Université de Montréal

Quantum Pseudo-Telepathy Games

par
Anne Lise Broadbent

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

avril, 2004

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

Quantum Pseudo-Telepathy Games

présenté par:

Anne Lise Broadbent

a été évalué par un jury composé des personnes suivantes:

Michel Boyer
président-rapporteur

Alain Tapp
directeur de recherche

Gilles Brassard
codirecteur

Stefan Wolf
membre du jury

Mémoire accepté le 20|08|04

RÉSUMÉ

Le traitement de l'information quantique est au confluent des sciences physique, mathématiques et informatique ; il vise à déterminier ce qu'on peut et ne peut pas faire avec l'information quantique. Le sujet de ce mémoire est la complexité de la communication, qui est un domaine de l'informatique qui vise la quantification de la communication nécessaire à la résolution de problèmes distribués.

La pseudo-télépathie est une application surprenante du traitement de l'information quantique à la complexité de la communication. Grâce à une ressource quantique appelée « intrication », deux joueurs ou plus peuvent accomplir une tâche *sans communiquer*, tandis que ceci serait impossible pour des joueurs classiques (qui n'ont pas accès à l'intrication). Un jeu de pseudo-télépathie à n joueurs se présente comme suit: chaque joueur reçoit en entrée une question. Sans communiquer, chacun émet en sortie une réponse. Le jeu est gagné si les réponses conjointes satisfont une certaine condition. Il s'agit d'un jeu de pseudo-télépathie si les joueurs quantiques peuvent gagner de façon systématique, tandis que ceci est impossible pour les joueurs classiques.

Dans ce mémoire, nous décrivons sept jeux de pseudo-télépathie, tirés de la littérature de la physique et de l'informatique quantique. Nous incluons aussi des résultats originaux de l'auteur. Les jeux sont présentés du point de vue informatique, et de façon uniforme, ce qui facilite leur comparaison. Certains points de comparaison sont: le nombre de joueurs, la taille de l'entrée, la taille de la sortie, la condition gagnante, l'état intriqué partagé et la probabilité maximale de réussite pour les joueurs classiques.

Mots clés : informatique quantique, complexité de la communication quantique, non-localité, intrication, théorème de Bell, échappatoire de la détection.

ABSTRACT

Quantum information processing is at the crossroads of physics, mathematics and computer science; it is concerned with what we can and cannot do with quantum information. This thesis deals with communication complexity, which is an area of computer science that aims at quantifying the amount of communication necessary to solve distributed problems.

Pseudo-telepathy is a surprising application of quantum information processing to communication complexity. Thanks to a quantum resource called "entanglement", two or more quantum players can accomplish a task with *no* communication, whereas this would be impossible for classical players (who do not have access to entanglement). A pseudo-telepathy game with n players is the following: each player receives as input a question. Without communicating, each player outputs an answer. The players win if their joint answers satisfy a certain condition. We say that the game exhibits pseudo-telepathy if quantum players can systematically succeed at this game, whereas this would be impossible for classical players.

In this thesis, we describe seven pseudo-telepathy games which appear in the physics and quantum information processing literature. We have also included original results of the author. The games are presented from a computer scientist's perspective, and in a uniform way, in order to facilitate comparison. Some points of comparison are: number of players, size of the inputs, size of outputs, winning condition, shared entangled state and maximum success probability for classical players.

Keywords: quantum information processing, quantum communication complexity, nonlocality, entanglement, Bell's theorem, detection loophole.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

BKS	Bell-Kochen-Specker
EPR	Einstein-Podolsky-Rosen
GHZ	Greenberger-Horne-Zeilinger
QIP	Quantum Information Processing

NOTATION

$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\imath$	imaginary number, $\imath = \sqrt{-1}$
$\lvert\alpha\rvert$	complex norm of α
$\mathcal{H}_d$	d-dimensional complex inner product space
$\lvert\psi\rangle$	quantum state
$\lVert\lvert\psi\rangle\rVert$	norm of $\lvert\psi\rangle$
$\Delta(x)$	Hamming weight of a binary string x
$\overline{x}$	bitwise complement of x
$\equiv$	modular equivalence, (mod 2) if not specified
$\lg(x)$	base-two logarithm, $\log_2(x)$
$\widetilde{\omega}_c(G_n)$	maximum success proportion, over all possible deterministic strategies for classical players that play the game G_n
$\omega_c(G_n)$	maximum success probability, over all possible strategies for classical players that play the game G_n
$\omega_q(G_n)$	maximum success probability, over all possible strategies for quantum players that play the game G_n
p	probability that a player's answer corresponds to the predictions of quantum mechanics in a game with errors
$p_*(G_n)$	maximum value of p for which a classical strategy can succeed as well as a quantum strategy
η	probability that a player outputs something other than $\perp$ in an error-free game
$\eta_*(G_n)$	maximum value of η for which a classical strategy can succeed as well as a quantum strategy

To my teachers, past and present.

ACKNOWLEDGEMENTS

I would like to thank my supervisors, Dr. Gilles Brassard and Dr. Alain Tapp for their help, encouragement and support. Thank-you also to my friends and family, in particular, my mother, father, sister, and Didier. Thanks to you, I found the motivation to bring this project to term. I also thank my grad school friends here at the Université de Montréal.

Many thanks to the Natural Sciences and Engineering Research Council of Canada, the Université de Montréal and the National Bank of Canada, for having funded this work.

PREFACE

This research project was motivated by the need for a comprehensive survey of work that has been done in the multi-disciplinary area of pseudo-telepathy.

This need became apparent to me when, after Gilles Brassard, Alain Tapp and I published a pseudo-telepathy game that we though was new [BBT03], Serge Massar kindly pointed out to us that similar work [Mer90b] had appeared more than ten years ago in the physics literature.

