed produces G in polynomial time. If $\mathcal{P}$ is honest then they know π and can simply return $\psi = \phi \circ \pi^b$, and $\mathcal{V}$ then applies $\psi(G_b) = \phi(\pi^b(G_b)) = G$. Notice that $\pi^b(G_b) = G_0$, and that finding π from ψ is as difficult as finding π, because ψ is uniformly sampled independent of the value of b because ϕ was randomly sampled.

The above was the interactive proof which can be shown to have appropriate completeness and soundness. Now let us build a simulator that interacts with the verifier and can reproduce the prover's outputs showing the zero-knowledge condition. Here we need to consider a malicious verifier, $\mathcal{V}^*$, that samples b arbitrarily trying to extract π and show that even then it is not possible. $S^{\mathcal{V}^*}(G_0, G_1)$ samples the random bit b the composite permutation ψ and the verifier's random tape r, and queries $\mathcal{V}^*(r, G_0, G_1, \phi(G_b))$, the oracle will return the next message to the prover which is the bit b^* that it samples, if $b^* = b$ then the simulator outputs the view $= (r, G, b, \phi)$, else the simulator rewinds to the beginning and samples a different ϕ, b and starts over till it succeeds. □

In the above example the auxiliary input for the verifier and the simulator could be half the isomorphism map π. In this case, we demand that the verifier is not able to know anything about the other half of the π. Notice if the aux input is the full π minus the mapping between two vertices for example, then the verifier without talking to the prover can try the permutations for both vertices and check the complete isomorphism, so it is critical that our requirement for zero-knowledge is that the verifier gains no knowledge for their interaction with the prover.

Chapter 3

Lead Up Work

In this chapter we will focus on a literature review of two player non-local games, introduce local strategies, quantum strategies, no-signalling strategies and (one-way) signalling strategies. This will enable us to extend to multiple players in the following chapter, state Crépeau's theorem and showcase our proof for it.

3.1 Strategies

We start by viewing definition 2.8.2 from an information theoretic perspective. Strategies 2.8.7 and 2.8.8 were focused more on the implementation needed to reply with specific macro-actions. However, we can hide the implementation details and model a strategy as a communication channel where the players produce outputs conditioned on their inputs. One could imagine that there are many implementations (using combinations of micro action types) that would produce the same channel (or conditional probability distribution). To organize this situation and make analyzing it tractable, we mimic complexity theorists by lumping implementations based on particular micro-action types[1], and try finding the weakest strategy that could implement any particular channel. This way we can start classifying strategies (as was done with complexity classes in Figure 2.19), reducing strategies to one-another and use the complete arsenal of literature developed in complexity theory.

Throughout this chapter, unless otherwise specified, $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in \mathcal{X}$, and $y \in \mathcal{Y}$, where the calligraphic set symbols are as defined in 2.8.3. Moreover, A, B, X, Y will be random variables over the elements in the sets $\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}$ respectively.

Definition 3.1.1 (Strategy (information theory))**.** *A two player strategy in non-local games is a communication channel (as in definition 2.5.2) encapsulating away the details of the possible algorithms the parties could perform on their part of the input questions $\langle x, y \rangle$ and*

[1] We mean a strategy cannot use both a no-signalling micro-action and a quantum micro-action. We will consider strategies using multiple micro-action types in the following chapter.

their shared physical resources, in order to output answers $\langle a, b \rangle$.

$$\Omega(A, B \mid X = x, Y = y)$$

If we represent $\Omega(A, B \mid X = x, Y = y)$ by a 4-dimensional matrix, where each quadruple $\langle a, b, x, y \rangle$ specifies a unique element in this matrix, then from a topological perspective, we can define the set of all matrices generated from the strategies of type T, and then we can ask questions about separating sets of different strategy types T and T', their intersections, etc.

Definition 3.1.2 (T Strategy)**.** *We say a strategy is a* ***T strategy*** *or a* ***strategy of type T****, if the micro-strategy used by the players only picks micro-actions of type T.*

The remainder of this section will be defining T strategies for

$$\text{T} \in \{\text{DET,NA,LOC,QPE,COMOP,NOSIG,R-SIG,L-SIG,SIG}\}$$

Definition 3.1.3 (Concrete T Strategy)**.** *If we specify the exact details of T micro-actions performed in the T Strategy, then we call that* ***a concrete T strategy***[2]*.*

Definition 3.1.4 (Strategy Class)**.** *Let* $\Omega_S(A, B \mid X = x, Y = y)$ *be a correlation resulting from a concrete S-strategy. Then we denote the class of all possible correlations produced by concrete S-strategies by blackboard bold-ing the strategy type,* $\mathbb{S}$*, and define it as*

$$\mathbb{S} = \{\Omega_S(A, B \mid X = x, Y = y)\}$$

Below we will define the main strategy types used in the literature.

Definition 3.1.5 (Deterministic Strategy)**.** *Let* $f_{Alice} : \mathcal{X} \to \mathcal{A}$ *and* $f_{Bob} : \mathcal{Y} \to \mathcal{B}$ *be functions. Then we define a deterministic strategy as one that produces correlations obeying*

$$\Omega_{DET}(a, b \mid x, y) = \mathbb{1}_{(a=f_{Alice}(x) \ \cap \ b=f_{Bob}(y))}$$

Therefore, there are as many unique $\Omega_{DET}(. \mid .)$ *as there are functions*[3]*.*

Definition 3.1.6 (Non-Adaptive Strategy)**.** *We define a non-adaptive strategy as the ones where the output is independent of the input.*

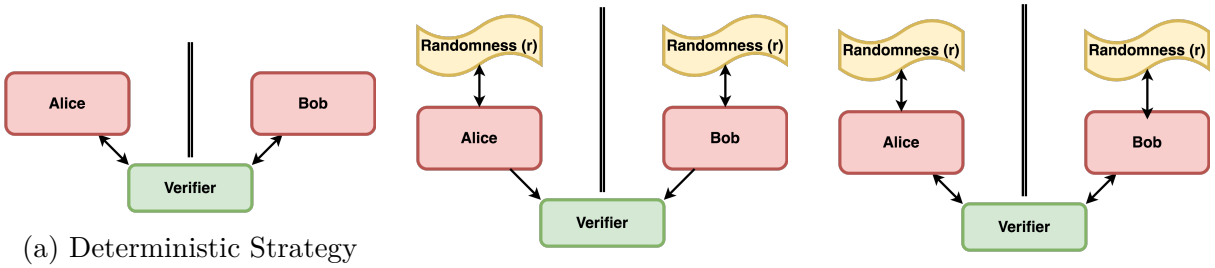
$$\Omega_{NA}(a, b \mid x, y) = \Omega_{NA}(a, b)$$

[2]We provide examples of concrete T strategies at the end of this section 3.1 after defining all the various strategies of type T.

[3]In the case where the inputs and outputs are n bits, the number of functions is 2^{2^n} for f_{Alice} and similarly for f_{Bob}.

Definition 3.1.7 (Local Strategy[4])**.** *Let R be an at most countable set $\mathcal{R}$ (denoting the shared randomness) with R being a random variable over elements of $\mathcal{R}$ following the probability mass function (PMF) $P(R = r)$ with $r \in \mathcal{R}$, and a bijection $\pi : \mathbb{N} \to \mathcal{R}$, and $f_{Alice} : \mathcal{X} \times R \to \mathcal{A}$ and $f_{Bob} : \mathcal{Y} \times R \to \mathcal{B}$ be functions. Then we define a local strategy as*

$$\Omega_{LOC}(a, b \mid x, y) = \lim_{k\to\infty} \sum_{j=1}^{k} P(R = \pi(j)) \cdot \mathbb{1}_{(a=f_{Alice}(x,\pi(j)) \ \cap \ b=f_{Bob}(y,\pi(j)))}$$



(a) Deterministic Strategy (b) Non-Adaptive Strategy (c) Local Strategy

Figure 3.1: Local Hidden Variable Strategies Schematic Diagrams

Theorem 3.1.1 ($\mathbb{DET} \cap \mathbb{NA} = \mathbb{CST}$)**.** *where $\mathbb{CST}$ denotes the strategies with constant functions, f_{Alice} and f_{Bob}, for the players.*

Theorem 3.1.2 ($\mathbb{DET} \cup \mathbb{NA} \subset \mathbb{LOC}$)**.**

Definition 3.1.8 (Quantum Prior-Entanglement Strategy)**.** *A strategy $\Omega_{QPE}(a, b \mid x, y)$ is said to be quantum prior-entanglement (QPE) if there exists:*

- *An at most countable set $\mathcal{D}$ (denoting Hilbert space dimensions) with D being a random variable over elements of $\mathcal{D}$ following the PMF $P(D = d)$ with $d \in \mathcal{D}$.*
- *A bijection $\pi : \mathbb{N}^+ \to \mathcal{D}$.*
- *Hilbert spaces, $\mathcal{H}^{(d)}_{\text{Alice}}$ and $\mathcal{H}^{(d)}_{\text{Bob}}$ for Alice and Bob respectively for each dimension $d \in \mathcal{D}$.*
- *Quantum states $|\Phi^{(2d)}\rangle \in \mathcal{H}^{(d)}_{\text{Alice}} \otimes \mathcal{H}^{(d)}_{\text{Bob}}$ for each $d \in \mathcal{D}$ as the shared quantum state between Alice and Bob.*
- *For each $d \in \mathcal{D}$, $\{M^{(d)}_a\}$ is a set of projective measurements for $\mathcal{H}^{(d)}_{\text{Alice}}$ for all $a \in \mathcal{A}$.*
- *For each $d \in \mathcal{D}$, $\{N^{(d)}_b\}$ is a set of projective measurements for $\mathcal{H}^{(d)}_{\text{Bob}}$ for all $b \in \mathcal{B}$.*
- *For each $d \in \mathcal{D}$, $\{U^{(d)}_x\}_{x\in\mathcal{X}}$ are unitary operators on $\mathcal{H}^{(d)}_{\text{Alice}}$.*
- *For each $d \in \mathcal{D}$, $\{V^{(d)}_y\}_{y\in\mathcal{Y}}$ are unitary operators on $\mathcal{H}^{(d)}_{\text{Bob}}$.*

such that:

$$\begin{aligned}\Omega_{QPE}(a, b \mid x, y) &= \lim_{k\to\infty} \sum_{d=1}^{k} P(D = \pi_d) \cdot \langle\Phi^{(2\pi_d)}| \left((U^\dagger)^{(\pi_d)}_x M^{(\pi_d)}_a U^{(\pi_d)}_x\right) \otimes \left((V^\dagger)^{(\pi_d)}_y N^{(\pi_d)}_b V^{(\pi_d)}_y\right) |\Phi^{(2\pi_d)}\rangle \\ &= \lim_{k\to\infty} \sum_{d=1}^{k} P(D = \pi_d) \cdot \langle Q^{(\pi_d)}_{x,y}\Phi^{(2\pi_d)}| \, M^{(\pi_d)}_a \otimes N^{(\pi_d)}_b \, |Q^{(\pi_d)}_{x,y}\Phi^{(2\pi_d)}\rangle\end{aligned}$$

[4]Local is sometimes referred to as **Local Hidden Variable** (LHV) or **Classical**.

where π_d is shorthand notation for the bijection map $\pi(d)$, $Q_{x,y}^{(\pi_d)} = U_x^{(\pi_d)} \otimes V_y^{(\pi_d)}$, and all $\otimes$ will be 'spatial tensor products'

This definition includes infinite Hilbert spaces (imagine adding an infinite tape to the players' Turing machines). One complication arising from this is that regular tensor products no longer exist for infinite Hilbert spaces and we needed to extend the operators to $\mathcal{C}^*$-algebras represented on the possible infinite dimensional Hilbert spaces, and use a norm-based tensor product, called the spatial tensor product, that is the minimal $\mathcal{C}^*$-norm on tensor product $\mathcal{C}^*$-algebras.

It turns out that $\mathbb{QPE}$ is an open[5] set. This led to defining the **quantum prior-entanglement asymptotic correlation set** which is the closure[6] of the set QPE as:

$$\mathbb{QPE}_\bullet = \overline{\mathbb{QPE}}$$

A generalization of QPE strategies with a richer structure is the commuting operator strategies that were first introduced in Tsirelson's seminal paper [Cir80].

Definition 3.1.9 (Commuting Operator Quantum Strategy)**.** *Let $\mathcal{H}$ be some (possible infinite dimensional) Hilbert space. Then we define a commuting operator quantum strategy as*

$$\Omega_{COMOP}(a, b \mid x, y) = \langle\Psi| \left(U_a^\dagger M_x U_a\right) \cdot \left(V_b^\dagger N_y V_b\right) |\Psi\rangle$$

where

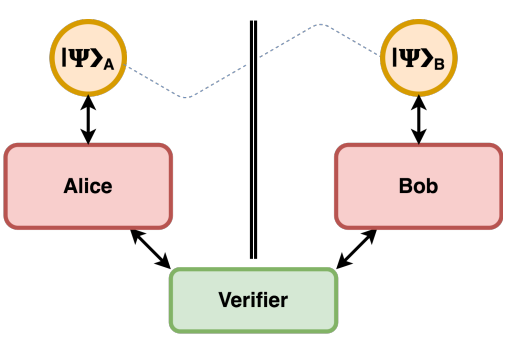
- $|\Psi\rangle \in \mathcal{H}$ *is the quantum state Alice and Bob have access to.*
- $\{M_a\}$ *is a set of projective measurements for $\mathcal{H}$ for all $a \in \mathcal{A}$*
- $\{N_b\}$ *is a set of projective measurements for $\mathcal{H}$ for all $b \in \mathcal{B}$*
- $\{U_x\}_{x\in\mathcal{X}}$ *are unitary operators on $\mathcal{H}$*
- $\{V_y\}_{y\in\mathcal{Y}}$ *are unitary operators on $\mathcal{H}$*
- $A \in \{M_a\} \cup \{U_x\}_{x\in\mathcal{X}}$*, and* $B \in \{N_b\} \cup \{V_y\}_{y\in\mathcal{Y}}$ *we have* $[A, B] = 0$

First notice the difference between prior-entanglement and commuting operator quantum strategies. The key is in how we compose two quantum systems together. In the quantum mechanics section in the background chapter we introduced composing systems using tensor product of the subsystems. However, in the commuting operator model, we allow both players to interact with a private quantum system $|\Psi\rangle$ that they both have access to. This interaction has to be agnostic to when / how each one operates on $|\Psi\rangle$. To achieve this, they are only allowed to use operators that commute with one-another[7] and composition

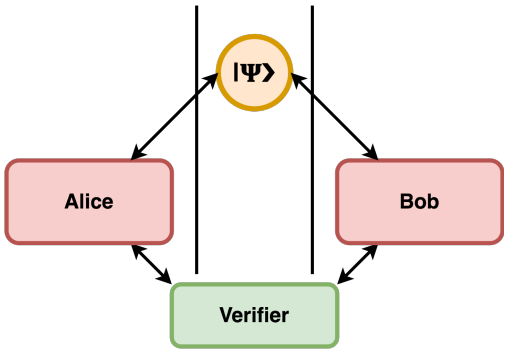
[5] **Topology Overview:** A *set*, S, in a topological space $\mathcal{T}$ consists of all the interior points in some subspace of $\mathcal{T}$, together with the *boundary*. An *open set* thus contains the interior points S might not include its full boundary but instead parts (or none of it). The *boundary* are all the elements in the space that can be reached from both inside and outside of S.

[6] The closure of S is the union of the interior and the boundary.

[7] By definitions commuting operators A and B yield the same result whether A was applied first or B, aka $AB|\Psi\rangle = BA|\Psi\rangle$.



(a) Quantum Prior-Entanglement Strategy



(b) Commuting-Operator Quantum Strategy

Figure 3.2: Quantum Strategies Schematic Diagrams

becomes regular multiplication. ***Implementing a commuting operator strategy in a relativistic setting is unknown. Namely, how can we enforce that the provers do not communicate while at the same time allowing them to interact with this same state*** $|\Psi\rangle$ ***that resides somewhere in space-time? Furthermore how can we enforce that their interaction with*** $|\Psi\rangle$ ***is using operators that commute with the operators of the other provers?***

Definition 3.1.10 (Tsirelson's problems)**.** *[SW08] Let* $\mathbb{S} \in \{\mathbb{QPE}, \mathbb{QPE}_\bullet\}$.

$$\mathbb{S} \stackrel{?}{=} \mathbb{COMOP}$$

Theorem 3.1.3 ($\mathbb{LHV} \subsetneq \mathbb{QPE} \subsetneq \mathbb{QPE}_\bullet \subsetneq \mathbb{COMOP}$)**.** *proofs for each of the three strict containment results can be found in [Bel64; CS17; Slo17; Ji+20]. This last result in 2020, solved the last of Tsirelson's problems.*

Definition 3.1.11 (No-Signalling Strategy)**.** *Includes any strategy,* $\Omega_{NOSIG}(a, b \mid x, y)$*, satisfying:*

$$\sum_{b\in\mathcal{B}} \Omega_{NOSIG}(a, b \mid x, y) = \sum_{b\in\mathcal{B}} \Omega_{NOSIG}(a, b \mid x, y'),\ \forall\ y, y' \in \mathcal{Y}\ s.t.\ y \neq y'$$
$$\sum_{a\in\mathcal{A}} \Omega_{NOSIG}(a, b \mid x, y) = \sum_{a\in\mathcal{A}} \Omega_{NOSIG}(a, b \mid x', y),\ \forall\ x, x' \in \mathcal{X}\ s.t.\ x \neq x'$$

Namely, Alice's output causally precedes[8] *Bob's input* ($a \preceq y$) *and Bob's output causally precedes Alice's input* ($b \preceq x$)*.*

No-signalling strategies contain the correlations that are at least as strong as those of quantum strategies, and are bounded from above by the very limits of what could be physically possible [Bar+05]. In 1994, Popescu and Rohrlich (PR) managed to define correlations

[8] Event u causally precedes event v means that u and v are time like separated with $u_t < v_t$ in all frames of reference.

which are stronger than those generated using quantum entanglement that do not violate the no-communication theorem[9] [PR94]. It is not known how to physically implement these beyond quantum correlations, although with advances in physics, it is theoretically not impossible. **Before introducing their definition, let us recall the distinction between uniform[10] and non-uniform[11] models of computation, and draw the analogy that strategies introduced till now are somewhat an algorithm that could be extended uniformly to different number of players and that is indeed what we will be doing in the next chapter. However, the correlation defined by PR resembles the non-uniform model, where they define a channel as a black-box, which is appropriate given we don't know how to actually implement it. We will discuss this contrast in detail in the next chapter.**

Definition 3.1.12 (PR-Box). *Let $X_1, X_2, Y_1, Y_2 \in \mathbb{F}_2$, then we define the Popescu-Rohrlich box as a, two-input (X_1, X_2), two-output (Y_1, Y_2), channel described by the following correlation:*

$$\Omega_{PR\text{-}BOX}(Y_1, Y_2 \mid X_1, X_2) = \begin{cases} \frac{1}{2} & \text{if } Y_1 \oplus Y_2 = X_1 \wedge X_2 \\ 0 & \text{otherwise} \end{cases}$$

$\oplus$ is the bit-wise XOR or addition modulo 2, and $\wedge$ is the bit-wise AND operator.

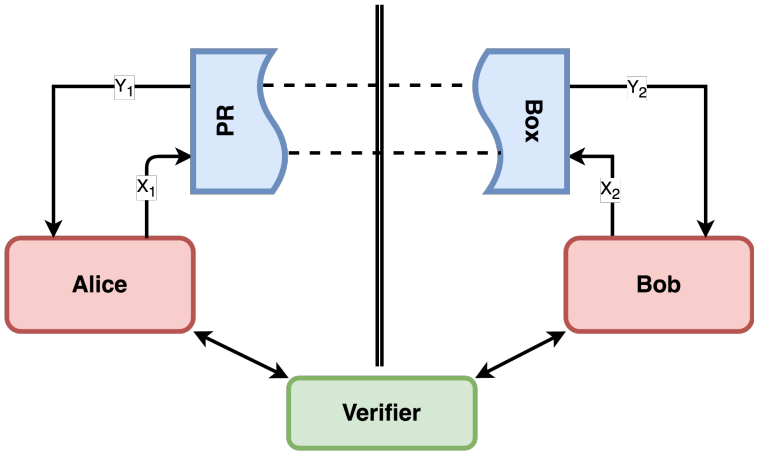


Figure 3.3: A No-Signalling Strategy Schematic Diagram using a PR-Box

Notice that the PR-box produces outputs that are completely random on its own, yet when observing the whole system, the correlation appears.

Theorem 3.1.4 (PR-Box is Two Player №-$ig-Complete). *[Bru+14] Any two player no-signalling strategy can be implemented using PR-Boxes.*

[9] see definition 2.4.3.
[10] example: a Turing machine (TM)
[11] example: family of circuits

It is not known why quantum correlation are not maximal among no-signalling correlations that obey causality. [Bra+06] showed that if quantum correlations were even slightly stronger, communication complexity[12] becomes trivial[13].

We can now introduce the complexity class $\mathsf{MIP}^{\mathbb{N}\$}$ presented in Figure 2.19 to have our complexity picture completed.

Definition 3.1.13 (Multi-Player No-Signalling Box (informal))**.** *Multi-player no-signalling boxes will be defined in detail in chapter 4, definitions 4.3.4, 4.3.5, and 4.3.6. For now, one can think of them as the generalization of PR-boxes with multiple input/output pairs. Each player has an input/output pair, such that the correlation of the outputs does not allow these players to communicate with one another in any way using this box.*

Definition 3.1.14 (MIP with No-Signalling Provers ($\mathsf{MIP}^{\mathbb{N}\$}$))**.** *Same as* MIP*, except that the provers can share arbitrary multi-player no-signalling boxes before starting interaction with verifier and the verifier is still classical, as are all messages between the provers and verifier.*

Theorem 3.1.5 ($\mathsf{MIP}^{\mathbb{N}\$}(2) = \mathsf{IP}$)**.** *[Ito09]*

Theorem 3.1.6 ($\mathsf{MIP}^{\mathbb{N}\$}\left(O(\sqrt{\log n})\right) = \mathsf{IP}$)**.** *[HK19]*

Theorem 3.1.7 ($\mathsf{MIP}^{\mathbb{N}\$}(O(\log n)) = \mathsf{EXP}$)**.** *[KRR14]*

Let n be the size of the input given to the provers and the verifier. Then the above three theorems state that no-signalling proofs with $1 \to O(\sqrt{\log n})$ provers are all equal to $\mathsf{IP} = \mathsf{PSPACE}$, while with more than $O(\log n)$ provers it capture exponential languages. It is still an open problem how strong are no-signalling proof in the number of provers between $O(\sqrt{\log n}) \to O(\log n)$.

Definition 3.1.15 (Right-Signalling Strategy)**.** *R-SIG strategies are the channels,* $\Omega_{R\text{-}SIG}$*, where Alice could signal to Bob, but Bob cannot signal Alice.*

$$\sum_{b\in\mathcal{B}} \Omega_{R\text{-}SIG}(a,b \mid x,y) = \sum_{b\in\mathcal{B}} \Omega_{R\text{-}SIG}(a,b \mid x,y'),\ \forall\ y,y' \in \mathcal{Y}\ s.t.\ y \neq y'$$

Namely, Alice's output causally precedes Bob's input ($a \preceq y$)*.*

Definition 3.1.16 (Left-Signalling Strategy)**.** *L-SIG strategies are the channels,* $\Omega_{L\text{-}SIG}$*, where Bob could signal to Alice, but Alice cannot signal Bob.*

$$\sum_{a\in\mathcal{A}} \Omega_{L\text{-}SIG}(a,b \mid x,y) = \sum_{a\in\mathcal{A}} \Omega_{L\text{-}SIG}(a,b \mid x',y),\ \forall\ x,x' \in \mathcal{X}\ s.t.\ x \neq x'$$

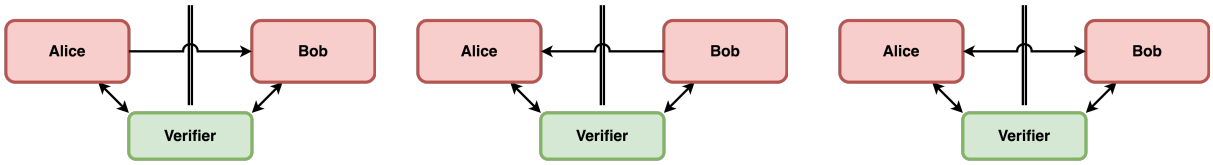
Namely, Bob's output causally precedes Alice's input ($b \preceq x$)*.*

[12] Communication complexity simply is the minimum number of bits Alice and Bob need to communicate to be able to compute a boolean bivariate function $f(x,y)$ where the binary string x is known to Alice and the binary string y known to Bob.

[13] Trivial means communication complexity is just one bit.

The final strategy we will cover below is complete signalling which defies the idea of non-local games, and it might seem that it reduces the power of the provers back to the complexity class $\mathsf{IP} = \mathsf{PSPACE}$, however, it turns out that because that verifier thinks they are not communicating, but they are signalling, they can cheat the verifier and that gives them the ability to generate stronger correlations[14].

Definition 3.1.17 (Signalling Strategy)**.** *SIG strategies are the channels, Ω_{SIG}, where Alice and Bob can communicate (hypothetically even at speeds faster than the speed of light) hence there are no restrictions on $\Omega_{SIG}(a, b \mid x, y)$.*



(a) Right Signalling (b) Left Signalling (c) Signalling Strategy

Figure 3.4: Signalling Strategies Schematic Diagrams

Theorem 3.1.8 (R-SIG $\cap$ L-SIG = NO-SIG)**.** *[CY18]*

Theorem 3.1.9 (R-SIG $\cup$ L-SIG $\subset$ SIG)**.**

A Venn diagram summarizing the relationship between the various strategy correlation sets introduced in this section is in Figure 3.5.

Concrete T Strategy Examples: First recall Figure 2.21. Let us consider the Entangled Quantum state micro action. If players are using a QPE strategy, and we specify the exact micro-action—meaning specifying the quantum state the players share, say $|\Psi+\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|00\rangle_{AB} + |11\rangle_{AB}\big)$, the exact projective measurements used, say X-basis and Z-basis measurements, and on which part of the state will these measurements be applied for all possible micro strategies any player makes, say each performs an X measurement on their qubit if their input was 1, and a Z measurement if their input was 0, then this is a concrete QPE strategy. Another example is if players are using a NOSIG strategy. If they specifically agree to only use PR-Boxes, that is a concrete NOSIG strategy. On the other hand, if they decided to use PR-Boxes in the first round of the game, then an n-input-output-no-signalling box in the second round, then this is another different concrete NOSIG strategy.

[14] In fact, the output of the provers could be perfectly correlated, because the provers can send their questions to each other and they know from their agreed upon strategy how each will act based on these inputs.

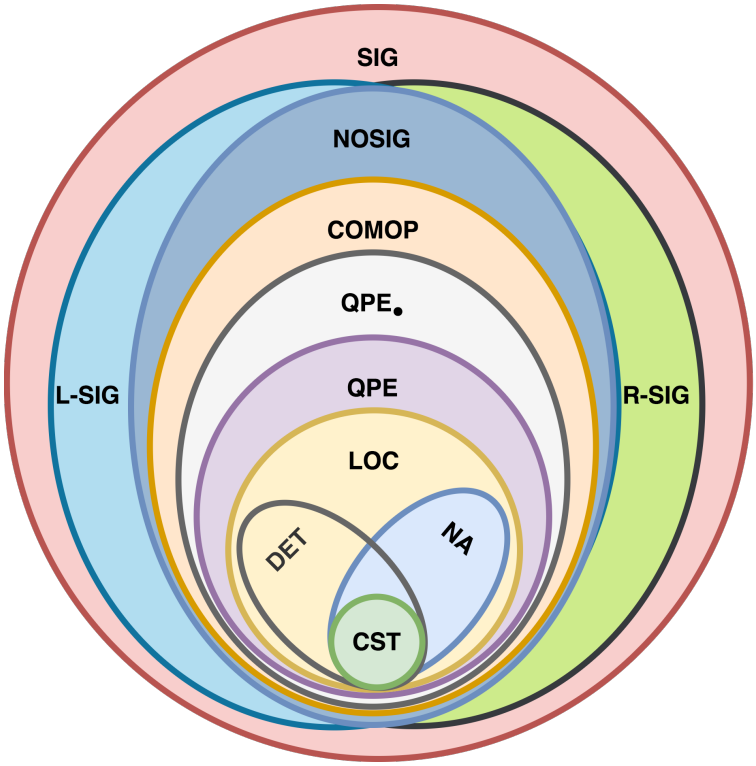


Figure 3.5: Venn Diagram of discussed Strategy Correlation Sets

3.2 Two Player Games and their Strategy Values

Building upon definition 2.8.3, we will now give the two main concrete examples from the literature for *Two Player Non-Local games*. Observe that a game is specified by assigning specific definitions to the tuple $\langle \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \Xi, W \rangle$.

3.2.1 Understanding the CHSH Game

The CHSH game—named after Clauser, Horne, Shimony, and Holt in [Cla+69]—is based on an important milestone in quantum information theory exemplifying Bell's Inequalities which cannot be violated by any local hidden variable theory, yet quantum entanglement has be shown to violate said inequalities both mathematically and experimentally (see section 2.6.1).

Definition 3.2.1 (CHSH Game)**.** *Any Two Player Non-Local game*[15] *with:*

- $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B} = \{0, 1\}$
- Ξ *is the uniform distribution over* $\mathcal{X}$ *and* $\mathcal{Y}$

[15] See the Game Theory review in 2.8.

Table 3.1: Cases where $W = 1$ for the CHSH Game.

x	y	$a \oplus b$
0	0	0
0	1	0
1	0	0
1	1	1

- *For* $x \in \mathcal{X},\ y \in \mathcal{Y},\ a \in \mathcal{A},\ b \in \mathcal{B}$, *we define*

$$W = \begin{cases} 1, & \text{if } x \wedge y = a \oplus b \\ 0, & \text{otherwise} \end{cases}$$

The winning function W is a manifestation of Bell's Operator such that the expectation value of S over all possible strategies is proportional to the probability of Alice and Bob winning ($W = 1$) minus the probability of them losing ($W = 0$)[16].

$$\langle \Phi | \, S \, | \Phi \rangle = 4 \cdot \big(Pr[win] - Pr[lose] \big)$$

This can be seen from Table 3.1. Observe that in the first 3 rows Alice and Bob must output $a = b$, while in the last case they must output $a \neq b$. Next observe that for any of the terms in $\langle \Phi | \, S \, | \Phi \rangle$

$$\begin{aligned} \langle \Phi | \, A_x \otimes B_y \, | \Phi \rangle &= \sum_{a,b \in \{\pm 1\}} a \cdot b \cdot \mathbb{P}(a, b \mid x, y) \\ &= \sum_{a,b \in \{\pm 1\}} a \cdot b \cdot \langle \Phi | \, A_x^a \otimes B_y^b \, | \Phi \rangle \end{aligned}$$

Putting these two observations together we deduce the correspondence between the CHSH game's winning function and Bell's Operator.

The probability of Alice and Bob winning the game using some strategy $|\Phi\rangle$ and measurements $\{A_x\}_{x \in \{0,1\}}$ and $\{B_y\}_{y \in \{0,1\}}$ is

$$\begin{aligned} Pr[\text{win}] &= \sum_{x,y,a,b} \Xi(x,y) \cdot W(x,y,a,b) \cdot Pr[a, b \mid x, y] \\ &= \frac{1}{4} \sum_{x,y,a,b} W(x,y,a,b) \cdot Pr[a, b \mid x, y] \\ &= \frac{1}{4} \sum_{x,y,a,b} W(x,y,a,b) \cdot \langle \Phi | \, A_x^a \otimes B_y^b \, | \Phi \rangle \end{aligned}$$

$Pr[\text{lose}]$ has the negation of W, it is now simply a direct calculation knowing the winning values for x, y, a, b and substituting for $Pr[\text{win}] - Pr[\text{lose}]$ the deduced formula.

[16] This analysis was covered best in Logan Meredith notes here, and in [Bru+14].

Analysing the strategies of the CHSH Game

- The CHSH game value if we limit ourselves to local hidden variable strategies, $\mathcal{S}_{\text{LHV}}$, is $\text{val}^*_{\text{LOC}}(\mathcal{CHSH}) = \text{val}^*_{\text{DET}}(\mathcal{CHSH}) = \text{val}^*_{\text{NA}}(\mathcal{CHSH}) = 0.75$. The winning strategy is simply Alice and Bob pre-agree to always output the same value (i.e. $a = b = 1$).
- The CHSH game value if we allow quantum entanglement strategies, $\mathcal{S}_{\text{QPE}}$, is $\text{val}^*_{\text{QPE}}(\mathcal{CHSH}) = \cos^2(\pi/8) \approx 0.854$. The winning strategy is using the operators in figure 2.20 and entangled EPR state $|\Phi^-\rangle$.
- The CHSH game value if we allow commuting operator quantum strategies[17]

$$\text{val}^*_{\text{QPE}}(\mathcal{CHSH}) \overset{?}{<} \text{val}^*_{\text{COMOP}}(\mathcal{CHSH})$$

- The CHSH game value if we allow no-signalling strategies, $\mathcal{S}_{\text{NOSIG}}$, is $\text{val}^*_{\text{NOSIG}}(\mathcal{CHSH}) = 1$. The winning strategy is by sharing a PR-Box.

Any strategy involving signalling could always win, because one player could send their input (and output) to the other, which will output an answer resulting in $W(.) = 1$.

3.2.2 Understanding the Magic Square Game

The Magic square game is the second canonical example of a non-local game, it was designed by Mermin and Peres in the 1990's with the objective of having a classical game value strictly lesser than 1, but a perfect (= 1) quantum prior-entanglement game value.

It is important at this point to draw a connection between non-local games and multi-prover interactive proof systems (MIPs). **In Interactive Proofs, Provers are trying to certify to the verifier that the answer to a specific decision problem is YES.**

In Games, Players try to certify a physical property of the states they share or that they are sharing a particular quantum state (i.e. an EPR pair).

In a magic square, players are equipped with a 3×3 matrix $\mathcal{M}$ with the element in the i^{th}-row and j^{th}-column $\mathcal{M}_{i,j} \in \mathbb{F}_2$, s.t. each row i should have even parity (aka. $\sum_j M_{i,j} = 0$), while each column j should have odd parity (aka. $\sum_i M_{i,j} = 1$). By a simple parity argument (and recalling that even+even=even and odd+odd=even), it should be clear that the sum of all the matrix elements cannot be both even and odd, hence such a square does not exist. However, in the magic square game, the verifier asks Alice for some row at random, and asks Bob some column at random, and for them to win the game they should return the elements in the asked row (for Alice) and column (for Bob) satisfying the above conditions, with the condition that the intersecting element between their queries needs to be the same (the consistency constraint).

Definition 3.2.2 (Magic Square Game)**.** *A Two Player Non-Local game with:*

- $\mathcal{X}, \mathcal{Y} = \{0, 1, 2\}$

[17] For finite Hilbert space COMOP, it is known that the CHSH game value is the same for QPE and COMOP.

- $\mathcal{A}$, $\mathcal{B} = \{0,1\}^{\times 3}$
- Ξ *is the uniform distribution over* $\mathcal{X}$ *and* $\mathcal{Y}$
- *For* $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $a \in \mathcal{A}$, $b \in \mathcal{B}$, *we define*

$$W = \begin{cases} 1, & \text{if } \bigoplus_{i=0}^{2} a_i = 0 \text{ and } \bigoplus_{j=0}^{2} b_j = 1 \text{ and } a_y = b_x \\ 0, & \text{otherwise} \end{cases}$$

where a_i *is the* i^{th} *bit in Alice's 3-bit answer, similarly for Bob.*

The magic square game is part of a family of games called the linear constraint system games, where the linear constraint equations are the ones found in the condition of the winning function W above.

Analysing the strategies of the Magic square Game

- The Magic square game value if we limit ourselves to non-adaptive strategies, $\mathcal{S}_{\text{NA}}$, is $\text{val}^*_{\text{NA}}(\mathcal{MAGIC}) = 6/9$. The winning strategy is Alice always outputs $a = 110_{\text{binary}}$, and Bob outputs $b = 111_{\text{binary}}$ where if Bob gets asked $y = 0, 1$ they win, but if he was asked $y = 2$ they lose.
- The Magic square game value if we limit ourselves to local hidden variable strategies, $\mathcal{S}_{\text{LHV}}$, is $\text{val}^*_{\text{LOC}}(\mathcal{MAGIC}) = \text{val}^*_{\text{DET}}(\mathcal{MAGIC}) = 8/9$. The winning strategy is Alice and Bob pre-agree on

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & \alpha \end{pmatrix}$$

  where Alice substitutes $\alpha = 1$ if asked $x = 2$ and Bob substitutes $\alpha = 0$ if asked $y = 2$. They lose only when $x = y = 2$.
- The Magic square game value if we allow quantum entanglement strategies, $\mathcal{S}_{\text{QPE}}$, is $\text{val}^*_{\text{QPE}}(\mathcal{MAGIC}) = 1$. The winning strategy is:
  1. Map $\{0,1\} \to \{1,-1\}$ for the elements of matrix $\mathcal{M}$ and addition with multiplication in the definition of W. This is an equivalent formulation.
  2. Associate with each element of $\mathcal{M}$ a Hermitian operator (an observable) $O_{i,j} \in \mathbb{C}^4$ with ± 1 eigenvalues s.t.
     - $\forall i$, $\Pi_{j=0}^{2} O_{i,j} = I$ and $[O_{i,j}, O_{i,j'}] = 0$ [18]
     - $\forall j$, $\Pi_{i=0}^{2} O_{i,j} = J$ and $[O_{i,j}, O_{i',j}] = 0$, where J is some operator that will represent -1.
     - $O_{i,j}^2 = I$ and $J^2 = I$

     Using representation theory, we can figure out what $O_{i,j}$ we should use, namely we think of $O_{i,j}$ and J as the generators of a group (called the "solution group"),

[18] Whenever all operators appearing in the same equation commute, this implies an operator solution. We require an operator solution to be able to measure all observables in an equation at the same time. In Linear Constraint System Games, $\exists$ an operator solution $\iff$ a perfect strategy [CLS17].

and we use standard techniques to find a representation that maps $J \to -I$ (turns out this representation is unique up to local isometries[19]), and the solution group satisfying it is the tensor product of 2 Pauli Groups[20] $\mathcal{P}^{\otimes 2}$. Imagine each cell in $\mathcal{M}$ to contain the operator $O_{i,j}$:

$$\mathcal{M} = \begin{pmatrix} Z \otimes I & I \otimes Z & Z \otimes Z \\ I \otimes X & X \otimes I & X \otimes X \\ Z \otimes X & X \otimes Z & Y \otimes Y \end{pmatrix}$$

3. Alice and Bob then share the maximally entangled state

$$|\Phi\rangle_{A,B} = \frac{1}{2}\Big(|00\rangle_{A,B} + |11\rangle_{A,B} + |22\rangle_{A,B} + |33\rangle_{A,B} \Big) \in \mathbb{C}^4 \otimes \mathbb{C}^4$$

this state is analogous to the EPR state in $\mathbb{C}^2 \otimes \mathbb{C}^2$, where $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ are an orthonormal basis[21]). Now because the solution group is $\mathcal{P}^{\otimes 2}$, then $|\Phi\rangle$ is just two EPR pairs.

4. When Alice (analogously for Bob) receives question x signifying a row in $\mathcal{M}$, she measures her 2-qubits, $|\Phi\rangle$, using $O_{x,0}$, $O_{x,1}$, and $O_{x,2}$ each will produce either ± 1, but collectively will have a $+1$ product, and because Alice and Bob's use the same observable $O_{x,y}$ at the intersection of their row and column and this observable commutes with both the operators in its row and column, both will have the same eigenvalue (because they are sharing an EPR state) and hence satisfy the consistency constraint.

If in the QPE strategy we required that all observables $O_{i,j}$ pair-wise commute, then we can measure all of them simultaneously which implies that that would have reduced the strategy to the classical LHV one which has game value only 8/9. Furthermore, obviously the commuting operator strategy is the same as the quantum prior-entanglement strategy and both achieve game value 1. And w.l.o.g, if Alice can signal Bob, then they can always win this game.

Another equivalent variant of the Magic Square game is one where Alice gets asked to give the 3 elements in a row *or a column*, while Bob gets asked to output the value of a specific element in the row or column that Alice was asked. This game is asymmetric since Alice and Bob receive different kinds of questions and respond with different kinds of answer, yet more or less, similar strategies could be employed in this game to give the same game values as above.