Since writing this Master's thesis, I have prepared, along with my co-authors, two manuscripts that originate from this work. *Quantum Pseudo-Telepathy* [BBT04a] is a survey of pseudo-telepathy games, and *Recasting Mermin's multi-player game into the framework of pseudo-telepathy* [BBT04b] presents the novel results from section 5.2 of the present document, some of which have been greatly simplified.

CHAPTER 1

INTRODUCTION

Niels Bohr, one of the fathers of quantum physics, said that if studying quantum mechanics doesn't make you dizzy, you haven't understood it properly.

The present thesis, which deals with quantum information processing (QIP), is meant to be a remedy to the sometimes profound dizziness we feel when studying such strange concepts. With the use of pseudo-telepathy games, it objectively shows the power of the quantum world and unveils some of its mysteries.

QIP is concerned with what we can and cannot do with quantum information; its fundamentals lie in the area of quantum mechanics, which is the study of matter at the atomic level. Quantum mechanics is the best tested theory that describes our world. To better understand the wonders of quantum mechanics and thus of QIP, it is good to see how our predecessors saw and thought about these ideas.

1.1 Measurements and Spooky Action at a Distance

According to the predictions of quantum mechanics, when performing measurements related to the position and momentum of an electron, the precise knowledge of one quantity prevents such a knowledge of the other.

This prompts the following question: If it is impossible to measure both the position and momentum of an electron with arbitrary precision, then can an electron have both a position and momentum?

For many physicists, including Bohr, the answer to this question is that the two quantities cannot simultaneously exist. As Jordan asserts:

> observations not only disturb what has to be measured, they produce it! ... We compel it [the electron] to assume a definite position ... we ourselves produce the results of measurement. [Jam74]

For Einstein, however, the answer was different. He did not reject the predictions of quantum mechanics, but was bothered by its consequences. For him, if the quantum theory cannot describe both the position and momentum of an electron, then the quantum theory does not provide a complete description of the electron. Thus, he concluded that quantum mechanics must be "incomplete".

In support of this conviction, Einstein published in 1935 an article with Podolsky and Rosen [EPR35], in which they present a *gedanken* experiment. A gedanken ("thought") experiment is "a hypothetical sequence of events about which the quantum theory makes quite definite predictions" [Mer90a]. The purpose of the scenario is to challenge the quantum theory on the basis of its *predictions*, and so to make the point, it is not necessary to actually carry out the experiment. This particular gedanken experiment is meant to provide evidence of the existence of *elements of reality*, also called *hidden variables*, defined as in [EPR35]:

> If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

In the *gedanken* experiment, Einsten, Podolsky and Rosen (EPR) consider two particles that may originally interact. They are then separated into two distinct regions, A and B. EPR then claim that by choosing to measure either the position or the momentum of a particle in region A, one could learn either the position or the momentum of a second particle in region B. Since the measurements in A can not disturb the particle in region B, they conclude that the particle in region B must have had both its position and momentum all along, i.e. there are elements of reality that correspond to the position and momentum.

Because the quantum theory cannot assign values to both quantities at once, it must provide an incomplete description of physical reality. But there is an alternative explanation: the position or momentum measurement at A could influence the the particle at B, setting its position or momentum: "Spukhafte Fernwirkung" or "spooky action at a distance". This phenomenon, which is predicted by quantum mechanics, was also rejected by Einstein. He did not doubt the predictive power of quantum mechanics, but insisted that it was incomplete. According to him, (and supported by his gedanken experiment), there had to be some underlying information (elements of reality or hidden variables) which determines the outcome of the measurements. The elements of reality are not directly observable, yet we witness their effect each time that we perform a measurement in region A or B.

The reaction of other physicists to the EPR paper was that this was an area of meta-physics; the question was unanswerable to scientific observation, and unworthy of argumentation. As Pauli wrote,

> As O. Stern said recently, one should no more rack one's brain about the problem of whether something one cannot know anything about exists all the same, than about the ancient questions of how many angels are able to sit on the point of a needle. But it seems to me that Einstein's questions are ultimately always of this kind. [EBB71]

1.2 Bell's Response

In 1964, Bell gave a shocking reply to EPR by publishing a paper [Bel64] in which he proposes a *gedanken* experiment that rules out any possibility of hidden variables in the quantum theory.

Having put the EPR thesis in perspective in the previous section, one should be surprised that Bell was able to irrefutably show his result. EPR's argument was not a question of meta-physics, after all! The physicist Henry Stapp called Bell's discovery "the most profound discovery of science" [Sta75]. In order to be able to state Bell's theorem, we first give some definitions:

Definition 1.2.1. A *local theory* is one in which no action performed at location A can have an instantaneous (faster than light) observable effect at location B.

Definition 1.2.2. A *realistic theory* in one in which all measurement outcomes pre-exist before the measurement.

With this formalism, we note that EPR argued in 1935 that *any* complete theory must be local and realistic, Bell's answer is to show the following theorem:

Theorem 1.2.1 (Bell's Theorem). *No local, realistic theory can explain the predictions of quantum mechanics.*

Bell proved his theorem by exhibiting a quantum system involving two particles. He showed that if we assume the presence of hidden variables, as well as the locality condition, then the outcomes of the experiment are in contradiction with the outcomes predicted by quantum mechanics. Thus quantum mechanics is not a local, realistic theory.

We won't give the details of Bell's argument here, because in the next one hundred pages or so of the present document, we will effectively prove over and over again Bell's theorem. Exactly how this is done is explained in the following section.

1.3 Pseudo-Telepathy

The previous section presented a part of the history of physics, which motivates our research. We wish to adopt for the rest of this thesis the QIP paradigm; for that, we must note an important correspondence: a *classical* theory denotes a *local* and *realistic* theory. Thus, if something or someone is constrained to act in a classical fashion, they do not have access to any quantum mechanical resource.

To which quantum mechanical resource are we referring? The answer is *entanglement*, the "iron to the classical world's bronze age" [NC00]. The properties of this resource are still not well understood, but we can say for sure that it is thanks to entanglement that we get results such as Bell's theorem. Entanglement causes the "spooky action at a distance" (also referred to as *nonlocality*) that Einstein rejected. It is also thanks to entanglement that we can devise amazing games such as pseudo-telepathy games: *pseudo-telepathy* is defined informally as the characteristic of a game in which no communication is allowed, and in which quantum players (sharing entanglement) always succeed, but for which the classical players have an unavoidable, non-zero probability of failure.

1.3.1 Telepathy and *Pseudo*-Telepathy

Telepathy is “communication from one mind to another without using sensory perceptions”. With this definition in mind, what do we mean by *pseudo*-telepathy? Suppose that we have a pseudo-telepathy game that involves two players, Alice and Bob. They are not allowed to communicate with each other. If they were classical, we know that they would sometimes fail. However, if they share entanglement, they always succeed at the given game. So, if we introduce a witness, who looks at the results of the game, but who does not believe in the quantum theory (or anything beyond the classical theory), then the *only* possible explanation, given that Alice and Bob consistently win, is that they must have a way to signal to each other—they must be telepathic!

We know, however, that this is not the case. We know that Alice and Bob share entanglement and that it is thanks to this that they *appear* to be telepathic. Hence, pseudo-telepathy. There are limits to what Alice and Bob, who share entanglement, can do. Specifically, “entanglement alone cannot be used to signal information—otherwise faster-than-light communication would be possible and causality would be violated” [Bra03].

1.3.2 Pseudo-Telepathy and Bell’s Theorem

We’ve already stated that this document is dedicated to proving Bell’s theorem. Indeed, pseudo-telepathy proves Bell’s theorem in the following way: in pseudo-telepathy, the quantum players have a clear advantage over the classical players. Recall that classical players are restricted to a local, realistic theory. Since the quantum players always win and the classical players do not, we conclude that no local, realistic theory can reproduce the predictions of quantum mechanics—which is precisely the essence of Bell’s theorem.

1.4 Related Work

Research in the area of pseudo-telepathy originally appeared in the physics literature, as these games provide a proof of Bell's theorem. This area of research is still active. Of course, the terminology, notation and even the context differ widely from the usual paradigm adopted in QIP, which is part of the challenge in writing the present document. Pseudo-telepathy games sometimes appear under the following names:

- Bell's theorem without inequalities [GHSZ90]
- Bell's theorem without inequalities and without probabilities [Cab01b]
- GHZ-type game
- always-vs-never refutation of Einstein, Podolsky and Rosen [Mer90e]
- Bell inequality [BM93]
- all-versus-nothing violation of local realism [CPZ$^+$03].
- "all versus nothing" inseparability [Cab01b]
- inequality-free proof of Bell's nonlocality theorem [Ara99]

Other works on pseudo-telepathy appear in the QIP literature, more precisely in a *communication complexity* context. Here, we find pseudo-telepathy under such headings as "nonlocality games", "cooperative games", "interactive proof systems" and of course, "pseudo-telepathy". We also find related work in the philosophy literature.

1.5 Contributions

The present thesis is a collection of pseudo-telepathy games. Far from being a simple literature review, this document presents many original contributions:

1. The fact that the games appear in a variety of contexts (theoretical physics, experimental physics and QIP—see section 1.4) means that a considerable amount of work has been done to make a uniform presentation of the games and related results.

2. In section 3.2.1 ("The Promise"), we give a formal definition of a *promise game*.

3. In section 4.5 ("The Magic Square and Cabello's Game Are Equivalent"), we provide a definition of *equivalent* two-player games, and show that the two games are equivalent.

4. In section 5.2 ("Parity Game"), theorems 5.2.2 and 5.2.6, concerning the classical success proportion and classical success probability of the parity game are proven. This is original work of the author.

5. Also in section 5.2, theorem 5.2.16, concerning error-free strategies for the parity game is proven. This is also original work of the author.

1.6 Structure of the Thesis

The remainder of the present document is divided into four chapters. Chapter 2 gives the basic notation and principles of QIP. Chapter 3 is concerned with pseudo-telepathy in general: we give a formal definition of pseudo-telepathy and present general notation and concepts that are useful in presenting pseudo-telepathy games. Finally, chapters 4 and 5 are dedicated to the presentation of a total of seven pseudo-telepathy games (eight if we distinguish the two equivalent games). They are divided into chapter 4, which presents *two-party* games and chapter 5, which presents *multi-party* games, which are games with three or more players.

CHAPTER 2

QUANTUM INFORMATION PROCESSING

In this chapter, we give definitions and theorems that relate to quantum information processing, which we will need in the rest of the document. This is not meant to be a comprehensive introduction to the area, but only to specific tools that are required in the context of pseudo-telepathy. A good reference for quantum information processing is [NC00].

2.1 The Qubit

The *bit* is the fundamental unit of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit or *qubit.* Qubits, like bits, are realized on actual physical systems. Here, we treat them as abstract mathematical objects. A qubit can be in the state $|0\rangle$ or $|1\rangle$. It can also be in a *superposition* of states $|0\rangle$ and $|1\rangle$: an arbitrary qubit can be written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. We also write $|\psi\rangle$ as a column vector using the convention that $\{|0\rangle, |1\rangle\}$ form the *standard basis*:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

The nature of quantum information implies that we cannot extract the *amplitudes* α and β from $|\psi\rangle$; we are only able to make statistical inferences about these values (more about this in section 2.3). It is also impossible to *clone* quantum information. That is, it is not possible to start from one qubit in an unknown state and make two identical copies of it.