[19] Isometries were introduced when defining quantum channels in the Background chapter, where we paired our system with an environment/garbage system and then trace it out or ignore it.

[20] The Pauli Group $\mathcal{P}$ is the group generated by the Pauli Matrices and identity (X, Y, Z, I) introduced in the Quantum Computation section where X and Z anti-commute ($XZ = -ZX$), and operators on a qubit (i.e. $\mathbb{C}^2$). The group thus contains elements $\{\pm i \cdot g\}$ where $g \in \{X, Y, Z, I\}$.

[21] For $i = 0, 1, 2, 3$, $|i\rangle$ could be thought of as the binary encoding of this state, meaning $i = 00_{\text{binary}}, 01_{\text{binary}}, 10_{\text{binary}}, 11_{\text{binary}}$, so $|i\rangle$ is really 2-qubits (i.e. $\in \mathbb{C}^4$

3.2.3 Understanding the GYNI Game

The Guess Your Neighbour's Input (GYNI) game [Alm+10] is a non-local game with two or more players that are arranged in a circle while space-like separated, where each player receives an input and is required to output a correct guess of their left neighbour's input. In the GYNI game, LHV and quantum strategies always have the same game value, however no-signalling strategies achieve strictly higher game value for three or more players and specific input distributions Ξ. We will cover here the definition of the game for two players and the best classical and quantum strategies, and we will expound on this in the next chapter when extending non-local games to more than two players.

Definition 3.2.3 (GYNI Game)**.** *Any Two Player Non-Local game with:*

- $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B} = \{0, 1\}$
- Ξ *is allowed to be any distribution over* $\mathcal{X}$ *and* $\mathcal{Y}$
- *For* $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $a \in \mathcal{A}$, $b \in \mathcal{B}$, *we define*

$$W = \begin{cases} 1, & \text{if } a = y \text{ and } b = x \\ 0, & \text{otherwise} \end{cases}$$

Because this game by design requires players to signal one-another, and we will focus on no-signalling strategies. Hence, we relax the definition of the game value to be the expected game value over all possible inputs:

$$\text{val}^*(\mathcal{GYNI}) := \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \Xi(x, y) Pr[a = y, b = x \mid x, y]$$

Notation for analysing GYNI game: Let $\langle u, v \rangle$ denote the string concatenation of some u, v with $u \in \mathcal{X}, v \in \mathcal{Y}$. If we call the string $s = \langle u, v \rangle$, then we can index elements in string s as follows: $s_0 = u$ and $s_1 = v$. Let $\overline{s}$ denote the bit-wise negation of the elements[22], $\overline{s} = \langle \overline{u}, \overline{v} \rangle$. Equality between strings, s and q, is an element-wise equality (i.e. $s = q$ iff $s_0 = q_0$ and $s_1 = q_1$).

Key Observation: Let $\lambda = \langle u, v \rangle$ be some string, and s be the string of the players inputs, $s = \langle x, y \rangle$, then if $s \neq \lambda$ and $t \neq \overline{\lambda}$ then $\exists$ index i s.t.

$$s_i = \lambda_i \text{ and } s_{i+1 \mod 2} \neq \lambda_{i+1 \mod 2}$$

Analysing the strategies of the GYNI Game

- The GYNI game value if we limit ourselves to local strategies, $\mathcal{S}_{\text{LOC}}$, is $\text{val}^*_{\text{LOC}}(\mathcal{GYNI}) = \max_{x,y}[\Xi(x, y), \Xi(\overline{x}, \overline{y})]$. The winning strategy is Alice and Bob pre-agree on some string λ, where Alice outputs

$$a = \begin{cases} \lambda_1, & \text{if } x = \lambda_0 \\ \overline{\lambda}_1, & \text{otherwise (aka. } x = \overline{\lambda}_0) \end{cases}$$

[22] $\overline{x} = x \oplus 1$

and Bob outputs

$$b = \begin{cases} \lambda_0, & \text{if } y = \lambda_1 \\ \overline{\lambda}_0, & \text{otherwise (aka. } y = \overline{\lambda}_1) \end{cases}$$

Therefore, $Pr[a = \lambda_1, b = \lambda_0 \mid \lambda] = Pr[a = \overline{\lambda}_1, b = \overline{\lambda}_0 \mid \overline{\lambda}] = 1$. However, if $s = \langle x, y \rangle \neq \lambda$ and $s \neq \overline{\lambda}$, then $Pr[a = y, b = x \mid x, y] = 0$ due to the key observation above. Thus the game value for a specific λ is $\Xi(\lambda_0, \lambda_1) + \Xi(\overline{\lambda_0}, \overline{\lambda_1})$, and the optimal is the maximum over all λ as claimed.

- The GYNI game value if we allow quantum entanglement strategies, $\mathcal{S}_{\text{QPE}}$, is $\text{val}^*_{\text{QPE}}(\mathcal{GYNI}) \leq \text{val}^*_{\text{LOC}}(\mathcal{GYNI})$. The winning strategy is Alice and Bob share and EPR pair $|\psi\rangle$, and projective measurements $\{M^a_x\}_{x \in \mathcal{X}}$ for Alice and $\{M^b_y\}_{y \in \mathcal{Y}}$ for Bob, where

$$Pr[a = y, b = x \mid x, y] = \langle \psi | \, M^y_x \otimes M^x_y \, | \psi \rangle := \langle \psi | \, M_{x,y} \, | \psi \rangle$$

In [Alm+10], they showed that if we constraint Ξ to be uniformly random on all input strings whose elements sum is even, then the players can exploit this constraint using a no-signalling strategy to beat the classical and quantum strategies for three or more players. Obviously, if it is a two player GYNI game with this constraint, the players would always win by just returning their input as an output.

There are many non-local games in the literature, we will mention two that we found interesting. The RGB game [CC19], is very simple to explain to anyone outside the field. The I3322 game [PV10], is a game where the larger the Hilbert spaces Alice and Bob could have, the better their game value for QPE strategies.

Chapter 4

Main Result

In this chapter we generalize previous definitions of non-local games from 2 to n provers / players. We generalize strategies in this domain allowing heterogeneous strategy choices among the players (i.e. some players could be QPE and others could be No-Sig, some could have mixed strategies across both). We end this chapter introducing Crépeau's conjecture and proving it. The implications of the theorem are explicitly stated in 5.3.

4.1 Generalization of Non-Local Games

A note on terminology:

- Throughout this chapter we will use *player* and *prover* to mean the same thing. However, whenever we use *player*, the context can equally apply to the *verifiers*, or *simulators* used in zero-knowledge proofs, since we consider the verifiers to be players in the context of zero-knowledge proofs, as mentioned in the Game Theory background.
- Another reminder is that the terms *strategy*, *channel*, and *correlation* are loosely used interchangeably, each had a deeper meaning and interpretation that we discussed in earlier chapters, but for the purpose of this chapter they are sometimes used as synonyms.

Definition 4.1.1 (Relativistic Multi-Player Non-Local Game)**.** *The game is composed of n provers and n verifiers, where $n \in \mathbb{Z}$ and $n \geq 1$. Each prover $u \in [n]$, has an at most countable set of questions, $\mathcal{Q}_u$, they could get asked and an at most countable set of answers, $\mathcal{A}_u$, they can provide. Each prover u is connected to verifier u with a (bidirectional) classical communication channel. The n provers need not be symmetrical and they can employ different strategies from one another throughout the game.*

The game consists of a number of consecutive rounds $R > 0$. The verifiers intervene[1] *before each round, r s.t. $1 \leq r \leq R$, and sample questions, $\{q_{u,r}\}_{u\in[n]}$, from a distribution Ξ. The distribution Ξ is over the prover's question sets $\mathcal{Q}_1 \times ... \times \mathcal{Q}_n$ and could possibly depend*

[1] This is not typical in the non-local games literature. We expound of the differences in a remark following this definition.

on previous rounds. The verifiers intervene after the final round, R, and use the pre-defined winning predicate to determine if the provers win the game or lose.

$$W(a_{11}, ..., a_{n1}, ..., a_{1R}, ..., a_{nR}, ..., q_{11}, ..., q_{n1}, ..., q_{1R}, ..., q_{nR}) \in \{0, 1\}$$

where $a_{u,r}$ is prover u's answer in the r^{th} round to the question $q_{u,r}$.

Each round r consists of 2 phases:

1. *(Huddle Phase) The n verifiers can (optionally) choose to intervene, share answers from the previous round, $r-1$, if $r \geq 2$, and sample questions for this round r. This implies that the n provers will be able to huddle and agree on a strategy to answer questions of this round of the game (which could involve sharing resources).*
2. *(Exam Phase) Next the n verifiers separate from one another to publicly known space-time locations and broadcast their questions. Each prover u needs to be in close vicinity to their verifier in order to receive their question $q_{u,r}$ in a timely manner and be able to respond in the allotted time. This spatial separation and time constraint enables verifier u to ensure that answer $a_{u,r}$ was received before any $q_{v,r}$ could reach verifier u if it were travelling at the speed of light c, for all $v \in [n]$ and $v \neq u$.*

At the end of the R^{th} round, if any answer was not provided to a verifier in the allotted time, the provers automatically lose. Otherwise, the verifiers compute $W(.)$, which decides whether the provers lose ($W = 0$), or win ($W = 1$).

Remarks:

1. This definition extends definition 2.8.3 with the relativistic variant depicted in Figure 2.22 to the multi-prover setting.
2. The huddle phase is optional. If the verifiers in a specific game decide not to allow huddling, they have 4 options:
   - Sample all the questions before the first round. They will have to ask their first question, receive an answer, then ask their second question receive the second answer, and so on, but they will have to be far enough apart, in order for verifier u to receive the answer to their *last* question, before the *first* question from all other verifier $v \neq u$ could reach them if moving at the speed of light. This option does not allow adaptive verifiers.
   - Each samples independent questions (i.e. $\Xi(Q_1, .., Q_n) = \Xi(Q_1) \times .. \times \Xi(Q_n)$) for the R rounds. This again requires a larger distance between the verifiers, but allows for adaptive questions.
   - Use non-local strategies (similar to the ones the provers use) to be able to compute more complex distributions.
   - Delegate the question asking to the provers (introspection) which allows adaptive questions and allows the questions asked at each round to be correlated, however introspection is only possible for a limited number of distributions.

3. Point (2) makes the distance the verifiers have to be separated by much longer making the protocol less practical.
4. Our definition is more general, and reduces to the typical definitions in the literature if the verifiers decide not to allow the huddle phase.

4.2 Two Ways to View Non-Local Strategies

Let us take a detour to understand two ways of modeling strategies in these kinds of games. As stated in previous chapters, strategies involve sharing resources and using these resources, together with the input questions, to generate outputs via an algorithm (modelled as a TM). However, we also looked at strategies in a blackbox viewpoint (i.e. the PR-Box for example). Even a QPE strategy could be looked at solely in terms of the correlation $\Omega_{\text{QPE}}(. \mid .)$ generated from provers playing the game—that is, we could have given this QPE correlation to the players as a non-local blackbox, and they would have been able to win the game just as before when they shared an entangled quantum state and had agreed on measurements to apply in each possible input scenario.

We name these two non-local strategy viewpoints *the Blackbox Model* and *the Protocol Model*. The table below is a comparison between these two models. We first define how we think about strategies in each of the two models, then we explain how players communicate in these models. Afterwards, we expound on how the strategies introduced in section 3.1 are viewed in each model. The last three rows of the table showcases the resultant strategy in each model from the combinations of the strategies in section 3.1. The resultant strategy of these combinations will depend on (1) the way players communicate (View of the World row in the table) and (2) the way we defined the strategies for each model.

Model / **Metric**	**BlackBox Model**	**Protocol Model**
Definition	A box modeling the channel for n provers has n inputs and n outputs, and the relation between outputs to inputs is defined by a conditional probability distribution. Each player has a single $\langle \text{input}, \text{output} \rangle$ pair.	A protocol enforcing restrictions on players (location, time to reply) to implement the required conditional probability distribution.
View of the World	No one can communicate with anyone else, unless there is a blackbox shared between them.	Everyone can communicate with everyone else at speeds less than c, unless restrictions are imposed[2].

[2]By definition, in non-local games verifiers add a no-signalling constraint, unless signalling strategies are requested by the provers.

Quantum Prior-Entanglement (QPE)	We abstract away the details of the quantum computation and the shared state, and say that players sharing this box, can produce one of correlations that local quantum players sharing a specific quantum state can produce.	We think about players sharing the physical qubits, and applying quantum gates (that could be classically controlled) and finally apply measurements on their part of the quantum state and the output will exhibit the necessary correlations. Players are forced to be far away from each other for the full duration of the round by the techniques of relativistic non-local games[3].
No-Signalling	We imagine the players sharing this box (PR-Boxes for a two player example) s.t. their outputs may produce these super-quantum correlations (aka. no-signalling and causal).	We imagine a relativistic non-local game scenario, that enforces no faster than the speed of light communication (aka no-signalling). Furthermore, players may use any "hypothetical" no-signalling channel[4] (resource) to achieve the required output correlations.

[3]Because no-signalling correlations stronger than those allowed by QPE are hypothetical, we assume that separating the verifiers (hence the provers) is enough to restrict provers to QPE. See No-signalling below for how we allow provers to achieve such correlations.

[4]At the time of this writing, we do not know if this no-signalling resource can be in fact physically implemented, but we think of it analogously to quantum entanglement (where one shares some particles and apply an operation on them that produces an output producing these correlations.)

One-Way Signalling (from U to V)	Providing this asymmetric box between groups of players, $U, V \subset [n]$, $U \cap V = \emptyset$, and the output of the collection of players in V might have causal dependence on input of the collection of players in U, but not the other way around. Note you can define U and V whichever way you want, but it will defeat the purpose of the box if player $p \in U$ and $p \in V$ for example.	Because everybody can communicate with everybody else given enough time by definition in this model, we must to enforce a one way no-signalling channel from U to V to implement one-way signalling. To achieve this, we follow the 2 player idea in Figure 2.22 plot (c). That is, we again separate the players by various distances $D_{u,v}$ and require that each player returns their answers after Δ_i time from receiving their question. The Δ_v for players $v \in V$ will be shorter than that of the Δ_u for players $u \in U$, namely $\Delta_u \geq \Delta_v + \frac{D_{u,v}}{c}$ and $\Delta_v < \frac{D_{u,v}}{c}$, that way players in V will not have time to receive any messages from players in U. This could be extended to accommodate any complicated one-way-signalling channels among multiple groups of players[5].
Signalling	A normal communication channel[6] is supplied between players.	No channel is needed, this is by definition, as long as verifiers give players enough time (possible light years), any message would reach everyone.

[5]There is a slight nuisance that needs mentioning. One-way signalling channels in multi-player games behaves a bit like threshold secret sharing introduced in the cryptography background section. While the collective output of players in V has a dependence on the collective input of players in U, a possible one-way signalling correlation might not allow any individual player $v \in V$ to be able to understand this dependence except when joined with the appropriate subset of player in V.

[6]thought of as a correlation or conditional probability distribution as discussed in the information theory background section.

Combination of No-signalling and QPE strategies	Because QPE is a special case of NOSIG, both boxes can coexist. Just supply the required boxes to the designated players. One crucial point is that these black-boxes are like gates in a circuit, the can only be applied sequentially or in parallel but we cannot do boxes of boxes.	In the protocol model of no-signalling and QPE, players are space-like separated for the duration of the round and hence they still exhibit their quantum and no-signalling correlations, and can mix between them in ways not possible in the blackbox model. This might perhaps provide correlations stronger than each individual strategy. For example, a partial measurement of the players qubits in a quantum circuit could be fed into a PR-box, whose output could control the operation of a quantum gate applied later in the circuit, etc.
Combination of One-Way Signalling and No-Signalling strategies	Players become one-way signalling, because they can always use their one-way-signalling box to signal, and having the no-signalling box does not prevent signalling.	Players will be no-signalling, because enforcing time restrictions for no-signalling will be more stringent than those required for one way signaling (which drops the time constraint in one direction), this will force the players to reply before being able to receive messages from anyone they are connected to making the total channel a no-signalling one.
Combination of Signalling and One-Way-Signalling strategies	Players become signalling.	Players become one-way-signalling because it has more stringent time restrictions by the verifiers.[7]

While the blackbox model and the protocol (real world practical implementation) model are

[7]This is assuming the verifiers pick the smallest response time among the strategies the players are using. If they picked the maximum response time, the players would become signalling. However, following our convention to pick the more stringent response time when combining one-way-signalling and no-signalling above, we say here the resultant strategy will be one-way-signalling.

equivalent, in the signalling channels the former allows the provers the power to choose their shared resources without depending on the verifiers, while the latter requires the verifiers to relax their time constraints to allow the provers to communicate. It seems that with certain strategies the blackbox model is more appropriate, while in others thinking of the practical implementation eases the analysis.

Viewing one-way signalling strategies from the perspective of the protocol model will be used in our proof below (lemma 4.4.1) and so it is worth expanding a bit more on it here. As we saw in the protocol model viewpoint, one-way signalling, from players in set U to players in set V, is implicitly a specific configuration of no-signalling channels from players in V to ones in U. Because no-signalling channels do not allow signalling, they have a zero capacity in the direction from $V \to U$. We will rely on this point to prove that players $U \cup V$ sharing entanglement and that are connected by a one-way signalling channel from $U \to V$ cannot signal from $V \to U$, namely entanglement cannot increase the capacity in the direction $V \to U$.

4.3 Generalizing Non-Local Strategies

We can now think of the physical resources that the provers can be equipped with to implement various strategies.

Definition 4.3.1 (Strategy Resources)**.** *Players pick from the below resources to enable them to achieve their strategies.*

- *Turing Machine*
- *Classical Communication Channel*
- *Quantum Computer (Universal Set of Quantum Gates / Measurement / QRAM[8])*
- *Qubits*
- *One-way Quantum Communication Channel*
- *(Hypothetical) U-V No-Signalling Channel*
- *(Hypothetical) U-V Faster-than-light-Signalling Channel*

Let us now define the generalized strategies using such resources formally below.

[8] implementing a quantum memory is unknown, publicly at least, at the time of this writing.

Notation:

- In all below definitions, capital letter X_i denotes a random variable over elements of player i's question set $\mathcal{Q}_i$, while lower letter x_i denotes any such element. Capital letter Y_i denotes a random variable over elements of player i's answer set $\mathcal{A}_i$, while the lower letter y_i denotes any such element.
- We write $\Omega_{\mathrm{S}}(Y_1 = y_1, .., Y_n = y_n \mid X_1 = x_1, .., X_n = x_n)$ to denote the probability mass function (PMF) of the probability distribution $\Omega_{\mathrm{S}}(Y_1, .., Y_n \mid X_1 = x_1, .., X_n = x_n)$ where Ω_{S} is a probability measure for the strategy S. To contrast this with other notations, let us take the discrete Poisson distribution as an example. The probability distribution is called Pois(λ), while the PMF is written as $P[X = x] \equiv p_X(k) = \frac{\lambda^k \exp^{-\lambda}}{k!}$, where P is the probability measure.