2.2 Complex Inner Product Space

Let $\mathcal{H}_d$ denote a a d-dimensional complex inner product space (a complex vector space equipped with a complex inner product) over $\mathbb{C}$. The notation $\mathcal{H}_d$ reminds us of a *Hilbert* space; this is because the finite dimensional complex inner product spaces that come up in quantum computation and quantum information are Hilbert spaces. Qubits are column-vectors in $\mathcal{H}_2$. We define $\langle\psi|$ ("bra") to be the row vector that is the conjugate transpose of $|\psi\rangle$ ("ket"). Then $\langle\phi||\psi\rangle$, usually written as $\langle\phi|\psi\rangle$, denotes the *inner product* of $|\phi\rangle$ with $|\psi\rangle$. The *norm* of $|\psi\rangle$, denoted $\||\psi\rangle\|$ is defined as $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$. Thus qubits have norm 1.

2.3 Basic Operations

We introduce three basic operations on qubits: initialization, unitary transformation and measurement. In what follows, we take for granted that these operations can be performed perfectly.

1. *Initialization.* It is possible to initialize a qubit to the state $|0\rangle$ or $|1\rangle$.

2. *Unitary Transformation.* We can perform any unitary transformation, given by

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

   where $u_i \in \mathbb{C}$. U is *unitary* if and only if $UU^\dagger = I$, where $U^\dagger$ is the conjugate transpose of U and I is the identity matrix. We also denote the above U as:

$$|0\rangle \overset{U}{\longmapsto} u_{00}|0\rangle + u_{10}|1\rangle$$
$$|1\rangle \overset{U}{\longmapsto} u_{01}|0\rangle + u_{11}|1\rangle.$$

A very useful unitary transformation is the *Hadamard* transform, given by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

In other words,

$$|0\rangle \overset{H}{\longmapsto} \tfrac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$|1\rangle \overset{H}{\longmapsto} \tfrac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

3. *Measurement.* So far, we've seen that we can initialize a qubit and perform a unitary transformation. We also need to have a way to measure a qubit. As we have already stated, a measurement will not yield the complete description of the qubit; measurement in the standard basis of an arbitrary qubit $\alpha|0\rangle + \beta|1\rangle$ results in the following:

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \begin{cases} 0 \text{ with probability } |\alpha|^2 \\ 1 \text{ with probability } |\beta|^2 \end{cases}$$

Furthermore, measurement alters the qubit. After the measurement, the state *collapses* to $|0\rangle$ if 0 was measured and $|1\rangle$ if 1 was measured.

It is also possible to measure an arbitrary qubit $|\psi\rangle$ with respect to *any* orthonormal basis B of $\mathcal{H}_2$, say $B = \{|b_1\rangle, |b_2\rangle\}$. Then the probability of getting result b_i when measuring $|\psi\rangle$ is given by

$$p(b_i) = |\langle\psi|b_i\rangle|^2$$

Given that result b_i was measured, the state of the quantum system immediately after the measurement collapses to $|b_i\rangle$.

What if we want to start a protocol in a state other than $|0\rangle$ or $|1\rangle$, for example, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$? The solution is to start in the state $|0\rangle$ and apply a unitary transformation (for the specific example, we would apply the Hadamard transform). Hereafter, if we start a protocol in a state $|\psi\rangle$ other than $|0\rangle$ or $|1\rangle$, it is because, implicitly, we have applied a unitary transformation to one of the basis states to obtain $|\psi\rangle$.

2.4 n-Qubit Systems

We have seen how we can work with a single qubit. Now, we would like to be able to work with a system of n qubits. It turns out that we can easily extend the basic operations on a single qubit to operations on any number of qubits.

An n-dimensional qubit system is a 2^n-dimensional norm 1 vector in $\mathcal{H}_{2^n}$. For example, for $n = 3$, an arbitrary 3-qubit quantum register can be written as:

$$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{bmatrix} = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \ldots + \alpha_{111}|111\rangle = \sum_{x\in\{0,1\}^3} \alpha_x|x\rangle$$

where $\sum_x |\alpha_x|^2 = 1$.

Formally, we combine systems with the *Kronecker* product (also erroneously called the *tensor* product) of vectors; if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\phi\rangle = \alpha'|0\rangle + \beta'|1\rangle$, then $|\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_2 \otimes \mathcal{H}_2 = \mathcal{H}_{2^2}$, and

$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} \alpha\phi \\ \beta\phi \end{bmatrix} = \begin{bmatrix} \alpha\alpha' \\ \alpha\beta' \\ \beta\alpha' \\ \beta\beta' \end{bmatrix}.$$

In this representation, terms like $\alpha\phi$ denote the 2×1 submatrix whose entries are proportional to $|\phi\rangle$, with overall proportionality constant α. When using the ket notation, we often drop the $\otimes$ symbol. Thus, $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$.

The same three basic operations of section 2.3 hold for an n-qubit system: we may initialize to any basis state $|x\rangle$ where $x \in \{0,1\}^n$. We can perform any unitary operation given by a $2^n \times 2^n$ unitary matrix U. We can perform a measurement of a state $|\psi\rangle$ in any orthonormal basis B of $\mathcal{H}_{2^n}$, say $B = \{|b_1\rangle, \ldots, |b_{2^n}\rangle\}$. The probability of getting result b_i when measuring $|\psi\rangle$ is given by:

$$p(b_i) = |\langle\psi|b_i\rangle|^2.$$

Given that result b_i was measured, the state of the quantum system immediately after the measurement collapses to $|b_i\rangle$.

When referring an n-qubit system, we use denote $\overbrace{U \otimes U \otimes \cdots \otimes U}^{n}$ by $U^{\otimes n}$. We also write $|0^n\rangle$ to represent $|\overbrace{00\ldots0}^{n}\rangle$. Also, as in the one qubit case, if we start a protocol in a state $|\psi\rangle$ other than a basis state, it is because, implicitly, we have applied a unitary transformation to one of the basis states to obtain $|\psi\rangle$.

2.5 Operations on Parts of a System

So far, we've considered operations on a system as a whole. It is also possible to act on *part* of a system.

For example, Alice and Bob can share a two-qubit system: Alice takes the first qubit and Bob the second. Once this is done, they may become physically separated. Say Bob applies a unitary transformation U. Then the effect on the system is to apply the transformation $I \otimes U$, given by the matrix:

$$I \otimes U = \begin{bmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

This can be generalized to an operation on any partial system of any dimension. Measurements may also be performed on part of a system; for any state $|\psi\rangle \in \mathcal{H}_{ABC}$, we can measure the subspace B. A particular state of interest is:

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |a_i\rangle |i\rangle |c_i\rangle.$$

By measuring the subspace B, we obtain the result i with probability $|\alpha_i|^2$ and the resulting state is $|a_i\rangle|i\rangle|c_i\rangle$.

It is useful to note that we get the same effect if we perform two measurements on different subsystems, or if we perform the measurements together. Also, the same effect is obtained if two parties are to perform some unitary transformation and then measure—regardless of the order in which the parties perform their actions.

2.6 Entanglement

Given an $m+n$ qubit state $|\psi\rangle \in \mathcal{H}_{2^m} \otimes \mathcal{H}_{2^n}$, we say that $|\psi\rangle$ is a *product state* if $|\psi\rangle = |\gamma\rangle|\delta\rangle$ for $|\gamma\rangle \in \mathcal{H}_{2^m}$ and $|\delta\rangle \in \mathcal{H}_{2^n}$. If $|\psi\rangle$ is not a product state, then it is an *entangled* state.

Examples of entangled states are the *Bell states*:

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi^-\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi^-\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

The state $|\Psi^-\rangle$ is also known as an Einstein-Podolsky-Rosen (EPR) pair. We will use it to demonstrate one of the "mysteries" of entanglement: If Alice and Bob share an EPR pair, and Alice measures her qubit in the standard basis, the outcome will be 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. Likewise, Bob's measurement in the standard basis will yield 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. However, we know for sure that Alice and Bob's outcomes will be opposites. Hence, by knowing one of the outcomes, we can predict with certainty the other; this "spooky action at a distance" is a surprising feature of entanglement. Furthermore, if Alice and Bob perform measurements of $|\Psi^-\rangle$, in *any* basis, we can be sure that the outcomes will be opposites.

We will make use of the state $|\Phi^+\rangle$ in the following context: Suppose Alice and Bob share two $|\Phi^+\rangle$ states:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

where Alice has the first and third qubits, and Bob the second and fourth ones. We can re-write this as:

$$|\psi\rangle = \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right)$$

where, this time, Alice has the first two qubits and Bob the second two. Generalizing this, we see that if Alice and Bob share n $|\Phi^+\rangle$ states, then they share the entangled state $|\Phi^+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|jj\rangle$.

CHAPTER 3

PSEUDO-TELEPATHY

The goal of this chapter is to facilitate discussion by presenting notation and results that relate to pseudo-telepathy games in general. At the end of the chapter, we give details on the presentation of the games. The general framework of this chapter is useful in chapters 4 and 5, where several games are presented.

3.1 Playing the Games

Definition 3.1.1. An n-player *game* $G_n = (X, Y, P, W)$ consists of:

- $X = X_1 \times X_2 \times \ldots \times X_n$, where $X_1, X_2, \ldots X_n$ are sets of possible *inputs*
- $Y = Y_1 \times Y_2 \times \ldots \times Y_n$, where $Y_1, Y_2, \ldots Y_n$ are sets of possible *outputs*
- a predicate P on X called the *promise*
- a relation W on $X \times Y$, called the *winning condition*

An *instance* (figure 3.1) of the game proceeds in the following way:

1. A *question* $x = x_1, x_2, \ldots, x_n \in X$ is chosen from the set P. (We use a slight abuse of notation, using P as a predicate and as the set of elements in X that satisfy the predicate)
2. Each player i receives his input $x_i \in X_i$.
3. Each player i responds with an output $y_i \in Y_i$.
   Let $y = y_1, y_2, \ldots, y_n$ be the *answer*.
4. The players win if $(x, y) \in W$, and they lose otherwise.

The following rule governs the way the game is played:

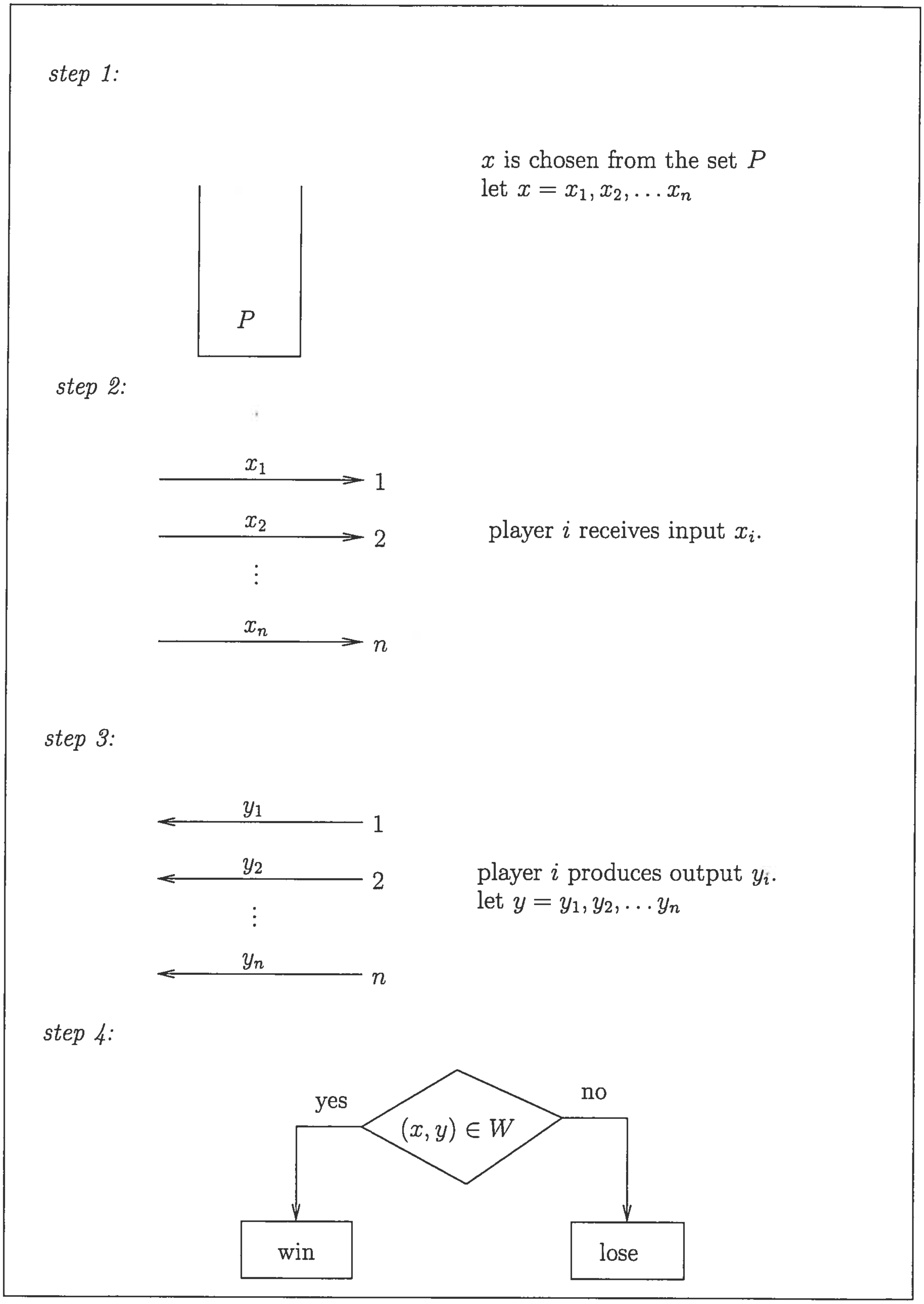

step 1:
P
x is chosen from the set P
let $x = x_1, x_2, \ldots x_n$
step 2:
x_1
1
x_2
2
$\vdots$
x_n
n
player i receives input x_i.
step 3:
y_1
1
y_2
2
$\vdots$
y_n
n
player i produces output y_i.
let $y = y_1, y_2, \ldots y_n$
step 4:
yes
$(x, y) \in W$
no
win
lose

Figure 3.1: A Pseudo-Telepathy Game

> No communication between the players is allowed during the game. Before the start of the game, the players may agree on a *strategy.* They may share random bits, and, if they are quantum players, they may share entanglement.

Suppose that we have a game $G_n = (X, Y, P, W)$ such that there exists an $x_0 \in X$ such that $P(x_0) = \mathit{true}$ and $x_0 \notin \mathit{domain}(W)$. Then there is no way of winning if the players are given question x_0. This leads to a game that is not interesting in the context that we wish to study. Hence, all games $G_n = (X, Y, P, W)$ that we consider have the property that:

$$\forall x \in X, P(x) = \mathit{true} \Rightarrow x \in \mathit{domain}(W). \tag{3.1}$$

3.2 Strategies

Players, whether classical or quantum, will always use a *strategy* to determine what their answer y will be, given a particular question x. According to game theory, a player's strategy is "a plan which specifies what choices he will make in every possible situation, for every possible actual information which he may possess at that moment ..." [NM44].

In the games that we study, as either all players win or they all lose, their best strategy is to collaborate to maximize their probability of winning. Such games are in the class of *cooperative games.* We specify if the players are *classical* or *quantum.* Classical players may have a *deterministic* strategy. They may also have access to shared randomness, which allows them to use a *probabilistic* strategy, which is a probability distribution over a finite set of deterministic strategies. Quantum players have access to entanglement, which they may exploit in their *quantum strategy.* In pseudo-telepathy, quantum players have a winning strategy and classical players do not. For the classical players, we want to know just how well they can succeed.

We say that a strategy is a *winning strategy* if it succeeds on all instances of the game. We also classify the success of strategies according to the following:

Definition 3.2.1. A deterministic strategy is successful in *proportion* p if the ratio of the number of instances for which the players win and the total number of instances is p.

Definition 3.2.2. A strategy is successful with *probability* q if it wins *any* instance with probability at least q.