Definition 4.3.2 (LOC Strategy)**.** *A correlation $\Omega_{LOC}(Y_1, ..., Y_n \mid X_1, ..., X_n)$ is said to be local if there exists an at most countable set $\mathcal{R}$ (denoting the shared randomness) with R being a random variable over elements of $\mathcal{R}$ following the PMF $P(R = r)$ with $r \in \mathcal{R}$, and a bijection $\pi : \mathbb{N}^+ \to \mathcal{R}$, and n functions $f_i : X_i \times R \to Y_i$ s.t.*

$$\Omega_{LOC}(Y_1 = y_1, .., Y_n = y_n \mid X_1 = x_1, .., X_n = x_n) = \lim_{k\to\infty} \sum_{j=1}^{k} P(R = \pi(j)) \cdot \mathbb{1}_{(\bigcap_i \ y_i = f_i(x_i, \pi(j)))}$$

Definition 4.3.3 (QPE Strategy)**.** *A correlation $\Omega_{QPE}(Y_1, ..., Y_n \mid X_1, ..., X_n)$ is said to be quantum prior-entanglement if there exists*

- *An at most countable set $\mathcal{D}$ (denoting Hilbert space dimensions) with D being a random variable over elements of $\mathcal{D}$ following the PMF $P(D = d)$ with $d \in \mathcal{D}$.*
- *A bijection $\pi : \mathbb{N}^+ \to \mathcal{D}$.*
- *Hilbert spaces, $\mathcal{H}^{(d)}$, for each quantum player u and dimensions $d \in \mathcal{D}$.*
- *Quantum states $|\Phi^{(nd)}\rangle \in \bigotimes_{u=1}^{n} \mathcal{H}^{(d)}$ for each $d \in \mathcal{D}$ as agreed upon by the players.*
- *Sets $\{M_x^{(d,u)}\}_{x\in\mathcal{X}_u}$ for each player u and dimension $d \in \mathcal{D}$, where $M_x^{(d,u)} = \{N_{x,y}^{(d,u)}\}_{y\in\mathcal{Y}_u}$ is a projective measurement over $\mathcal{H}^{(d)}$.*
- *Sets $\{U_x^{(d,u)}\}_{x\in\mathcal{X}_u}$ for each player u and dimension $d \in \mathcal{D}$, where $U_x^{(d,u)}$ is a unitary operator on $\mathcal{H}^{(d)}$.*

such that:

$$\Omega_{QPE}(Y_1 = y_1, .., Y_n = y_n \mid X_1 = x_1, ..., X_n = x_n) = \lim_{k\to\infty} \sum_{d=1}^{k} P(D = \pi_d) \cdot \langle \Phi^{(n\pi_d)} | \bigotimes_{u=1}^{n} \left[(U^\dagger)_{x_u}^{(\pi_d,u)} \ N_{x_u,y_u}^{(\pi_d,u)} \ U_{x_u}^{(\pi_d,u)} \right] |\Phi^{(n\pi_d)}\rangle$$

where π_d is shorthand notation for the bijection map $\pi(d)$, and all $\otimes$ will be 'spatial tensor products' which use the smallest norm of all possible norms.

We explain this definition as follows, the quantum players can share as much entanglement between any subset of them as they agree in the Huddle phase. The perform unitary

operations on their qubits then perform a general measurement. This yields the quantum entanglement output distributions. Notice that we made all players having the same Hilbert space dimension d, this is because even if a player needed only a Hilbert space of lower dimension $d' < d$, then they can ignore the unneeded dimensions from their d-dimensional Hilbert space.

Definition 4.3.4 (U-V No-Signalling Strategy (UV-NOSIG))**.** *For n-players, for specific $U, V \subset [n]$, where $U \cap V = \emptyset$, we say that a correlation, $\Omega_{UV\text{-}NOSIG}(. \mid .)$, is no-signalling from players in U to players in V iff $\forall\ \alpha_{u\in U}$, $\beta_{u\in U}$, and $\gamma_{v\in V}$*

$$\sum_{Y_{k\in\overline{V}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{v\in V} = \gamma_v, X_{u\in U} = \alpha_u) = \sum_{Y_{k\in\overline{V}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{v\in V} = \gamma_v, X_{u\in U} = \beta_u)$$

where $\overline{V} = [n] \setminus V$ and $X_{v\in V} = \gamma_v$ is shorthand notation listing all random variables $X_{v'}$ of player $v \in V$ with the corresponding value γ_v for each player.

Furthermore, we define the set $W = \{\text{player } w \mid w \in \overline{U \cup V}\}$[9], we apply a triangle rule, where U can signal W as long as we have a W-V No-Signalling channel[10]*. Or if W signals V, then we require that we have a U-W No-Signalling channel.*

Mathematically, in addition to the above constraint on $\Omega_{UV\text{-}NOSIG}(. \mid .)$, we require that at least one of the following two constraints to be satisfied to call $\Omega_{UV\text{-}NOSIG}(. \mid .)$ a U-V No-Signalling correlation:

- *W-V No-Signalling Strategy: $\forall \lambda_{w\in W}$, $\mu_{w\in W}$, and $\rho_{v\in V}$*

$$\sum_{Y_{k\in\overline{V}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{v\in V} = \rho_v, X_{w\in W} = \lambda_w) = \sum_{Y_{k\in\overline{V}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{v\in V} = \rho_v, X_{w\in W} = \mu_w)$$

- ***Or** U-W No-Signalling Strategy: $\forall \tau_{u\in U}$, $\chi_{u\in U}$, and $\eta_{w\in W}$*

$$\sum_{Y_{l\in\overline{W}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{w\in W} = \eta_j, X_{u\in U} = \tau_i) = \sum_{Y_{l\in\overline{W}}} \Omega_{UV\text{-}NOSIG}(Y_1, ..., Y_n \mid X_{w\in W} = \eta_i, X_{u\in U} = \chi_i)$$

[9]Note that W could contain the verifier(s) and the external environment if relevant to the analysis, but mostly we will restrict it to the provers.

[10]Recall here we are in the Protocol model, hence the channel (aka. strategy) involves the verifiers applying constraints to enforce that players in W cannot signal players in V and vice versa. Also recall in the protocol model, combining NOSIG strategies and any signalling strategy, resulted in an overall NOSIG strategy.

All equalities (=) in this definition can be stated as the Kullback-Leibler Divergence = 0 for the two distributions on both sides of the equality.

In plain English, changing the input of players $u \in U$ does not affect the overall distribution of the joint players $v \in V$. It is obvious that the channel's maximum capacity is zero. **It is important to note here that although the output of players in V does not depend inputs of players in U, it is possible if you change an input that it will permute output elements of equal probability, and that would be unnoticeable on the output distribution $\Omega_{\textbf{UV-NOSIG}}(. \mid .)$. That is why we used the KL-Divergence in the equalities above.**

Definition 4.3.5 (U-$\overline{U}$ No-Signalling Strategy)**.** *A U-V no-signalling strategy with $V = \overline{U}$.*

Definition 4.3.6 (No-Signalling Strategy)**.** *The correlation, $\Omega_{NOSIG}(Y_1, ..., Y_n \mid X_1, ..., X_n)$, is said to be no-signalling iff $\forall\ U, V \subset [n]$, where $U \cap V = \emptyset$, there is a U-V No-Signalling Strategy.*

Again we reiterate that a verbal explanation of these definitions is that for any two subsets of the n-players, the output of each is independent of any value of the inputs to the other subset. In other words, if we split the n-players to two subsets P and Q, then we cannot change the resulting distribution from collection of players in Q by tweaking the input of any player (or collection of players) in P. and although tweaking the input of anyone in Q does not change the output distribution of P, it can permute it/re-label it. This is not considered signaling because the collective output distribution is the same.

Notation: For any random variable R and set $V = \{v(1), v(2), .., v(|V|)\}$, we write $R_{v \in V}$ to denote $R_{v(1)}, R_{v(2)}, ..., R_{v(|V|)}$.

Definition 4.3.7. *Let U, V be two disjoint sets of players. A direct consequence of the definition of NOSIG strategies and the above discussion, is that the marginal for any no-signalling distribution $\Omega(. \mid .)$ on outputs $Y_{v \in V}$ is independent on the inputs $X_{u \in U}$. Namely:*

$$\sum_{u \in U} \Omega(Y_1, ..., Y_n \mid X_1, ..., X_n) = \Omega_{Y_{v \in V}}(Y_{v \in V} \mid X_{v \in V}, X_{u \in U}) = \Omega_{Y_{v \in V}}(Y_{v \in V} \mid X_{v \in V})$$

where $\Omega_{Y_{v \in V}}(.)$ denotes the marginal.

Another important point, is that in our definition of the Multi-Player Non-Local Games, we allowed provers to huddle in between rounds. In the case of No-SIG strategies, one might think that the provers discussing in between rounds would entail signalling. We argue that this is not the case (see Claim 4.3.0.1).

Definition 4.3.8 (U-V Signalling Strategy)**.** *Typical communication channels are bi-directions. For one way communication channels to exist from U to V, we are implicitly stating that we have a V-U No-Signalling strategy in place to block communication in the direction $V \to U$.*

In other words, in the Protocol Model, unless player i is space-like separated from player j, we assume they can communicate unless a No-Signalling strategy is present to block it.

Definition 4.3.9 (SIG Strategy)**.** *$\Omega_{SIG}(Y_1, ..., Y_n \mid X_1, ..., X_n)$ is said to be a Signalling correlation, if $\forall\ U, V \subset [n]$ where $U \cap V = \emptyset$, there is a U-V Signalling strategy.*

Definition 4.3.10 (Strategy Classes)**.** *Multi-Players in non-local games could be equipped with various resources which gives the group the ability to produce various correlations. We define here homogeneous strategies, that is, ones where all provers are using identical strategy types. As in the Lead Up Work chapter, for strategy S, the strategy class is $\mathbb{S}$.*

- *($\mathbb{LOC}$ / $\mathbb{LHV}$) pronounced local, local hidden variable, or classical. The class of all distributions where each player has a Universal Turning Machine, which means they can store/use random strings, and their strategies can be probabilistic.*
- *($\mathbb{QPE}$) pronounced quantum prior entanglement. The class of all distributions that can be produced by players that use a LOC strategy. In addition, each player has a quantum computer and an at most countable number of qubits, that could be entangled with (collections of) qubits of other players.*
- *($\mathbb{T}$otal-$\mathbb{PR}$-$\mathbb{BOX}$) The class of all distributions that can be produced by players that use a LOC strategy. In addition, For each pair of players i and j, player i has access to the input, and the corresponding output, of PR-boxes, and player j has access to the other input/output.*
- *($\mathbb{NOSIG}$) pronounced no signaling. The class of all distributions that can be produced by players that use a LOC strategy. In addition, each player has access to the input and corresponding output of a NOSIG strategy.*
- *(Π-$\mathbb{SIG}$) pronounced pi signaling. Let $\Pi : [n] \to [n]$ be one of the $n!$ permutations of the index labelling the n-players. Then the class of all distributions that can be produced by players using a LOC strategy,[11] in addition, player $\Pi[u]$ has a one-way signalling channel to player $\Pi[u+1]$, where $1 \leq u < n$ and indexing $\Pi[u]$ gives the label for the u^{th} player in permutation Π.*
- *($\mathbb{SIG}$) (pronounced totally signalling.) The class of all distributions that can be produced by players that use a LOC strategy, in addition having a SIG strategy.*

Note:

- Each strategy class $\mathbb{S}$ above contain distributions that are implemented using concrete S-strategies among the players. Each of these concrete strategies can be thought of in two ways as indicated in table 4.2. Namely, you can think of a NOSIG-strategy between n-players as either a NOSIG-box with n-input-outputs (blackbox model), or enforcing a relativistic non-local game scenario where non of the players have enough time to receive a signal for any of the other players and the players share a no-signalling channel. This extends to all other strategy classes.

[11] Note that this definition assumes the protocol model, if we were to define it in the blackbox model, we would force players to have a general n-input-n-output NOSIG box, and add one-way signalling boxes between successive players in the permutation Π.

- Throughout this chapter, Π-SIG strategies will typically be written as Π_j-SIG for some $1 \leq j \leq n!$. This index j tells us which of the $n!$ permutations among n players are the players using.

Notation: For any Strategy class $\mathbb{S}$, let $\mathbb{S}(n)$ denote all the distributions produced by n players using strategies of type S. If it is not obvious, $\mathbb{S}$ is the set of all distributions using strategies of type S for all possible number of players.

Definition 4.3.11 (Distributions from Non-Local Games)**.** *For a specific choice of (1) players' resources, (2) question distribution Ξ for the verifiers, (3) winning function $W(.)$, and (4) the Huddle Phase's pre-agreed strategy between the players: we get a different $\Omega_S(Y_1, ..., Y_n \mid X_1 = x_1, ..., X_n = x_n)$ in the class $\mathbb{S}$.*

Claim 4.3.0.1 (Huddle Phase $\not\Rightarrow$ Players can produce any signalling correlation)**.** *The existence of a Huddle phase in definition 4.1.1 does not allow the provers to achieving any U-V signalling correlation. This is because the no-signalling strategy definition does not depend on inputs from previous rounds, but rather the ones in the current round. The huddle phase is signalling but at the wrong time, hence, it cannot help the provers in achieving any U-V signalling correlation.*

Conjecture 4.3.0.1 (LOC + Total-PR-boxes $\subsetneq$ QPE + Total-PR-boxes)**.** *LOC-Players where all pairs of players are equipped with PR-boxes produce a strict subset of the distributions of players using quantum prior-entanglement strategies together with having pairwise PR-boxes in multi-player non-local games.*

Theorem 4.3.1 ($\mathbb{NOSIG}(\mathrm{k}) \subsetneq \mathbb{QPE}(\mathrm{k+1})$)**.** *Players using quantum prior entanglement typically produce correlations that are a subset of those using no-signalling strategies. However, if we restrict the no-signalling provers to share arbitrary many k-input-output NOSIG boxes (blackbox model for NOSIG strategies among k players), while restricting the quantum provers to share states that are $k+1$-wise entangled, then these quantum provers can produce correlations strictly not possible by the provers using k-input-output NOSIG boxes in specific multi-player non-local games [CR17].*

4.4 Proof of Crépeau's Theorem

We now write two lemmas that will be used in proving Crépeau's conjecture (now theorem), and prove them. Following that, we state the theorem and prove it.

Lemma 4.4.1. *Let $\mathcal{C}$ be a one-way communication channel from Alice to Bob both using QPE strategies. Then Bob cannot signal Alice.*

Proof. By our construction of one-way communication channels, there is a no-signalling channel from receiver (Bob) to sender (Alice). This no-signalling channel has zero channel

capacity. All what is left to do is show that Bob cannot use shared Bell states (QPE strategies) with Alice to send classical information back to Alice. Recalling our discussion in section 2.6 in the information theory background, we know that without quantum channels shared between Alice and Bob and vice versa, there is no known way to amplify this zero capacity no-signalling channel from Bob to Alice. Since strategies of type QPE between Alice and Bob are not quantum communication channels between them, then we conclude that Bob cannot signal to Alice because they cannot amplify the channel from him to her. □

Lemma 4.4.2. *Let n be the number of provers in a non-local game. Then $\forall S \subseteq [n]$, where S signals $\overline{S}$[12], $\exists \left(|\overline{S}|! \cdot |S|!\right) \Pi_j$ signalling strategies that cannot implement[13] signalling from S to $\overline{S}$, where $1 \leq j \leq n!$.*

Proof. We begin with splitting the n-players into two sets S and its complement $\overline{S}$ ($S \cap \overline{S} = \emptyset$) and arranging the players in each set in cliques[14] K_S and $K_{\overline{S}}$. Furthermore, we allow a single player, say $s \in S$, to be connected by a one-way signalling channel with a player, say $\overline{s} \in \overline{S}$, from s to $\overline{s}$ (denoted by $s \to \overline{s}$).

Motivation: The reason we start the proof from the configuration where we allow the players in each set to be able to signal to any other player in their set (the clique configuration) is because it is the most powerful strategy the players in the set can have (recall figure 3.5). Hence, if we show that even using this powerful strategy the players cannot signal from $\overline{S} \to S$, then neither can a weaker Π-signalling strategy, chosen from a subset of the channels in the starting clique configuration, signal from $\overline{S} \to S$.

This implies that any player $i \in S$ can signal any player $j \in \overline{S}$ through the path:

$$i \xrightarrow{\text{through clique}} s \to \overline{s} \xrightarrow{\text{through clique}} j$$

Proof Sketch: the proof of lemma 2 will continue as follows:

1. Given that players in K_S can signal players in $K_{\overline{S}}$ with S connected to $\overline{S}$ through $s \to \overline{s}$, but not the other way around:
   (a) These $|S|+|\overline{S}|$ players can implement strategies Π_l-SIG constrained to s signalling $\overline{s}$. (e.g. see Figure 4.1)
   (b) These players can never implement any correlation where the collection of players $U \subseteq \overline{S}$ can signal the collection $V \subseteq S$.

[12] aka. with a S-$\overline{S}$ Signalling strategy.

[13] When we say "cannot implement" we mean: in a Multi-Player Non-Local Game, where provers are adopting a Π_j-SIG strategy, they cannot produce all the distributions that can result from when provers in $s \subseteq S$ are able to signal players in $\overline{s} \subseteq \overline{S}$ without losing the game w.h.p.

[14] For a set S, A clique K_S implies that $\forall i, j \in S$, i and j are connected by a bi-directional signalling channel. Here in the context of multi-player non-local games, we say that the players $s \in S$ are using a Clique-SIG strategy.

2. We conclude the proof with the argument that from (a) and (b), we deduce that the aforementioned Π_l-SIG can never implement any correlation where $\overline{S}$ can signal S. (e.g. see Figure 4.2)

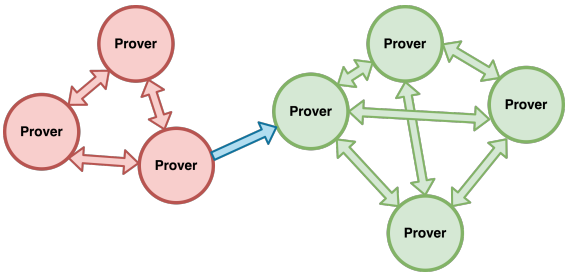
We can now assume w.l.o.g. that we fix s and $\overline{s}$ as above, and that for any permutation[15], $\Pi_{S\setminus\{s\}}$, of the remaining $|S|-1$ players in the set S and any permutation, $\Pi_{\overline{S}\setminus\{\overline{s}\}}$, of the remaining $|\overline{S}|-1$ players in $\overline{S}$, we can construct a specific n-player permutation

$$\Pi_l := \Pi_{S+\overline{S}} = \Pi_{S\setminus\{s\}} \to s \to \overline{s} \to \Pi_{\overline{S}\setminus\{\overline{s}\}}$$

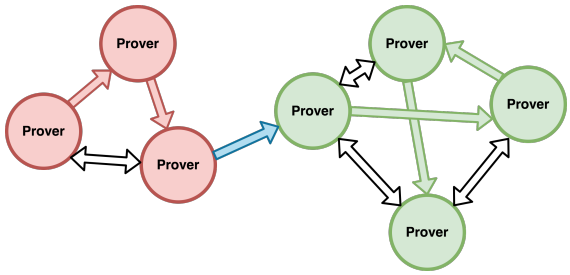
for some $1 \leq l \leq n!$.

Explaining the above Notation:

- For a set of players $S \subseteq [n]$, we write Π_S to denote the pi-signalling strategy between the players in set S. It will be understood from the context which fixed pi-signalling strategy among the players in S we are talking about.
- $\Pi_{S+\overline{S}}$ above means the aggregate pi-signalling strategy of all n-players that is constructed by concatenating the pi-signalling strategy $\Pi_{S\setminus\{s\}}$ with the one-way communication channel $s \to \overline{s}$ then appending at the end the pi-signalling strategy of the $|\overline{S}|-1$ players in set $\overline{S}$.
- This aggregate pi-signalling strategy is one of the $n!$ pi-signalling strategies that the n players could implement. We just name it Π_l.



(a) A split of 7 players in Clique K_S colored in red, and $K_{\overline{S}}$ colored in green.



(b) One of the possible permutation Π_l of the 7 players, white arrows are idle channels in this strategy.

Figure 4.1: An example visualizing the proof sketch of Lemma 4.4.2.

This clearly can be implemented by n-players using a Π_l-SIG strategy. In fact there are $|S|$ ways to choose s and then we get $(|S|-1)!$ possible valid permutations, and similarly $|\overline{S}|$ ways to pick $\overline{s}$ then we have $\big(|\overline{S}|-1\big)!$ possible permutations, which in total yields $|S| * (|S|-1)! * |\overline{S}| * \big(|\overline{S}|-1\big)! = |S|! * |\overline{S}|!$ as required in the lemma. This concludes step (1) in our proof sketch above.

[15]We mean the players are constraint to communicate in the specific order of whichever permutation chosen.

To prove step (2) in the proof sketch, we recall that we have K_S and $K_{\overline{S}}$ where $s \in S$ is connected with $\overline{s} \in K_{\overline{S}}$ by a one-way signalling channel $(s \rightarrow \overline{s})$. Since this channel is the only communication channel between players in S to those in $\overline{S}$, and from lemma (1) we established that the capacity of the channel in the opposite direction (see Figure 4.2) from $s \leftarrow \overline{s}$ is zero which cannot be amplified[16] because of the $\{\overline{s}\}$-$\{s\}$ no-signalling channel[17]. Hence, no player in $\overline{S}$ can signal any of the players in S.

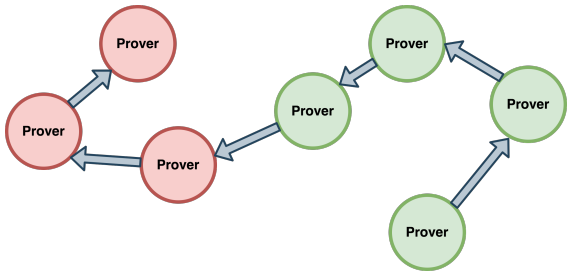


Figure 4.2: An example of an (*opposing*) Π-strategy to the one in Figure 4.1 that cannot signal from S to $\overline{S}$.

It directly follows then that Π_l-SIG strategy above cannot implement any distribution that signals from $\overline{S}$ to S, since the more general Clique case was not able to—namely the clique K_S which was signalling the clique $K_{\overline{S}}$. □

Theorem 4.4.3 ($\mathbb{NOSIG}(\mathrm{n}) = \bigcap_i \Pi_i\text{-}\mathbb{SIG}(\mathrm{n})$)**.** *Crépeau conjectured that:* $\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n)$ *is a NOSIG correlation iff* $\forall$ n*-prover permutations* j*, where* $1 \leq j \leq n!$*, the* Π_j*-SIG strategy can produce* $\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n)$ *in a relativistic* n*-prover non-local game without losing.*

Proof.

($\Rightarrow$) We start by proving the forward direction, where we assume that $\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n)$ is a NOSIG correlation that is well-known to the n-players before the beginning of the non-local game.[18] We want to show that any Π_j-SIG strategy for the n players can implement $\Omega(. \mid .)$. We start by providing the players with the needed resources (one-way signalling channels[19]) needed for a Π_j-SIG strategy and the agreed upon strategy will be that prover $\Pi_j[u]$ will send their input and output, as well as that of players $Pi_j[v]$ for $v < u$, to $\Pi_j[u+1]$, for $1 \leq u < n$ as depicted in Figure 4.3.

The proof sketch: Now each prover i, given the inputs passed to them and their local description of $\Omega(. \mid .)$, will produce the appropriate output, $y_i \in \mathcal{A}_i$, so that the n provers' collective output distribution given their inputs indeed implements $\Omega(. \mid .)$.

[16] see Information Theory background, the capacity definition 2.5.5 and the paragraph following it.

[17] The NOSIG channel is a resultant of the NOSIG strategy, which is enforced by the verifiers by restricting the response time of the provers.

[18] Here we mean each prover $i \in [n]$ has a local description of $\Omega(. \mid .)$ to use (aka. imagining the correlation, $\Omega(. \mid .)$, as a blackbox, each prover i has their own box, and all the box's inputs and outputs are with i).

[19] The verifiers relax the time restrictions on the provers' response times. (recall plot (c) in Figure 2.22).

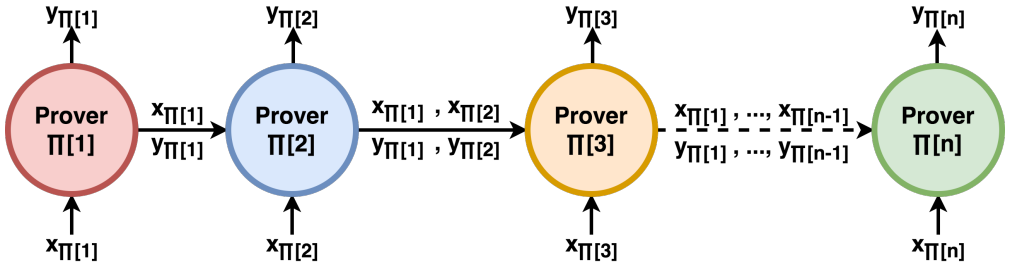


Figure 4.3: A diagram showcasing for some permutation Π, the Π-SIG strategy employed to produce the no-signalling correlation $\Omega(. \mid .)$.

Formally, for the first prover, $\Pi_j[1]$, in the permutation, they will take the marginal of $\Omega(. \mid .)$ and then produce the output from $\Omega_{Y_{\Pi_j[1]}}(. \mid .)$ given the input provided by their verifier.

Notation: we write $\sum_{Y_{\Pi_j[2]}}$ to denote $\sum_{y_{\Pi_j[2]} \in Y_{\Pi_j[2]}}$

$$\begin{aligned}
&\boldsymbol{Pr(Y_{\Pi_j[1]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]})} \\
&\quad = \sum_{Y_{\Pi_j[2]},\ldots,Y_{\Pi_j[n]}} \Omega(Y_{\Pi_j[1]}, \ldots, Y_{\Pi_j[n]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, \ldots, X_{\Pi_j[n]}) \\
&\quad := \Omega_{Y_{\Pi_j[1]}}(Y_{\Pi_j[1]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]})
\end{aligned}$$

Prover $\Pi_j[1]$ then sends their input $x_{\Pi_j[1]}$ and output $y_{\Pi_j[1]}$ to prover $\Pi_j[2]$ which proceeds to compute the marginal $\Omega_{Y_{\Pi_j[1]},Y_{\Pi_j[2]}}(. \mid .)$ and samples from this marginal till they get $Y_{\Pi_j[1]}$ equalling the output of prover $\Pi_j[1]$, $y_{\Pi_j[1]}$, once they get such a sample, they output the $Y_{\Pi_j[2]}$ corresponding to it to their verifier.
To get the distribution that prover $\Pi_j[2]$ will sample from, they do the following simple manipulation of their local description of $\Omega(.)$:

$$\begin{aligned}
&\boldsymbol{Pr(Y_{\Pi_j[2]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]}, Y_{\Pi_j[1]} = y_{\Pi_j[1]})} \\
&\quad = \frac{\sum_{Y_{\Pi_j[3]},\ldots,Y_{\Pi_j[n]}} \Omega(Y_{\Pi_j[1]}, \ldots, Y_{\Pi_j[n]} \mid X_{\Pi_j[1]}, \ldots, X_{\Pi_j[n]})}{\Omega_{Y_{\Pi_j[1]}}(Y_{\Pi_j[1]} = y_{\Pi_j[1]} \mid X_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]})} \\
&\quad = \frac{\Omega_{Y_{\Pi_j[1]}=y_{\Pi_j[1]},Y_{\Pi_j[2]}}(Y_{\Pi_j[1]}, Y_{\Pi_j[2]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]})}{\Omega_{Y_{\Pi_j[1]}}(Y_{\Pi_j[1]} = y_{\Pi_j[1]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]})}
\end{aligned}$$

Prover $\Pi_j[2]$ has all the ingredients needed to sample from the distribution on the right hand side (RHS) of the above equation:

$$\frac{\Omega_{Y_{\Pi_j[1]}=y_{\Pi_j[1]},Y_{\Pi_j[2]}}(Y_{\Pi_j[1]}, Y_{\Pi_j[2]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]})}{\Omega_{Y_{\Pi_j[1]}}(Y_{\Pi_j[1]} = y_{\Pi_j[1]} \mid X_{\Pi_j[1]} = x_{\Pi_j[1]}, X_{\Pi_j[2]} = x_{\Pi_j[2]})}$$

Namely, they have the local description of $\Omega(.)$, and they have $y_{\Pi_j[1]}, x_{\Pi_j[1]}, x_{\Pi_j[2]}$. Afterwards, prover $\Pi_j[2]$ then passes inputs $x_{\Pi_j[1]}$, $x_{\Pi_j[2]}$ and outputs $y_{\Pi_j[1]}$ and $y_{\Pi_j[2]}$ to prover $\Pi_j[3]$, which gets the marginal, inserts the two previous inputs together with their input, then samples till they get a triple with $Y_{\Pi_j[1]} = y_{\Pi_j[1]}$ and $Y_{\Pi_j[2]} = y_{\Pi_j[2]}$, then outputs the corresponding $y_{\Pi_j[3]}$ and so on and so forth.
The combination of all the y_i's will be implementing the original $\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n)$ by virtue of the product rule in probability theory for multi-variate probabilities. To show this, recall that by the product rule we can rewrite the multivariate conditional probability $\Omega(. \mid .)$ as:

$$\begin{aligned}\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n) = \Omega(&Y_n \mid X_1, ..., X_n, Y_1, ..., Y_{n-1}) \\ &* \Omega(Y_{n-1} \mid X_1, ..., X_n, Y_1, ..., Y_{n-2}) \\ &* ... \\ &* \Omega(Y_2 \mid X_1, ..., X_n, Y_1) \\ &* \Omega(Y_1 \mid X_1, ..., X_n)\end{aligned}$$

And since $\Omega(. \mid .)$ is NOSIG, each output Y_i does not depend on the previous inputs $X_{j<i}$ by 4.3.7, hence we know that the above reduces to:

$$\begin{aligned}\Omega(Y_1, ..., Y_n \mid X_1, ..., X_n) = \Omega(&Y_n \mid X_1, ..., X_n, Y_1, ..., Y_{n-1}) \\ &* \Omega(Y_{n-1} \mid X_1, ..., X_{n-1}, Y_1, ..., Y_{n-2}) \\ &* ... \\ &* \Omega(Y_2 \mid X_1, X_2, Y_1) \\ &* \Omega(Y_1 \mid X_1)\end{aligned}$$

where the terms on the RHS of the above equation are precisely the local strategies mentioned above in bold, $\boldsymbol{Pr(.)}$, each prover made *after* receiving the previous provers' inputs, taking the marginals, and sampling through the particular Π_j-SIG we outlined above.

($\Leftarrow$) For the backward direction, we assume that all n-prover Π_j-SIG strategies can implement a certain correlation $\Omega_?(Y_1, ..., Y_n \mid X_1, ..., X_n)$ in an n-prover non-local game, our task is to show that this correlation, $\Omega_?(. \mid .)$, *has to be* a NOSIG correlation.
Proof by Contradiction. We know from lemma 4.4.2 that for each way we can split the n-provers into two non-empty groups, S and $\overline{S}$, such that provers in S can signal provers in $\overline{S}$, there will be at least one of the $n!$ permutations, call it Π_j, that cannot implement signaling from S to $\overline{S}$. Hence, for each partitioning of the provers into two sets there always exists *an opposing* Π_k that cannot signal in that direction (as in Figure 4.1 for example).
If we assume (*for the sake of contradiction*) that all the Π_k signaling permutations are able to implement / produce some SIG correlation, $\Omega_{\text{SIG}}(. \mid .)$, that signals from

one subset $P \subset [n]$ to another subset $Q \subset [n]$. Then by invoking lemma 4.4.2, we know that there exists at least one permutation Π_* that cannot signal from P to Q, so provers using this Π_* strategy would never be able to implement such a signaling $\Omega_{\text{SIG}}(. \mid .)$ without losing the non-local game. Which contradicts our initial assumption and hence shows that $\Omega_?(. \mid .)$ has to be a NOSIG correlation.

□

Corollary 4.4.3.1 ($\mathbb{NOSIG} = \bigcup_{n\in\mathbb{N}^+} \bigcap_{i=1}^{n!} \Pi_i\text{-}\mathbb{SIG}(\text{n})$)**.** *The strategy class* $\mathbb{NOSIG}$ *is the union over the intersection of all the pi-signalling strategies among any number of provers in relativistic multi-player non-local games.*

Proof. This follows directly from Crṕeau's theorem together with the definition that

$$\mathbb{NOSIG} = \bigcup_{n\in\mathbb{N}^+} \mathbb{NOSIG}(n) = \bigcup_{n\in\mathbb{N}^+} \left[\bigcap_{i=1}^{n!} \Pi_i\text{-}\mathbb{SIG}(n) \right]$$

□

Chapter 5

Non-Local Zero-Knowledge

In this chapter, we will extend the definitions of zero-knowledge proof systems in the cryptography background section 2.9 to relativistic multi-player non-local games. We will show that for some provers' strategies, we will need to provide the simulators with more than just oracle access to the verifiers and rewinding to allow them to fool the verifiers. Simulators will be able to use non-local strategies to get an advantage over the provers. Noticing that the non-communicating provers were considered to be computationally unbounded, made us not care about the time complexity of non-local strategies. However, because the simulator(s) are considered to be efficient, this will lead us to define what it means for the various non-local strategies to be polynomial time in the size of the input.

5.1 Multi-Player Zero-Knowledge

We first extend the notation of output() and view() random variables:

- Let $\mathcal{P}_1, ..., \mathcal{P}_n$ and $\mathcal{V}_1, ..., \mathcal{V}_n$ be the machines of n provers and n verifiers, and R be the number of rounds of interaction, we know that $\mathcal{P}(x) \overset{k}{\longleftrightarrow} \mathcal{V}(x)$ denoted R-rounds of interaction between the $\mathcal{P}$ and $\mathcal{V}$ (see notation introduced in 2.2). We define $\left\langle \mathcal{P}_i(x) \overset{k}{\longleftrightarrow} \mathcal{V}_i(x) \right\rangle_i$ to be the pair wise interaction of each prover $\mathcal{P}_i(x)$ with verifier $\mathcal{V}_i(x)$ for R rounds with a possible Huddle phase between rounds.
- We define $\text{output}_{\langle \mathcal{V}_1,...,\mathcal{V}_n \rangle}\left(\left\langle \mathcal{P}_i(x) \overset{R}{\longleftrightarrow} \mathcal{V}_i(x) \right\rangle_{i\in[n]} \right)$ to be a random variable over the joint outputs of each of the n verifiers $\mathcal{V}_i$ when $\mathcal{V}_i$ interacts with $\mathcal{P}_i$ on input x for R successive rounds with a possible Huddle phase between rounds. An output 1 means they accept. In the context of relativistic non-local games, this output is produced after round R when the verifiers intervene to compute $W(.)$.

- We define $\text{view}_{\langle \mathcal{V}_1,...,\mathcal{V}_n \rangle}\left(\left\langle \mathcal{P}_i(x) \overset{R}{\longleftrightarrow} \mathcal{V}_i(x) \right\rangle_{i\in[n]} \right)$ to be a random variable over the prover's and verifier's non-local strategies, denoting the verifier's view throughout the protocol on input x, namely the messages exchanged between each pair of prover-verifier and the private strategy that the verifiers used.
- Let $(\mathcal{M}_1, ..., \mathcal{M}_n)_{\mathcal{T}}$ denote that the n players, with TMs $\mathcal{M}_1, ..., \mathcal{M}_n$, are using a strategy of type $\mathcal{T}$ (see definition 3.1.2).

Definition 5.1.1 (($\mathcal{A}$,$\mathcal{B}$,$\mathcal{C}$)-Relativistic n-Player Zero-Knowledge Proof System)**.** *A language L has a relativistic multi-player zero-knowledge proof system if there exists n provers $(\mathcal{P}_1, .., \mathcal{P}_n)_{\mathcal{A}}$ using a strategy of type $\mathcal{A}$, and n polynomial time verifiers $(\mathcal{V}_1, .., \mathcal{V}_n)_{\mathcal{B}}$ using a strategy of type $\mathcal{B}$, such that*

- *(Completeness) If $x \in L \implies$*

$$Pr\left[output_{\langle \mathcal{V}_1,...,\mathcal{V}_n \rangle}\left(\left\langle \mathcal{P}_i(x) \overset{R}{\longleftrightarrow} \mathcal{V}_i(x) \right\rangle_{i\in[n]} \right) = 1 \right] \geq 2/3$$

- *(Soundness) If $x \notin L \implies \forall\ \mathcal{P}_1^*, ..., \mathcal{P}_n^*$ using same $\mathcal{A}$-strategy,*

$$Pr\left[output_{\langle \mathcal{V}_1,...,\mathcal{V}_n \rangle}\left(\left\langle \mathcal{P}_i^*(x) \overset{R}{\longleftrightarrow} \mathcal{V}_i(x) \right\rangle_{i\in[n]} \right) = 1 \right] \leq 1/3$$

- *(Zero-Knowledge) $\exists n$ polynomial time simulators $(\mathcal{S}_1, .., \mathcal{S}_n)_{\mathcal{C}}$ using a strategy of type $\mathcal{C}$ such that $\forall\ x \in L, \forall$ possible i^{th} verifiers $\mathcal{V}_i^* \in \mathbb{V}_i, \forall\ aux_i \in \mathbb{B}$, and aux_i runs in polynomial time[1], we have:*

$$view_{\langle \mathcal{V}_1^*,...,\mathcal{V}_n^* \rangle}\left(\left\langle \mathcal{P}_i(x) \overset{R}{\longleftrightarrow} \mathcal{V}_i^*(x, aux_i) \right\rangle_{i\in[n]} \right) = \left\langle S_i^{\mathcal{V}_i^*}(x, aux_i) \right\rangle_{i\in[n]}$$

Remarks:

1. $\left\langle S_i^{\mathcal{V}_i} \right\rangle_{i\in[n]}$ denotes the joint random variable over the outcome of all $S_i^{\mathcal{V}_i}$'s where $S_i^{\mathcal{V}_i}$ is as defined in 2.9.6, namely, it is a random variable over the outcome of i^{th} simulator with oracle access to $\mathcal{V}_i^*$ and is distributed over possible concrete $\mathcal{C}$ strategies.
2. The probability in the completeness and soundness is over the possible concrete $\mathcal{A}$ strategies and concrete $\mathcal{B}$ strategies.
3. The equality between the verifiers' view and the simulator's output could be any of the ones in definition 2.9.2.
4. "aux $\in \mathbb{B}$" means the auxiliary input is some concrete strategy of type $\mathcal{B}$. This allows for it to be a random tape as before if $\mathcal{B}$=LOC, or it could be a quantum state if $\mathcal{B}$=QPE, notice in this case that the measurement operators can be ignored if one of them is projections onto the state of interest[2]. It also allows NOSIG resources without

[1] As will be shown in 5.2 below.

[2] Say the concrete QPE strategy is {state: $|\psi\rangle$, measurements: $\{|\psi\rangle\langle\psi|, |\psi'\rangle\langle\psi'|\}$}, then the strategy reduces to the physical resource $|\psi\rangle$.

worrying about quantifying what that means here. Of course, aux has to not jeopardize the polynomial time of the verifier / simulator. We will make that more formal in the next section.

5. $\mathcal{C}$ has to be at least as strong as $\mathcal{B}$.
6. Definition 2.9.6, corresponds to $n = 1$ and $\mathcal{A} = \mathcal{B} = \mathcal{C} = \text{LOC}$, aka shared randomness, but since each of these strategy is for a single player, it reduces to a random tape, and the probabilities are then over the coin tosses (aka. the random tape).
7. The zero knowledge multi-prover interactive proof system introduced in [GMR89], then corresponds to $\mathcal{A} = \text{LOC}$ and $\mathcal{B} = \mathcal{C} = \text{SIG}$, which basically reduces the verifiers to a single verifier and the simulators to a single simulator while allowing for multiple provers.
8. There are subtleties that need to be mentioned.
   (a) What does it mean for a simulator to rewind a verifier using a QPE strategy? What about a NOSIG strategy? For QPE strategies this was studied in [Van97; Wat02; Kob03; DFS04; Wat09]. We are not aware of anyone studying rewinding for NOSIG verifiers. Furthermore, the auxiliary input could also be a quantum state, which again complicates things.
   (b) We require that verifiers and simulators are polynomial time in input size $|x|$. However, with the introduction of strategies, what does it mean for a QPE simulator to be polynomial time? what about a NOSIG simulator?

5.2 Time Complexity of Non-Local Strategies

We intend to address point 8.(b) above in the remainder of this chapter. Mainly, recalling Figure 2.21, our task is to formalize the notion of time complexity of each micro-action type, in particular what it means for a micro-action to be polynomial time.

We start by making the observation that the time complexity for a player performing any of the micro-action types that are *not* signalling, is independent of the other players sharing the resources with. This independence lets us focus on the amount of computation each player does separately. To see this we go through the various strategies introduced in chapter 3. In LOC strategies each player has their own randomness and does not wait on the others. In QPE strategies applying a measurement on your part of the system is equivalent to taking the partial trace on the parts of the system not held by the player, in other words, the player acts on their part of the Hilbert space and as if the other Hilbert spaces are acted upon by an identity operator. For any COMOP strategy, the operators of the players are commuting with each other, so the order of the players operating on the shared state does not affect the outcomes. NOSIG strategies / boxes produce the player's output(s) directly after they provide their inputs, with the guarantee that when all the players provide their inputs the outputs are correlated in the way we defined in chapter 4. However, SIG strategies have the dependency of waiting on the other player to provide their input.