Some strategies are better than others; those that are *optimal* reach the following optimal bounds:

Definition 3.2.3. Let G_n be a game. We define:

1. $\widetilde{\omega}_c(G_n)$ to be the maximum success proportion, over all possible deterministic strategies, for classical players that play the game G_n
2. $\omega_c(G_n)$ to be the maximum success probability, over all possible strategies, for classical players that play the game G_n
3. $\omega_q(G_n)$ to be the maximum success probability, over all possible strategies, for quantum players that play the game G_n

In pseudo-telepathy, the quantum players have a winning strategy, and the classical players do not. This amounts to saying that $\omega_q(G_n) = 1$ and $\widetilde{\omega}_c(G_n) < 1$.

Definition 3.2.4. An n-player pseudo-telepathy game is a game G_n for which $\omega_q(G_n) = 1$ and $\widetilde{\omega}_c(G_n) < 1$

Suppose that a deterministic strategy is successful in proportion $p < 1$. Then there is at least one instance of the game where the players systematically fail, hence the strategy's success probability is $q = 0$, so we must consider probabilistic strategies in order to obtain a meaningful bound on $\omega_c(G_n)$. However, the next two theorems state that if we know that the maximum success proportion of a deterministic strategy is p, then we have that $\omega_c(G_n) \leq p$.

Proposition 3.2.1. *Let G_n be a game. Then $\widetilde{\omega}_c(G_n)$ is the maximum probability that the players win if the questions are asked uniformly at random among questions that satisfy the promise.*

Proof. We consider a general probabilistic strategy s which is a probability distribution over a finite set of deterministic strategies, say $\{s_1, s_2, \dots s_m\}$. Let $\Pr(s_i)$ be the probability that strategy s_i is chosen, and let p_i be the success proportion of strategy s_i. The probability that the players win the game is:

$$\begin{aligned}\sum_{i=1}^{m} \Pr(s_i) p_i &\leq \sum_{i=1}^{m} \Pr(s_i) \widetilde{\omega}_c(G_n) \\ &= \widetilde{\omega}_c(G_n)\end{aligned}$$

Furthermore, by definition, there exists a strategy that succeeds with probability $\widetilde{\omega}_c(G_n)$. □

Theorem 3.2.2. *For any game G_n, $\omega_c(G_n) \leq \widetilde{\omega}_c(G_n)$.*

Proof. Consider any strategy s that is successful with probability $\omega_c(G_n)$. By definition, for every question x satisfying the promise P, the probability of winning on question x is $\Pr(\text{win} \mid x) \geq \omega_c(G_n)$. If the question is chosen uniformly at random, the probability q of winning the game using the same strategy s is

$$\begin{aligned}q &= \sum_{x \in P} \frac{\Pr(\text{win} \mid x)}{|P|} \\ &\geq \sum_{x \in P} \frac{\omega_c(G_n)}{|P|} \\ &= \omega_c(G_n)\end{aligned}$$

By proposition 3.2.1, $\widetilde{\omega}_c(G_n) \geq q$, and since $q \geq \omega_c(G_n)$, then $\widetilde{\omega}_c(G_n) \geq \omega_c(G_n)$. □

The next lemma is useful when determining values of $\widetilde{\omega}_c(G_n)$.

Lemma 3.2.3. *Let $G_n = (X, Y, P, W)$ be a game with $\widetilde{\omega}_c(G_n) < 1$. Then*

$$\widetilde{\omega}_c(G_n) \leq \frac{|P| - 1}{|P|}$$

Proof. Since $\widetilde{\omega}_c(G_n)$ is the maximum success proportion, over all possible deterministic strategies, for classical players that play the game G_n, it is the ratio of the maximum number of questions that satisfy the promise and on which classical players can win, and the total number of questions that satisfy the promise.

Since $\widetilde{\omega}_c(G_n) < 1$, the next best alternative is that $\widetilde{\omega}_c(G_n) = \frac{|P|-1}{|P|}$. So we conclude that $\widetilde{\omega}_c(G_n) \leq \frac{|P|-1}{|P|}$. □

3.2.1 The Promise

In step 1 of an instance of the game $G_n = (X, Y, P, W)$, a question is chosen among all questions satisfying the promise P. In other words, it is possible that a certain $x = x_1, x_2, \ldots, x_n \in X$, yet x is not a valid question ($P(x) = false$). Although they make the game more artificial, we often (but not always—see sections 4.3, 4.4 and 4.6) rely on such promises in order to ensure an advantage for the quantum players.

The concept of a promise game has appeared in QIP literature before, for example, in the context of the Deutsch-Jozsa problem [DJ92]. In the case of pseudo-telepathy, we give our interpretation for defining a game with and without a promise:

Definition 3.2.5. Let $G_n = (X, Y, P, W)$ be a game. We say that G_n is *promise-free* if all of the following hold:

1. $\forall x \in X, P(x) = true$
2. $\forall x \in X, \exists y \in Y$ such that $(x, y) \notin W$
3. $\forall i \in \{1, 2, \ldots, n\}, \forall y_i \in Y_i, \exists x \in X, \exists y = y_1, y_2, \ldots, y_i, \ldots, y_n \in Y$ such that $(x, y) \in W$

Otherwise, we say that G_n is a *promise game.*

A game is promise-free if all three conditions of definition 3.2.5 are met. The motivation for the first and second conditions is obvious. The third condition is there to ensure that each element in $Y = Y_1 \times Y_2 \times \ldots \times Y_n$ is useful. In other words, one cannot introduce a bogus element in one of the player's answers, and then conclude that the game is error-free according to condition 2.

Of course, given a game $G_n = (X, Y, P, W)$ where $P(x_0)$ is false for a given $x_0 \in X$, it is possible to convert it to a game $G'_n = (X, Y, P', W')$ where $P'(x_0) = \text{true}$ (and $P'(x) = P(x)$ otherwise), by simply specifying in the winning condition W' that $\forall y \in Y$, $(x_0, y) \in W'$ (and W' is otherwise unchanged from W). By repeatedly applying this technique to all such x_0, we convert G_n into a game $G''_n = (X, Y, P'', W'')$ where P'' is the constant true predicate, and so we have eliminated the need for the promise P. Note, however, that according to definition 3.2.5, G''_n is still a promise game (since, for example, $(x_0, y) \in W, \forall y \in Y$).