We will follow the same notion of complexity theory, and define efficiency computation (for a given strategy) to be one whose runtime on any input, x, is bounded by a polynomial function in $|x|$[3]. We use here asymptotic complexity. However, is $|x|$ the only relevant input here? An extra parameter is the interaction message sizes, $|m_i|$, and the number of players, n, sharing resources. For example, imagine a relativistic non-local game where the questions asked to the provers are graphs of size $|x|$, but the number of players is $2^{|x|}$. Because this is a relativistic non-local game, their will be $2^{|x|}$ verifiers each talking to their own prover, however the complexity of the prover's strategy could involve sharing exponential resources[4]. This leads us to include three parameters as inputs to a strategy: (1) The input statement x, (2) The message sizes $|m_i|$ exchanged between provers and verifiers, and (3) the number of players sharing this strategy k. And a polynomial time simulator or verifier, needs to be polynomial in all these parameters to be considered efficient, unless we restrict $k, m_i \in O(\mathsf{poly}(|x|))$ in which case we only care about the input size $|x|$. Either way, for the remainder of this chapter, we will call the total input to the strategy x and its length $|x|$.

Definition 5.2.1 (LOC Polynomial Time Complexity)**.** *For input x, the player's TM is allowed to read $O(\mathsf{poly}(|x|))$ bits from their shared random tape.*

We can restrict efficient QPE strategies to those strategies that can be modelled by polynomial time uniform families of quantum circuits $\{Q_{|x|}\}$ using a universal set of gates each acting on a constant (independent on $|x|$) number of qubits. We assume that the time complexity of such a gate is $O(1)$. In BQP we restrict these circuits to have a single output, but we could think of a polynomial number of these circuits for any specific input size that can output strings of polynomial length number of qubits. Notice that since we only care about the asymptotic time complexity, we can restrict each time slice to include a single gate operating on a constant number of qubits.

Notation: Let g be some quantum gate acting on a constant number of qubits, c, then we say $\text{fan-in}(g) = c$.

Definition 5.2.2 (QPE Polynomial Time Complexity)**.** *Let $\mathcal{US}$ be a finite universal set of quantum gates with constant fan-in. For input x, the player is allowed to only have $m \in O(|x|^a)$ qubits for some constant $a \geq 0$, split between qubits shared with other players and ancilla qubits used as a work-register. Then for each time-slice, the player can apply one of*

$$|\mathcal{US}| \times \binom{m}{\textit{fan-in}(g)} \times (\textit{fan-in}(g))!$$

[3]Here x stands for the language that the provers and the verifiers receive that the provers want to prove is in some language L.

[4]The reader might ask well how will the efficient verifiers be able to verify these exponential number of messages from each other after huddling? There are many ways to go around this, one way is to consider Oracularization techniques for answer reduction mentioned in the motivation appendix so that only one verifier can compute the winning function.

$O(1)$-operations, where $g \in \mathcal{US}$.[5] *The player is allowed to apply $O(|x|^a)$ such operations to be considered efficient or polynomial time.*

This definition strongly relates to the statement we made in chapter 2.7. Namely, that there exists a finite universal quantum gate set that can implement any unitary transformation. This is not entirely true. The caveat is that quantum gates in the universal sets suffice to generate a dense subset of the special unitary group of degree 2, and that they can approximate any unitary U up to some ϵ-error with $O(\log^c(1/\epsilon))$ gates from any of the finite universal quantum gate sets, that is our circuit with $O(\log^c(1/\epsilon))$ gates has the effect of unitary S s.t. $||S-U|| \leq \epsilon$ where the operator norm is defined as $||M|| = \max_\psi ||M|\psi\rangle||$. This is known as the Solovay-Kitaev Theorem.

Furthermore, to understand how QPE strategies (as defined in 4.3.3) relate to definition 5.2.2 above, notice that the unitaries, $U_x^{(d,u)}$ in 4.3.3, have to be restricted to gates in $\mathcal{US}$, and the set $\mathcal{D}$ must have size that is polynomial in $|x|$ with each dimension $d \in \mathcal{D}$ also being polynomially sized (which directly implies the number of qubits is also $\mathsf{poly}(|x|)$).

Next, we define polynomial time NOSIG strategies in a similar way to the quantum case above. The main difference is that we do not know of a universal set of NOSIG boxes that can approximate all NOSIG correlations. Hence we will restrict ourselves to a finite set of NOSIG boxes each with constant fan-in and fan-out[6] independent on the input size. We assume the time complexity of operating such a box to be $O(1)$. Notice that because these are non-local boxes/gates, the fan-in is the number of inputs that are in the possession of the player, and the other players would have the other inputs/outputs local to them. Recall that NOSIG boxes produced output directly after the player provides their input, while maintaining the NOSIG correlation between all the outputs independent of the order of player's providing their inputs. (*Similar definitions can be made for SIG/Π-SIG strategies.*)

Definition 5.2.3 (NOSIG Polynomial Time Complexity)**.** *Let $\mathcal{NS}$ be a finite set of NOSIG boxes with universal constant fan-in and fan-out independent of the input size and number of players in the proof system. For input x, the player is allowed to have $m \in O(|x|^a)$ such boxes for some constant $a \geq 0$, shared with the other players. Then an efficient NOSIG strategy is one modelled by polynomial time uniform families of NOSIG circuits $\{NS_{|x|}\}$ using gates from $\mathcal{NS}$.*

Zero-knowledge is defined, as we have seen in the background section, by a simulator. In the literature, the simulator had the same computational power as the verifier, but was given the advantage to rewind computation with the verifier or knowledge of a trapdoor in a commitment scheme. When extending to relativistic non-local zero-knowledge proof systems, a verifier was associated with each prover, and hence the simulator could also be

[5] Here we pick g uniformly, then select the fan-in(g) qubits that g will be applied to, then consider all permutations of mapping the inputs of g to these qubits.

[6] Same as fan-in but for outputs of a NOSIG box, we did not consider this in QPE because quantum gates are reversible so fan-in=fan-out.

split into multiple simulators. As we saw in this chapter, a single simulator (which is what is found in the literature of Zero-Knowledge MIP) corresponds to n-simulators sharing a SIG strategy. We also saw from chapter 3 (specially Figure 3.5) and from Crépeau's theorem, that SIG strategies are strictly stronger than NOSIG strategies. The natural question we asked is do the simulators need a SIG strategy to prove soundness? What is the minimum ("least powerful") strategy that the simulators can use to fool the verifiers? Using the time complexity definitions we just defined allows us to rigorously speak about polynomial time (efficient) simulators and verifiers in zero-knowledge proofs that use non-local strategies. This is a critical starting point to finding the most stringent polynomial time strategy for simulators to achieve soundness. Why is a more stringent strategy better? One great example by Crépeau is to imagine **a judge** comparing the probability ensemble of the verifier(s)' view and the simulators' output. If the simulators are space-like separated from one-another, and they are using a SIG strategy, then in a practical relativistic implementation of the proof, the time-stamps of their messages to one another to generate the final transcript of the proof will not be instantaneous, but will convey information about the time it took light to travel between them. Thus this judge could be able to distinguish between the simulators versus the verifiers and provers, hence could incorrectly lead us to conclude that the proof is not zero-knowledge. However, if the same simulators could have generated this final transcript using a QPE strategy, then no such knowledge will exist, and the judge would not be able to distinguish the two ensembles and the zero-knowledge property will be preserved.

5.3 Putting It All Together

In [Cré+19], the authors aspired to physically build and test a scalable zero-knowledge multi-prover interactive proof system and they succeeded. They used the idea of relativistic constraints to ensure provers are non-communicating, but had to come up with two new zero-knowledge proof systems for the NP-complete 3-colorability language that required much less interaction between the verifiers and provers. This was critical to making the experiment feasible, by only needing to separate the verifier by 100± meters which sufficed for all the back-and-forth needed between the verifiers and the provers, irrespective of the input graph size! In our notation, one of the proof systems was a **(LOC,SIG,SIG)-relativistic 2-player zero-knowledge proof system** and the other was a **(QPE,SIG,SIG)-relativistic 3-player ZKP system**. They relied on a bit-commitment scheme that obeys the new *unveil-via-commit principle*, which is introduced and explained in their paper. The future work they proposed included finding:

1. a proof that [Cle+04] is sound against QPE-provers.
2. a (QPE,SIG,SIG)-relativistic 2-player zero-knowledge proof system.
3. a (NOSIG,SIG,SIG)-relativistic 3-player zero-knowledge proof system.
4. a (NOSIG,SIG,SIG)-relativistic 2-player zero-knowledge proof system.

Our work here creates a formal framework for pursuing some of these questions. In a future

paper we are working on, we show that a box introduced by authors of [Cré+19] that implements their bit-commitment scheme, which they named the CMS^{2}Y box. This box has the same number of inputs independent of the graph input size. This was inspired from our definition of polynomial time NOSIG strategies, namely that the set $\mathcal{NS}$ had to have boxes of constant fan-in. However, we needed to show that the CMS^{2}Y box was indeed a NOSIG box, and using definitions 4.3.4, 4.3.5, and 4.3.6 to prove this fact was challenging. However, using Crépeau's theorem that we proved in chapter 4, we were able to prove that the CMS^{2}Y box was indeed NOSIG. This enables us to consider efficient simulators using this box as a NOSIG advantage instead of a SIG advantage, and we are able to show that (3) and (4) above are not sound against NOSIG provers. More generally, we show that if simulators are using the same strategy type as the provers, then the proof cannot be sound.

Chapter 6

Conclusion and Future Work

Non-local Games can be used to implement a rich variety of protocols that could be useful in our everyday lives. They also give both computer scientists and physicists a new venue to understand the limits of both nature and information processing. Zero-knowledge multi-player non-local games is a relatively new area of research, and fully understanding the interplay between the provers' versus simulators' strategies is an exciting direction. We have detailed the Protocol Model in Chapter 4 that enables us to better understand non-local strategies from this new framework, and used this framework to prove Crépeau's theorem. This theorem is a proxy that can be used to prove that a non-local box indeed produces NOSIG correlations instead of relying on the more cumbersome definition 4.3.6 which was used to prove the theorem in the first place. We also used our understanding of non-local strategies in games to generalize the notion of zero-knowledge proof systems. Our new general definition of zero-knowledge showed that throughout the previous literature of zero-knowledge MIP, authors were implicitly assuming the simulators were using a SIG strategy, and our work allows us to consider giving simulators weaker advantages to be able to prove soundness of some of the zero-knowledge proofs.

Below are some of the questions that we would have loved to tackle, many of which could be good starters for research projects.

- We have seen that the verifiers needed to restrict the provers in certain ways depending on the provers' strategies. Can we devise cryptographic/internet protocols that forces players to be Π-signalling for example? or to forbid them from communicating all together without relying on space-like separation?
- What happens when we replace classical channels in Π_i-SIG with quantum channels? What about combining quantum and classical channels? What about quantum channel in one direction and a classical direction in the opposite direction? As mentioned in chapter 4, we would have enjoyed delving deeper into heterogeneous strategies amongst the n-players and understand the complexity classes arising from this mixing.
- Another question of personal interest is whether no-signalling correlations have a different entropy describing them than Von Neumann and Shannon's entropies? There

is work (see [Bru+14] section V) showing that PR-boxes and general no-signalling correlations have almost all the strange properties of quantum mechanics, like
  - A No-Cloning Theorem
  - The Monogamy of Correlations
  - A Disturbance vs. Information Gain trade-off in Measurements
  - An Inherent Randomness of Measurement Outcomes
  - The Complementarity of Measurements and Uncertainty Relations (An Uncertainty Principle)

  The question we ask is, what extra properties do these no-signalling correlations have that make them stronger than those of quantum mechanics? This could help us understand what sort of physical theory could realize these currently hypothetical (yet permissible) correlations.
- It is extremely interesting, and seemingly difficult, to find no-signalling boxes with more than 2-input-outputs. We saw that the PR-box is $\mathbb{NO}$-$\mathbb{SIG}$-Complete for 2 players, however, is there a 3-input-output box or generic n-input-output box that cannot be implemented by PR-boxes? We partially answer this question in a future paper, with Claude Crépeau and Nan Yang, showing a 3-input-output NOSIG box.
- Is there physical elements that could reside with Alice and Bob to achieve the PR-box correlations just like qubits in the case of QPE? or is it more like a magnetic dipole, that can only exist with the two poles intertwined in the box, without ever finding a magnetic monopole?
- Is there a systematic way to figure out how much entanglement is needed to win a non-local game optimally?
- Given the recent result that having only $\log n$ provers in a MIP protocol makes $\mathsf{MIP} = \mathsf{IP} = \mathsf{PSPACE}$, an interesting question, is understanding the spectrum of complexity classes as the number of provers increases between $\log n \ \to n$ provers.
- What clever new cryptosystems could be construct based on non-local games?
- Design introspection games for arbitrary distributions.
- It is interesting to consider heterogeneous resources among the players, and use reduction to map these configurations to the classes above (e.g. Imagine 4 players, 2 with quantum entanglement, and 2 with classical computers). A natural question is whether this is considered a new class altogether or if it reduces to one of the strategy classes in chapter 4.
- Investigate rewinding in zero-knowledge for verifiers using NOSIG strategies that could be given NOSIG auxiliary inputs.

References

[Alm+10] Mafalda L Almeida et al. "Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage". In: *Physical review letters* 104.23 (2010), p. 230404.

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[AS98] Sanjeev Arora and Shmuel Safra. "Probabilistic checking of proofs: A new characterization of NP". In: *Journal of the ACM (JACM)* 45.1 (1998), pp. 70–122.

[Aro+98] Sanjeev Arora et al. "Proof verification and the hardness of approximation problems". In: *Journal of the ACM (JACM)* 45.3 (1998), pp. 501–555.

[Bab85] László Babai. "Trading group theory for randomness". In: *Proceedings of the seventeenth annual ACM symposium on Theory of computing*. 1985, pp. 421–429.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. "Non-deterministic exponential time has two-prover interactive protocols". In: *Computational complexity* 1.1 (1991), pp. 3–40.

[BM88] László Babai and Shlomo Moran. "Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes". In: *Journal of Computer and System Sciences* 36.2 (1988), pp. 254–276.

[Bar+95] Adriano Barenco et al. "Elementary gates for quantum computation". In: *Physical review A* 52.5 (1995), p. 3457.

[Bar+05] Jonathan Barrett et al. "Nonlocal correlations as an information-theoretic resource". In: *Physical Review A* 71.2 (2005), p. 022101.

[Bel64] John S Bell. "On the einstein podolsky rosen paradox". In: *Physics Physique Fizika* 1.3 (1964), p. 195.

[Ben+88] Michael Ben-Or et al. "Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Chicago, Illinois, USA: Association for Computing Machinery, 1988, pp. 113–131. ISBN: 0897912640. DOI: 10.1145/62212.62223. URL: https://doi.org/10.1145/62212.62223.

[Ben+93] Charles H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 Mar.

1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

[BBM92] Charles H Bennett, Gilles Brassard, and N David Mermin. "Quantum cryptography without Bell's theorem". In: *Physical review letters* 68.5 (1992), p. 557.

[Ber09] Daniel J Bernstein. "Introduction to post-quantum cryptography". In: *Post-quantum cryptography*. Springer, 2009, pp. 1–14.

[BV97] Ethan Bernstein and Umesh Vazirani. "Quantum complexity theory". In: *SIAM Journal on computing* 26.5 (1997), pp. 1411–1473.

[BLR90] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. "Self-testing/correcting with applications to numerical problems". In: *Proceedings of the twenty-second annual ACM symposium on Theory of computing*. 1990, pp. 73–83.

[Boy+00] P Oscar Boykin et al. "A new universal and fault-tolerant quantum basis". In: *Information Processing Letters* 75.3 (2000), pp. 101–107.

[Bra+06] Gilles Brassard et al. "Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial". In: *Physical Review Letters* 96.25 (June 2006). ISSN: 1079-7114. DOI: 10.1103/physrevlett.96.250401. URL: http://dx.doi.org/10.1103/PhysRevLett.96.250401.

[Bru+14] Nicolas Brunner et al. "Bell nonlocality". In: *Reviews of Modern Physics* 86.2 (Apr. 2014), pp. 419–478. ISSN: 1539-0756. DOI: 10.1103/revmodphys.86.419. URL: http://dx.doi.org/10.1103/RevModPhys.86.419.

[Buh+10] Harry Buhrman et al. "Nonlocality and communication complexity". In: *Reviews of modern physics* 82.1 (2010), p. 665.

[CR17] Rui Chao and Ben W Reichardt. "Test to separate quantum theory from non-signaling theories". In: *arXiv preprint arXiv:1706.02008* (2017).

[Cir80] B. S. Cirel'Son. "Quantum generalizations of Bell's inequality". In: *Letters in Mathematical Physics* 4.2 (Mar. 1980), pp. 93–100. DOI: 10.1007/BF00417500.

[Cla+69] John F Clauser et al. "Proposed experiment to test local hidden-variable theories". In: *Physical review letters* 23.15 (1969), p. 880.

[CB97] Richard Cleve and Harry Buhrman. "Substituting quantum entanglement for communication". In: *Phys. Rev. A* 56 (2 Aug. 1997), pp. 1201–1204. DOI: 10.1103/PhysRevA.56.1201. URL: https://link.aps.org/doi/10.1103/PhysRevA.56.1201.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. "Perfect commuting-operator strategies for linear system games". In: *Journal of Mathematical Physics* 58.1 (Jan. 2017), p. 012202. ISSN: 1089-7658. DOI: 10.1063/1.4973422. URL: http://dx.doi.org/10.1063/1.4973422.

[Cle+04] Richard Cleve et al. "Consequences and limits of nonlocal strategies". In: *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* IEEE. 2004, pp. 236–249.

[CC19] Xavier Coiteux-Roy and Claude Crépeau. *The RGB No-Signalling Game*. 2019. arXiv: 1901.05062 [quant-ph].

[CS17] Andrea Coladangelo and Jalex Stark. *Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets*. 2017. arXiv: 1708.06522 [quant-ph].

[CY18] Claude Crépeau and Nan Yang. *Non-Locality in Interactive Proofs*. 2018. arXiv: 1801.04598 [quant-ph].

[Cré+] Claude Crépeau et al. "Classical and quantum strategies for two prover bit commitments". In: ().

[Cré+19] Claude Crépeau et al. *Practical Relativistic Zero-Knowledge for NP*. 2019. arXiv: 1912.08939 [quant-ph].

[DFS04] Ivan Damgård, Serge Fehr, and Louis Salvail. "Zero-knowledge proofs and string commitments withstanding quantum attacks". In: *Annual International Cryptology Conference*. Springer. 2004, pp. 254–272.

[Deu85] David Deutsch. "Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117.

[Din07] Irit Dinur. "The PCP theorem by gap amplification". In: *Journal of the ACM (JACM)* 54.3 (2007), 12–es.

[Ein19] Albert Einstein. *Relativity: The Special and the General Theory-100th Anniversary Edition*. Princeton University Press, 2019.

[Eke91] Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical review letters* 67.6 (1991), p. 661.

[FF15] Serge Fehr and Max Fillinger. "Multi-prover commitments against non-signaling attacks". In: *Annual Cryptology Conference*. Springer. 2015, pp. 403–421.

[FF16] Serge Fehr and Max Fillinger. "On the composition of two-prover commitments, and applications to multi-round relativistic commitments". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2016, pp. 477–496.

[GK90] Oded Goldreich and Hugo Krawczyk. "On the Composition of Zero-Knowledge Proof Systems". In: *SIAM Journal on Computing* 25 (1990), pp. 169–192.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The knowledge complexity of interactive proof systems". In: *SIAM Journal on computing* 18.1 (1989), pp. 186–208.

[GS86] Shafi Goldwasser and Michael Sipser. "Private coins versus public coins in interactive proof systems". In: *Proceedings of the eighteenth annual ACM symposium on Theory of computing*. 1986, pp. 59–68.

[HK19] Dhiraj Holden and Yael Kalai. *Non-Signaling Proofs with $O(\sqrt{\log n})$ Provers are in PSPACE*. 2019. arXiv: 1910.02590 [cs.CC].

[Ito09] Tsuyoshi Ito. *Polynomial-Space Approximation of No-Signaling Provers*. 2009. arXiv: 0908.2363 [cs.CC].

[Jai+09] Rahul Jain et al. *QIP = PSPACE*. 2009. arXiv: 0907.4737 [quant-ph].

[Ji+20] Zhengfeng Ji et al. "Mip*= re". In: *arXiv preprint arXiv:2001.04383* (2020).

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D Rothblum. "How to delegate computations: the power of no-signaling proofs". In: *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*. 2014, pp. 485–494.

[Ken99] Adrian Kent. "Unconditionally secure bit commitment". In: *Physical Review Letters* 83.7 (1999), p. 1447.

[Kil90] J Kilian. "Strong separation models of multi prover interactive proofs". In: *DIMACS Workshop on Cryptography*. 1990.

[Kit97] A Yu Kitaev. "Quantum computations: algorithms and error correction". In: *Russian Mathematical Surveys* 52.6 (1997), p. 1191.

[Kob03] Hirotada Kobayashi. "Non-interactive quantum perfect and statistical zero-knowledge". In: *International Symposium on Algorithms and Computation*. Springer. 2003, pp. 178–188.

[Lun+15] Tommaso Lunghi et al. "Practical relativistic bit commitment". In: *Physical Review Letters* 115.3 (2015), p. 030502.

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. "Robust self-testing of the singlet". In: *Journal of Physics A: Mathematical and Theoretical* 45.45 (2012), p. 455304.

[NV18] Anand Natarajan and Thomas Vidick. "Low-Degree Testing for Quantum States, and a Quantum Entangled Games PCP for QMA". In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (Oct. 2018). DOI: 10.1109/focs.2018.00075. URL: http://dx.doi.org/10.1109/FOCS.2018.00075.

[NV16] Anand Natarajan and Thomas Vidick. "Robust self-testing of many-qubit states". In: *arXiv preprint arXiv:1610.03574* (2016).

[NW19] Anand Natarajan and John Wright. "NEEXP is Contained in MIP". In: *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2019, pp. 510–518.

[NC02] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002.

[36] "On computable numbers, with an application to the Entscheidungsproblem". In: *J. of Math* 58.345-363 (1936), p. 5.

[PV10] Károly F Pál and Tamás Vértesi. "Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems". In: *Physical Review A* 82.2 (2010), p. 022116.

[PR94] Sandu Popescu and Daniel Rohrlich. "Quantum nonlocality as an axiom". In: *Foundations of Physics* 24.3 (1994), pp. 379–385.

[SW08] Volkher B Scholz and Reinhard F Werner. "Tsirelson's problem". In: *arXiv preprint arXiv:0812.4305* (2008).

[Sha92] Adi Shamir. "IP = PSPACE". In: *J. ACM* 39.4 (Oct. 1992), pp. 869–877. ISSN: 0004-5411. DOI: 10.1145/146585.146609. URL: https://doi.org/10.1145/146585.146609.

[Sha01] Claude Elwood Shannon. "A mathematical theory of communication". In: *ACM SIGMOBILE mobile computing and communications review* 5.1 (2001), pp. 3–55.

[Sho97] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

[Sip96] Michael Sipser. "Introduction to the Theory of Computation". In: *ACM Sigact News* 27.1 (1996), pp. 27–29.

[Slo17] William Slofstra. *The set of quantum correlations is not closed*. 2017. arXiv: 1703.08618 [quant-ph].

[SW85] Stephen J Summers and Reinhard Werner. "The vacuum violates Bell's inequalities". In: *Physics Letters A* 110.5 (1985), pp. 257–259.

[Van97] Jeroen Van De Graaf. *Towards a formal definition of security for quantum protocols*. Citeseer, 1997.

[Ver+16] Ephanielle Verbanis et al. "24-hour relativistic bit commitment". In: *Physical review letters* 117.14 (2016), p. 140506.

[Wat02] John Watrous. "Limits on the power of quantum statistical zero-knowledge". In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings*. IEEE. 2002, pp. 459–468.

[Wat09] John Watrous. "Zero-knowledge against quantum attacks". In: *SIAM Journal on Computing* 39.1 (2009), pp. 25–58.

[Wit20] Edward Witten. "A mini-introduction to information theory". In: *La Rivista del Nuovo Cimento* 43.4 (Mar. 2020), pp. 187–227. ISSN: 1826-9850. DOI: 10.1007/s40766-020-00004-5. URL: http://dx.doi.org/10.1007/s40766-020-00004-5.

[Wu+16] Xingyao Wu et al. "Device-independent parallel self-testing of two singlets". In: *Physical Review A* 93.6 (2016), p. 062121.

[YM08] Noson S Yanofsky and Mirco A Mannucci. *Quantum computing for computer scientists*. Cambridge University Press, 2008.

Appendices

Appendix A

Applications of Non-Local Games

This appendix chapter seeks to answer the question of why non-local games are important and what could be some of the practical application of correlations arising from these various strategies.

We will cover a wide range of applications superficially, albeit enough to give the reader a decent idea of the terrain. We will start by explaining what is self-testing and give a few concrete examples, then we will show how these games can be used in cryptography and information theory.

A.1 Self-Testing

Definition A.1.1 (Self-Test)**.** *Let $\epsilon > 0$ be our error tolerance. Then a non-local game $\mathcal{G}$ is said to be a self-test for a concrete strategy $S_{\mathcal{T}}$ of type $\mathcal{T}$ iff $\mathcal{G}$ has:*

- *(Completeness) Provers achieve $val^*_{NA}(\mathcal{G}) \geq c$ only if they use $S_{\mathcal{T}}$, for some completeness parameter c dependent on the self test $\mathcal{G}$.*
- *(Soundness) If provers achieve $val^*_{NA}(\mathcal{G}) \geq s$ for some concrete strategy $S'_{\mathcal{T}}$, for some soundness parameter s dependent on the self test $\mathcal{G}$, then*

$$S'_{\mathcal{T}} \approx_\epsilon S_{\mathcal{T}}$$

- *(Robustness) The gap is bounded by the error tolerance, roughly for some function f,*

$$c - s \leq f(\epsilon)$$

For a non-local game to be considered a self-test, we require that the optimal value of the game be unique (up to local isometries[1]) and robust (a nearly optimal strategy yields nearly optimal game value.)

[1]Meaning changes of basis of measurement at any of the provers, which cannot be ruled out.

For example if we consider a quantum strategy, and we denote by $\mathrm{S}_{\mathcal{T}} := \mathrm{OPT}$—our optimal strategy then the definition above translates to

$$\mathrm{val}_{\mathrm{S}'_{\mathcal{T}}}(\mathcal{G}) = \mathrm{val}^*_{\mathrm{OPT}}(\mathcal{G}) - \epsilon \implies |\Psi\rangle_{\mathrm{S}'_{\mathcal{T}}} \approx_{\sqrt{\epsilon}} |\Psi\rangle_{\mathrm{OPT}} \otimes |\mathrm{JUNK}\rangle$$

and furthermore, we require that

$$\implies ((O_{\mathrm{S}'_{\mathcal{T}}})^a_x \otimes I)\,|\Psi\rangle_{\mathrm{S}'_{\mathcal{T}}} \approx_{\sqrt{\epsilon}} ((O_{\mathrm{OPT}})^a_x \otimes I)\,|\Psi\rangle_{\mathrm{OPT}} \otimes |\mathrm{JUNK}\rangle$$

where $\approx_\epsilon$ is that the two-hand sides are ϵ-close relative to some appropriate distance metric.

Note: Perfect completeness of QPE strategies in the magic square game makes analysis of self-tests a lot easier than the CHSH game for example.

Remark: The definitions for the self tests below are not formal, but rather explain the game and its questions, the details of Ξ, the input and output sets, and the winning function $W(.)$ can be easily extracted from the explanations.

A.1.1 Testing Linearity of Boolean Functions

Let us start with a simple test covering a classical result related to Boolean functions.

Definition A.1.2 (Linear Function)**.** *A function $f : \{0,1\}^n \to \{1,-1\}$ is a linear function if $\forall x, y \in \{0,1\}^n$, we have*

$$f(x \oplus y) = f(x) \oplus f(y)$$

Theorem A.1.1 ([BLR90])**.** *If $Pr_{a,b}[f(x) \oplus f(y) = f(x \oplus y)] \geq 1 - \epsilon$ for some $\epsilon > 0$, then f is $O(\epsilon)$-close to some linear function g.*

Definition A.1.3 (Linearity Self Test)**.** *Let Alice and Bob share a function $f : \{0,1\}^n \to \{1,-1\}$ that they claim to be linear. The verifier uniformly samples $a, b, c \in \{0,1\}^n$, and randomly picks one of the provers to be Alice and the other to be Bob. They ask Alice $\langle a, b\rangle$, while asking Bob $\langle q, c\rangle$ where $q \in_{uniform} \{a \oplus b, a, b\}$. Because the questions are symmetric, the provers cannot know whether they are Alice or Bob. For any input $\langle x, y\rangle$, the provers need to return $\langle f(x), f(y)\rangle$. The verifier ignores Bob's $f(c)$, and checks the linearity condition if $q = a \oplus b$*

$$f(a \oplus b) = f(a) \oplus f(b)$$

and checks consistency between the provers answer if $q = a$, by checking

$$f_{Bob}(q) = f_{Alice}(a)$$

and similarly if $q = b$.

The above test can be repeated for multiple rounds to increase certainty. Obviously the more linear f is, the more probably Alice and Bob pass the test, this coincide with the robustness requirement in the self-test definition above. Next let us look at an example that we already mostly covered and one that will use this Linearity self test.

A.1.2 Testing EPR Pairs

Testing a single EPR pair was first introduced in [SW85]. In the CHSH game, definition 3.2.1, we saw that the maximum winning probability for QPE strategy was 85.4%, and from the proof of Tsirelon's bound 2.7.10, we saw that for players to achieve this game value, each player's two measurement bases needed to anti-commute, using this fact, we will now show that their concrete strategy has to involve sharing an EPR pair. In order to show this, let us first restrict the provers to each having a single qubit, we will consider the case where they have multiple qubits afterwards and reduce it to the single qubit case. Restricting to a qubit, Alice's measurements, A_0 and A_1, have to be acting on 2-dimensional Hilbert spaces, which is characterized uniquely[2] by the Pauli group[3]. The anti-commutation requirement by Tsirelon, implies that $A_0 = Z$ and $A_1 = X$, and similarly for Bob's $B_0 = Z, B_1 = X$. Now if we write down the Bell operator in this case we get:

$$S = Z \otimes Z + Z \otimes X + X \otimes Z - X \otimes X$$

Now by knowing that the maximum winning probability $\langle \Psi | S | \Psi \rangle$ is achieved if $|\Psi\rangle$ is the eigenvector corresponding to largest eigenvalue. Using a straightforward calculation, one gets that the state they share, $|\Psi\rangle$, has to be an EPR pair. Therefore, if verifier plays the CHSH game and sees the provers achieving maximum winning probability for QPE, then their shared state had to be an EPR pair[4]. [MYS12] computed that the robustness of this test was $O(\epsilon^2)$.

[Wu+16] used a similar technique to test 2 EPR pairs. Recall that the Magic Square game was perfectly won using a QPE strategy that involved sharing 2 EPR pairs between Alice and Bob. The operators in the matrix $\mathcal{M}$ that achieved the perfect game value obeyed certain relations as we saw in chapter 3, however, one byproduct of these rules was that any two operators not in the same row or column *had* to anti-commute[5]. Anti-commutation relations turn out to be also one of the properties of the Pauli group on 2 qubits, so winning the Magic Square Game with probability $1 - \epsilon$ means the provers had to have a state that is at least ϵ-close to sharing two EPR-states. The details are a little more involved than we let out here and can be found in paper.

Definition A.1.4 (Anti-Commutation Self Test)**.** *(Informal) Optimally winning the CHSH game certifies to the verifier that the two provers had to use anti-commuting operators on their shared quantum state. The Magic Square game was similar, in that the answer bits returned from cells that are not in the same row or column had to be produced by non-commuting operators. Furthermore, the variant of the Magic Square game where Alice gets asked a row or column and Bob gets asked a cell, also could be used by the verifiers lying half the time and asking Bob a cell not on the row / column of Alice.*

[2] again under local isometries.

[3] Recall the Pauli group is generated by Pauli X and Z, satisfying $X^2 = Z^2 = I$ and $XZ = -ZX$.

[4] If they were not restricted to a single qubit per player, then because they are restricted to two observables, whichever their state was could be reduced to a single qubit using Jordan's lemma.

[5] One can easily check that this is indeed the case by just looking at the elements in final matrix $\mathcal{M}$.

The 2 EPR self test result was extended to detect n EPR pairs through a series of work where robustness depended on n as $\frac{1}{poly(n)}$ that culminated in [NV16]'s result, where robustness was constant. We will roughly go over this result showcasing a few other interesting self-tests.

The first step is realizing that instead of testing qubits, one could test observables instead. To do this you need to extend the Pauli group and its properties to the n-qubit case. Let $a, b \in \{0,1\}^n$, where a denotes the n-qubits with Alice and b denotes the n-qubits with Bob, and $X(a)$ means apply a Pauli-X to the i^{th} qubit if the i^{th} bit in a is 1 (and similarly for $X(b)$ or $Z(.)$). The properties of the Pauli group are neatly extended into:

- (Linearity) $O(a)O(b) = O(a \oplus b)$, for $O \in \{X, Z\}$
- (Anti-Commutation) $X(a)Z(b) = (-1)^{\langle a,b \rangle} Z(b)X(a)$

Definition A.1.5 (Quantum Braiding Test (n EPR pair Self-Test))**.** *We construct a non-local game with the following four equiprobable questions (each is a self-test on its own):*

- *(Quantum Linearity Test) Ask Alice measure in the $X(a)$-basis and Bob to measure in the $X(b)$-basis and validate the linearity condition of their result.*
- *(Quantum Linearity Test) Ask Alice measure in the $Z(a)$-basis and Bob to measure in the $Z(b)$-basis and validate the linearity condition of their result.*
- *(Anti-Commutation Test) Ask Alice to measure in the $X(a)$-basis and Bob in the $Z(b)$-basis or vice versa and validate the anti-commutation condition of their result.*
- *(Consistency Test) Ask both Alice and Bob the same query and check that they return the same answer.*

It is proven that this indeed self-tests n EPR pairs in [NV16]. The quantum linearity test is similar to the linearity test we discussed previously, but quantized using the Linearity condition of Pauli-n operators, in a way that the provers' operators applied on some state $|\psi\rangle$ is similar to some linear operators acting on this state with high probability. The anti-commutation test is a generalization of any of the anti-commutation test above to n questions instead of 1, the key idea is that any two anti-commuting operators Z, X are equivalent to a qubit, so if the bit strings a and b used at Alice $X(a)$ and Bob $Z(b)$, have only one bit in common equalling 1, then this too is as if it is a single qubit, and could be tested with a single anti-commutation test, but the clever part is how to interleave that question with the rest of the questions so that Alice and Bob do not know which self test they are going through so they do not know how to cheat. However, the main idea of why this works is roughly the same, from these question they show that the provers had to have operators X' and Z' that very closely satisfy the Pauli-n-group relations to achieve a game value of $1 - \epsilon$, and that means there is an isometry that maps those $X' \to X$ and $Z' \to Z$ and hence the state they must have shared is ϵ-close to n EPR pairs.

The high level takeaway here is that the verifiers can force the provers to be sharing a specific quantum state, and can also force them to apply specific measurements to these states. They force them by taking advantage that each prover doesn't know the question asked to the other, and so the verifiers interleave consistency tests with EPR tests with Anti-commutation tests so that the provers are forced to behave honestly or else they will lose.

A.1.3 Answer Reduction

Consider the case when the answers returned by the provers are exponential in size, while we restrict our verifiers to polynomial time. Here, the verifiers are no longer able to read the full answer, let alone apply a winning function on it. This issue could be overcome, using ideas from the PCP literature (extensions to definition 2.2.25 and the PCP theorem 2.2.3), where the verifier can only query a small number of bits of the answer, and achieve completeness and soundness requirements. However, a critical, yet solved, issue is that PCPs require the whole answer to be formatted in a way to allow quick verification, however, in multi-prover settings, the full answer is split among the provers that are not communicating, hence they cannot construct such a PCP. The standard technique for overcoming this is called **oracularization**.

Definition A.1.6 (Oracularization)**.** *Let $\mathcal{G}$ be a non-local game. We define $\mathcal{G}'$ as the oracularization of $\mathcal{G}$ by splitting the provers into an oracle prover, and all the other provers to be isolated provers. The oracle prover receives the questions asked to all provers if they were playing in $\mathcal{G}$. The isolated provers, receive a single question just like they would have in $\mathcal{G}$. The answer provided by the oracle prover could be used as the PCP, while the answer from all isolated provers could be used as a consistency test with the oracle prover's answers.*

How is oracularization incorporated in self-tests? The high level answer is that the oracularization questions and the self-test questions are combined into a question set, and sampled with some probability, in a way that the provers would not know if they one of the other provers is an oracle prover in this round (so they cannot cheat or else they would fail the consistency test), or are they actually in the self-test. Details could be found in the recent literature in [NW19; Ji+20].

A.1.4 Introspection Games

Consider the case when the questions asked by the verifiers are exponential in size, while we restrict our verifiers to polynomial time. Here, sampling the questions and sending them to the provers is no longer possible by the verifiers. Introspection games enables the verifiers to ask the (all powerful) provers to sample these exponentially sized questions from some distribution Ξ, and return to them the question and answer pair where we could apply the answer reduction technique above. This idea at first sight seems impossible. Why would the

provers not cheat and sample questions that are easy for them to answer? Assuming you force them to sample according to the verifiers' distribution Ξ, how do you ensure that they cannot see each other's questions which would defy the fact that they are non-communicating provers?

It turns out that both hurdles can be overcome again with introspection self-test games introduced in [NW19] and refined in the authors later work in [Ji+20]. However, the provers introspect questions from very specific distributions, like the Point-Plane distribution [BFL91]. These we convenient in the proof of [Ji+20], because the quantum braiding test required many queries to test for the various linearity, anti-commutation, and consistency tests to truly capture if the provers were lying, the authors were able to smear out the error using an error correcting code called the low degree code, which could be tested by a low-degree self-test which was initially introduced by [BFL91; AS98], then extended to a quantum low-degree test by [NV18; NW19].

Definition A.1.7 (Point-Plane Distribution)**.** *Let q be a valid finite size, and $m \in \mathbb{N}$ be the dimension of our plane. Moreover, $x \in (\mathbb{F}_q^m)^3$ is a uniform randomly sampled affine plane, p, in $\mathbb{F}_q^m$ defined by $\{v_0 + \alpha_1 v_1 + \alpha_2 v_2 \ : \ \forall\ \alpha_1, \alpha_2 \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^m$, hence for plane type questions the prover gets three vectors $v_0, v_1, v_2 \in (\mathbb{F}_q^m)^3$ where v_0 is the intercept while v_1, v_2 are called the directions. $y \in \mathbb{F}_q^m$ is a uniformly random sampled point from the plane x.*

Definition A.1.8 (Classical Low-Degree Self-Test)**.** *Imagine the provers share k polynomials, $f_i : \mathbb{F}_q^m \to \mathbb{F}_q$ where $i \in [k]$, each of total degree-d. These are the low-degree polynomials. The sampled questions could be two points, two planes for consistency questions, or a plane for one prover and a point to the other prover for the low degree test.*

- *(Consistency Test) Give both provers the same plane or the same point and check that their answers match.*
- *(Low-Degree Test) Label the provers Alice and Bob randomly. Give Alice a plane $p \in (\mathbb{F}_q^m)^3$, and Bob a point $x \in \mathbb{F}_q^m$. Bob should return the evaluation of $f_i(x)$ for all $i \in [k]$ that is Bob's answer $b \in \mathbb{F}_q^k$. Alice should return a single polynomial, $g : \mathbb{F}_q^m \to \mathbb{F}_q^k$, of total degree d that maps points on the plane $p \in \mathbb{F}_q^m$ to the encoding by the low-degree polynomials. The verifier checks that $g(x) = b$.*

We will not cover low-degree error correcting codes which require a significant background beyond the scope of this document, however, it suffices to say that using some protocol, the provers return appropriate answers based on these questions they sampled from the Point-Plane distribution. We want to discuss on a high level how verifiers force provers to actually sample from this distribution without the provers knowing each others questions.

Solve the issue of them sampling from this distribution is not complicated, observe that if the provers share $3m \log q$ qubits as split them in three groups (or registers) as in Figure A.1, then if the verifiers force[6] Alice to apply a Pauli Z on all three registers, while orders Bob to apply a Pauli-Z on $|v_0\rangle$ and ignoring his $|v_1\rangle$ and $|v_2\rangle$ registers. This indeed gives

[6] via an EPR and Anti-commutation self-tests.

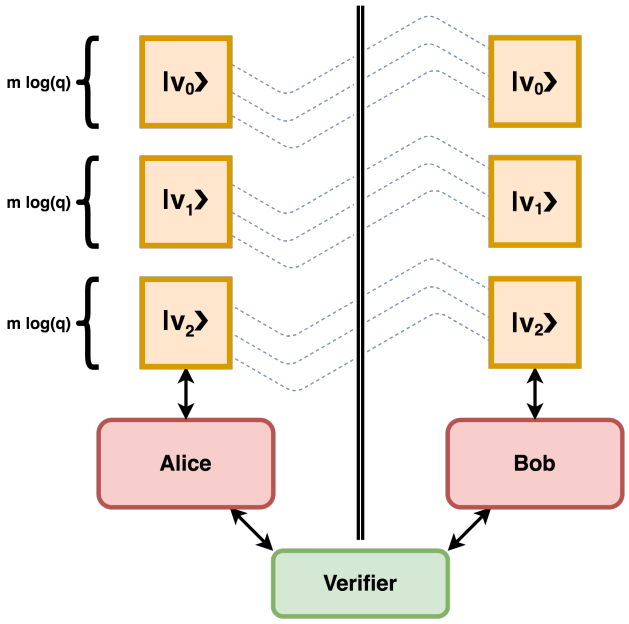


Figure A.1: Introspection by Provers to Sample Questions from a Point-Plane Distribution

Alice a random plane, and gives Bob a random point on the plane, however, Alice knows Bob's question since it is the intercept part of her plane, and Bob can measure the $|v_1\rangle$ and $|v_2\rangle$ registers in the Pauli-Z basis and figure out Alice's plane, hence reducing this to a single prover game. To fix this we define the famous Heisenberg Uncertainty Principle, that states that for observables, A, B, that do not commute, measuring one of the observables, say A, collapses the state to an eigenvector of A. If you now measure B on the new state it is guaranteed to distort it.

Definition A.1.9 (Heisenberg Uncertainty Principle)**.** *Let A, B be two Hermitian operators (aka. observables). Then the following inequality always holds:*

$$(\Delta A)^2(\Delta B)^2 \geq \left(\langle \Psi | \frac{1}{2i}[A, B] | \Psi \rangle \right)^2$$

where ΔA denotes the standard deviation or uncertainty in observing A[7]*.*

Using the uncertainty principle, we can now force Bob to measure $|v_1\rangle$ and $|v_2\rangle$ in the Pauli-X basis and that will completely erase the direction vectors from Bob's side because Alice was forced to measure these registers in the Pauli-Z basis and $[X, Z] \neq 0$. However, now we want Alice, to not know the intercept $|v_0\rangle$.

Using a similar idea, verifiers can force Alice to make partial measurements in the Pauli-X basis for $|v_0\rangle$ register, where a Pauli-X is applied for qubit i, for $1 \leq i \leq m \log(q)$, if the i^{th} bit read from registers $|v_1\rangle$ or $|v_2\rangle$ was 1, denote by this partial measurement $X(v_2)X(v_1)$.

[7] recall definition in information theory section, table 2.2.

$$|v_0\rangle \xrightarrow{X(v_i)} \frac{1}{\sqrt{q}} \sum_{\alpha \in \mathbb{F}_q} c(\alpha) \, |v_0 + \alpha \cdot v_i\rangle$$

for some constants, $c(\alpha)$, dependent on the shift α.

This partial measurement smears out the components of $|v_0\rangle$ matching a 1 in the measured v_1 and v_2, this way the new intercept $|v_0'\rangle = X(v_2)X(v_1)\,|v_0\rangle$ lies on the plane, but Alice now cannot know Bob's point.

Introspection is a form of the general idea of **delegating computations** to a server with a guarantee that the server actually performed the computational task, as opposed to cutting shortcuts and cheating with some answer. This is critical when asking a cloud provider to perform a computation intensive query on their cloud and return the answer to the typically computationally less powerful customer device while ensuring that you got your money's worth by them actually doing the computation as opposed to returning a random answer for example.

A.2 Other Applications

Non local games proved useful in Cryptography where it enabled applications like Quantum Key Distribution introduced in [Eke91; BBM92]. Moreover, bit commitment schemes were also shown to be implemented using non-local game as was first introduced in [Cré+] then followed by [FF15; FF16].

There are applications to non-local strategies in reducing communication complexity first realized in [CB97] and surveyed in [Buh+10].

We hope this appendix chapter gave the reader a flavor of why understanding non-local games and their dynamics under various player strategies could be used in practical applications that have the potential to influence many fields of computer science.

Appendix B

Quantum PR-Box Attempt

This appendix chapter is based on an attempt to create a new box that achieves correlations not possible by QPE-NOSIG strategies. To do this we wanted the box to have quantum inputs and outputs (to allow superpositions, interference, etc). The internal workings of the box could be signalling, as long as the outputs at Alice and Bob were no-signalling. That is okay since it is similar to the PR-box whose correlation $x \cdot y = a \oplus b$ could be implemented via signalling.

Our attempt implemented a PR-box with quantum inputs and outputs, however the achieved correlations from this box turnout to be statistically indistinguishable from the PR-box. It is still useful because we can now use PR-boxes with QPE-NOSIG strategies.

We begin by describing the classical control unit used in our classically controlled quantum circuit that implements our quantum PR-box (QPR box). The state machine below is responsible for making the box symmetric between the inputs. As long as the players did not attempt to latch their quantum input, the state machine remains in state A, once a player latches their input, they move to state B, the lower arrow is to break evens in case both Alice and Bob latch at the same time. Once in state B, the control signals S_1 and S_2 become zero indicating deactivation. The assumption here is that each player will use the box once, this is in their interest since the players are collaborating.

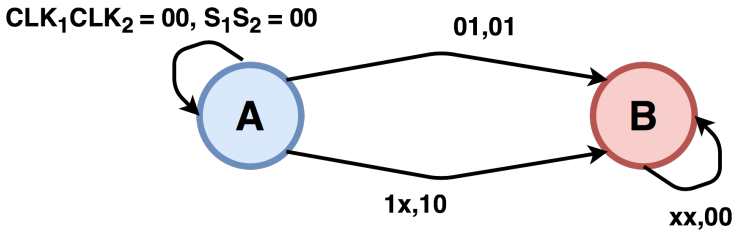


Figure B.1: Classical Control *Mealy* State Machine where the first 2 bits are for clock 1 (CLK_1) and clock 2 (CLK_2) respectively which act as input, and the last 2 bits are for the output signals S_1 and S_2. An $\times$ value means either 0 or 1.

Next using karnaugh map (K-Maps) and mapping state A to 0 and state B to 1 we get:

Table B.1: State-Transition Table For Classical Control of the QPR-Box

State S	Next State S'				Output S_1S_2			
	00	**01**	**11**	**10**	**00**	**01**	**11**	**10**
A	A	B	B	B	00	01	10	10
B	B	B	B	B	00	00	00	00

This gives the classical control digital circuit in Figure B.3. Before we show the full classically-controlled-quantum-circuit implementing the Quantum version of a PR-Box. We introduce a new quantum gate called the swap gate in Figure B.4. Moreover, recall that any quantum gate U can be made as a classically controlled gate controlled-U.

Below the RIP module is basically a Quantum memory that keeps the qubit as a closed system until the end of the interactive proof protocol. However, whether that module measures or not, should not change the output statistics.

To understand this circuit, it is best to assume player 1 enters their input first, then player 2, this way we can ignore the classical circuits and the swap gates as $S_1 = 1$ and $S_2 = 0$. The circuit reduces to Figure B.6. This is straightforward to analyze. Notice that the two internal qubit after we apply $H \otimes I$ then $CNOT$ becomes an EPR pair

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$$

We will now go through the four qubits from left to right, let $|x_1\rangle = a|0\rangle + b|1\rangle$ and $|x_2\rangle = c|0\rangle + d|1\rangle$

$$|x_1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |x_2\rangle \to |x_1\rangle \otimes H|0\rangle \otimes |0\rangle \otimes |x_2\rangle \to |x_1\rangle \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle \Big) \otimes |0\rangle \otimes |x_2\rangle$$

Now we apply the CNOT gate:

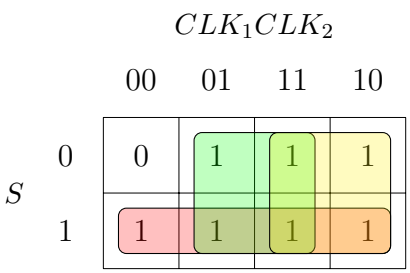
$$|x_1\rangle \otimes \text{CNOT}(\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle \Big) \otimes |0\rangle) \otimes |x_2\rangle \to |x_1\rangle \otimes \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \otimes |x_2\rangle$$

Next substituting for values of $|x_1\rangle$ and $|x_2\rangle$ our state becomes

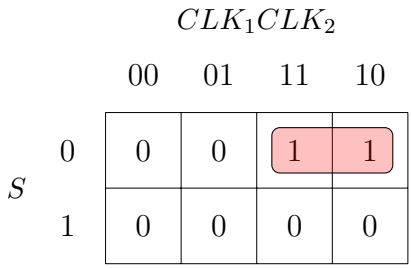
$$\begin{aligned}
&(a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \otimes (c|0\rangle + d|1\rangle) \\
&= \frac{1}{\sqrt{2}}(ac\big[\,|0000\rangle + |0110\rangle\,\big] + ad\big[\,|0001\rangle + |0111\rangle\,\big] \\
&+ bc\big[\,|1000\rangle + |1110\rangle\,\big] + bd\big[\,|1001\rangle + |1111\rangle\,\big])
\end{aligned}$$

We can now easily apply the Toffoli gate as in the circuit to give:

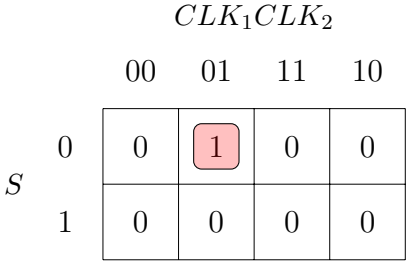
$$\begin{aligned}
&\frac{1}{\sqrt{2}}(ac\big[\,|0000\rangle + |0110\rangle\,\big] + ad\big[\,|0001\rangle + |0111\rangle\,\big] \\
&\quad + bc\big[\,|1000\rangle + |1110\rangle\,\big] + bd\big[\,|1011\rangle + |1101\rangle\,\big])
\end{aligned}$$



(a) For the D Flip Flop, we get $\boxed{D = CLK_1 + CLK_2 + S}$.



(b) For the output state S_1, we get $\boxed{S_1 = CLK_1 \wedge \overline{S}}$.



(c) For the second output state S_2, we get $\boxed{S_2 = \overline{CLK_1} \wedge CLK_2 \wedge \overline{S}}$.

Each term in the square brackets has the same input $|x_1x_2\rangle$. For terms with coefficient ac, ad, bc the AND of the inputs is 0, and thus the outputs y_1 needs to equal y_2 as seen they all have $|y_1y_2\rangle = |00\rangle + |11\rangle$, while for the last term with coefficient bd, the AND of the inputs is 1, and the outputs are indeed different $|y_1y_2\rangle = |01\rangle + |01\rangle$. □

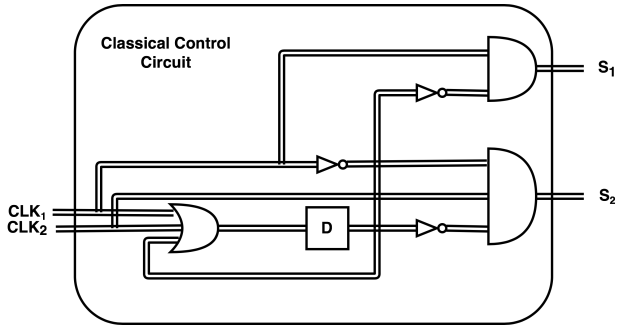


Figure B.3: Sequential Digital Circuit given a pair of clocks 1 and 2, yields the appropriate quantum control S_1 and S_2, this is the black box module used in Figure $B.5$

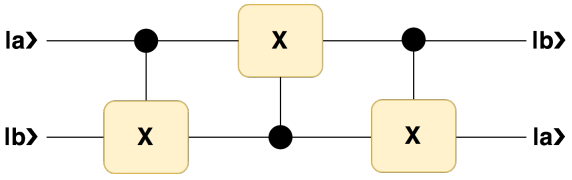


Figure B.4: Applying 3 CNOT gates in flipped order swaps the (unknown) input qubits.

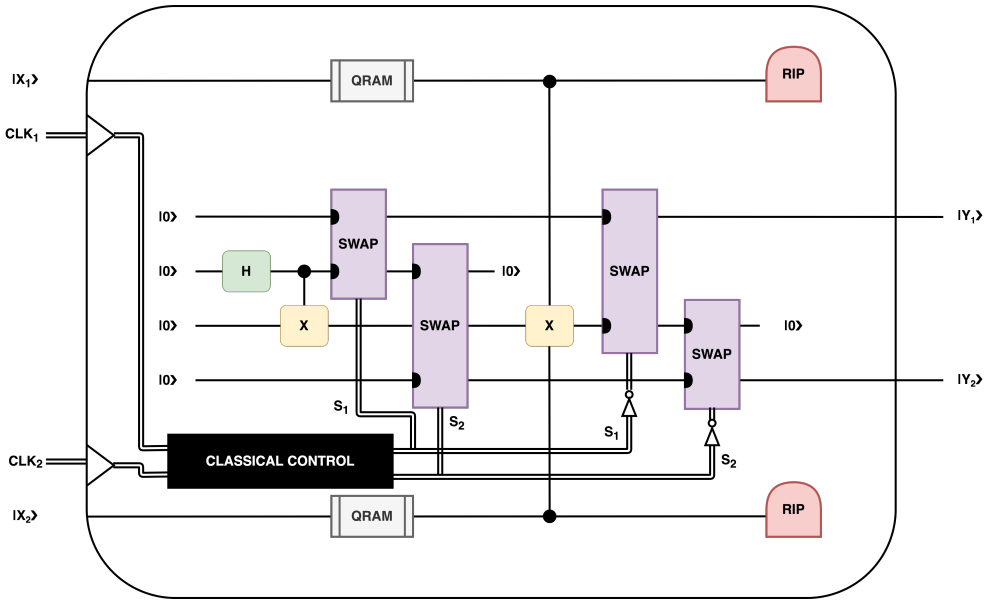


Figure B.5: QPR-Box Classically Controlled Quantum Circuit

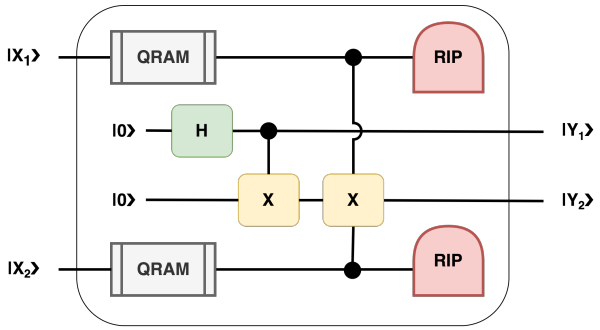


Figure B.6: Simplified QPR-box.

Appendix C

Quantum Gate Set Identities

Some of the useful identities:

$$X = HZH \implies Z = HXH \implies HX = ZH \implies HZ = XH \tag{C.1}$$

$$S = YSX \tag{C.2}$$

$$iX = SXS \implies iXSZ = SXSSZ = SXZZ = SX \tag{C.3}$$

$$\text{(the above conclusion does not imply } iXS = SX \text{ because } S^2 = Z) \tag{C.4}$$

Furthermore, if you compute the commutator of X and T, you get:

$$[X, T] = XT - TX = -iY \implies TX = XT - iY$$

and if you compute the commutator of X and S, you get:

$$[X, S] = XS - SX = \frac{1-i}{2}Y \implies SX = XS - \frac{1-i}{2}Y$$

Therefore, when applying H, S, or T gates to the state $XZ|\psi\rangle$ we get:

- $H[XZ|\psi\rangle] = ZH[Z|\psi\rangle] = ZX[H|\psi\rangle]$ (flips X and Z)
- $S[XZ|\psi\rangle] = iXSZ[Z|\psi\rangle] = iX[S|\psi\rangle]$
- $T[XZ|\psi\rangle] = (XT - iY)[Z|\psi\rangle] = XT[Z|\psi\rangle] - iY[Z|\psi\rangle] = XZ[T|\psi\rangle] - iYZ|\psi\rangle$
  This equation has an issue, because applying T to the output of the QPR-box, gives the required state $XZ[T|\psi\rangle]$, but adds to it the unwanted term $[-iYZ|\psi\rangle]$.

To attempt to solve this. We want to compute $T[XZ|\psi\rangle]$. Let us compute the matrix TXZ:

$$TXZ = iTY = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -e^{\frac{i\pi}{4}} & 0 \end{pmatrix} \tag{C.5}$$

We wish to decompose TXZ to some matrix V times T.

$$TXZ = VT = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -e^{\frac{i\pi}{4}} & 0 \end{pmatrix} \tag{C.6}$$

$$V = \begin{pmatrix} 0 & e^{\frac{-i\pi}{4}} \\ -e^{\frac{i\pi}{4}} & 0 \end{pmatrix} = -e^{\frac{-i\pi}{4}} \times \begin{pmatrix} 0 & -1 \\ e^{\frac{i\pi}{2}} & 0 \end{pmatrix} \tag{C.7}$$

$$= -e^{\frac{-i\pi}{4}} \times \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix} \tag{C.8}$$

The matrix V is equal to $Q = \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix}$ multiplied by some phase $-e^{\frac{-i\pi}{4}}$. $Q\left|\psi\right\rangle$ rotates the qubit $\left|\psi\right\rangle$ by π around the $X - Y$ axis. However, can Q be implemented without the T-gate?

To answer this, let us further decompose $Q = JS$, and solve for matrix J.

$$Q = JS = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{C.9}$$

$$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = iX \tag{C.10}$$

So $Q = iXS$. Hence $TXZ = VT = (-e^{\frac{-i\pi}{4}})QT = ((-e^{\frac{-i\pi}{4}}) \times i)XST$. Yielding:

$$TXZ = (e^{\frac{5i\pi}{4}})XST$$

We wish to include quantum-ly controlled $X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle$ where $\left|u\right\rangle$ and $\left|v\right\rangle$ are single qubits, and we can think of them in the computational basis $\{\left|0\right\rangle, \left|1\right\rangle\}$. So for unitary, U, and $\left|\phi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ we define:

$$U^{|\phi\rangle}\left|\psi\right\rangle = \alpha\left|0\right\rangle \otimes \left|\psi\right\rangle + \beta\left|1\right\rangle \otimes U\left|\psi\right\rangle$$

H and S are simple,

- $H[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = Z^{|u\rangle}H[Z^{|v\rangle}\left|\psi\right\rangle] = Z^{|u\rangle}X^{|v\rangle}[H\left|\psi\right\rangle]$ (flips X and Z)
- $S[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = i^{|u\rangle}X^{|u\rangle}SZ^{|u\rangle}[Z^{|v\rangle}\left|\psi\right\rangle] = i^{|u\rangle}X^{|u\rangle}Z^{|u\rangle}Z^{|v\rangle}[S\left|\psi\right\rangle]$

For T, we follow the same procedure as above and get:

$$T[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = (e^{\frac{-i\pi}{4}})S^{|u\rangle}X^{|u\rangle}T[Z^{|v\rangle}\left|\psi\right\rangle] = (e^{\frac{-i\pi}{4}})S^{|u\rangle}X^{|u\rangle}Z^{|v\rangle}[T\left|\psi\right\rangle] \tag{C.11}$$

To summarize:

- $\boxed{H[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = Z^{|u\rangle}X^{|v\rangle}[H\left|\psi\right\rangle]}$
- $\boxed{S[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = i^{|u\rangle}X^{|u\rangle}Z^{|u\rangle}Z^{|v\rangle}[S\left|\psi\right\rangle]}$
- $\boxed{T[X^{|u\rangle}Z^{|v\rangle}\left|\psi\right\rangle] = (e^{\frac{-i\pi}{4}})S^{|u\rangle}X^{|u\rangle}Z^{|v\rangle}[T\left|\psi\right\rangle]}$