We may also proceed in the opposite direction. Given a game G_n, suppose that $\exists x_0 \in X$ such that $\forall y \in Y$, $(x_0, y) \in W$. We can then derive a new game $G'_n = (X, Y, P', W')$ where $P'(x_0) = \mathit{false}$ (and $P'(x) = P(x)$ otherwise) and where x_0 is removed from *domain*(W), which yields W'[1]. Continuing in this way, we arrive at a game $G''_n = (X, Y, P'', W'')$ such that $\forall x \in X$, either $P''(x)$ is false or $\exists y \in Y$ such that $(x, y) \notin W''$. We call such a game a *min-promise* game (since $\{x \in X \mid P''(x) = \mathit{true}\}$ is smallest possible). In the present document, we will consider games G_n in their min-promise form only, since by the following lemma, $\widetilde{\omega}_c(G_n)$ is smallest for these games.

Lemma 3.2.4. *Let G''_n be a min-promise game, obtained from game G_n as above. Then $\widetilde{\omega}_c(G''_n) \leq \widetilde{\omega}_c(G_n)$.*

Proof. If G_n is already in its min-promise form, then $\widetilde{\omega}_c(G''_n) = \widetilde{\omega}_c(G_n)$. Otherwise, we claim that for each iteration i of the above process, assuming we start from game

[1] Strictly speaking, it is not necessary to clean up W in this way.

$G_n^i = (X, Y, P^i, W^i)$ and that the result is the game $G_n^{i+1} = (X, Y, P^{i+1}, W^{i+1})$, we have $\widetilde{\omega}_c(G_n^{i+1}) < \widetilde{\omega}_c(G_n^i)$. To show this, suppose that $\widetilde{\omega}_c(G_n^i) = \frac{x}{|P^i|}$. Then,

$$\begin{aligned}\widetilde{\omega}_c(G_n^{i+1}) &= \frac{x-1}{|P^{i+1}|} \\ &= \frac{x-1}{|P^i|-1} \\ &< \frac{x}{|P^i|} \\ &= \widetilde{\omega}_c(G_n^i).\end{aligned}$$

Since each iteration yields a game with smaller success proportion, we conclude that $\widetilde{\omega}_c(G_n'') < \widetilde{\omega}_c(G_n)$. □

We have given a definition for a promise-free game, yet there are other restrictions on W and P that may be interesting to study. Let $G_n = (X, Y, P, W)$ be a game. We consider two restrictions on W and on P:

1. W is a function (i.e. $(x, y_1) \in W \wedge (x, y_2) \in W \Rightarrow y_1 = y_2$)
2. W is a function and $\forall x \in X, P(x) = \mathit{true}$

A game G_n with $|X| > 1$ that satisfies (2) is a promise-free game according to definition 3.2.5, but this is not necessarily the case for (1).

We will see in chapter 4 that two-player promise-free pseudo-telepathy games exist. However, it is not known if there are pseudo-telepathy games satisfying (1) or (2). This would be an interesting question to ponder, and even more interesting to solve!

3.3 Physical Realizations and Loopholes

Suppose we want to execute a physical experiment to show that there is no local realistic (classical) model of reality, using a pseudo-telepathy game. We call this an *experimental demonstration of Bell's Theorem.*

The *ideal* experiment would be to set up a quantum system and run many instances of the game until either:

1. the players lose, in which case we conclude that the predictions of quantum mechanics are wrong, and it's back to the drawing board, or

2. the players win consistently for a sufficiently large number of instances to rule out (with high probability) any classical strategy (based on a local, realistic model)

This experiment contrasts with many experimental demonstrations of Bell's theorem in that we are not interested in verifying a *statistical* difference between the quantum and classical players, such as in the Bell [Bel64], CHSH [CHSH69], or Mermin [Mer81a, Mer81b] proofs of Bell's theorem. Instead, the ideal experiment above tells us that as soon case 1 happens, we reach a definite conclusion. This principle is referred to as an "all-or-nothing" experiment, since it involves either complete success or failure (as long as we run enough instances of the game). It is surprising that we can devise such an experiment. After Bell stated his famous theorem in 1964, and for about 20 years, the only experimental demonstrations of Bell's theorem were statistical, which is what lead Mermin [Mer90e] to write:

> I was surprised to learn of this always-vs-never refutation of Einstein, Podolsky and Rosen. ... I recently declared in writing that no set of experiments, real or *gedanken*, was known that could produce such an all-or-nothing demolition of the elements of reality. With a bow of admiration to Greenberger, Horne and Zeilinger, I hereby recant.[2]

The laboratory setting offers conditions that are far from the ideal world. Therefore, we must now incorporate imperfections into the analysis of experimental data drawn from an "all-or-nothing" experiment. In this non-ideal situation, a single occurrence of case 1 does not allow us to reach a definite conclusion; instead, we

[2] Mermin was probably unaware of the earlier pseudo-telepathy game, described in section 4.1.

must account for errors. This is not an easy task; it seems that for each real-world experiment that is reported, there is consistently an argument that comes up which invalidates the experiment and allows for a classical theory to explain the results. These counter-arguments exploit what are called *loopholes*, i.e. ambiguities that make it possible to evade a difficulty.

For example, one of the first experimental demonstrations of Bell's theorem [AGR82, ADR82] suffered from the locality loophole, [Fra85, GZ99], which exploits a timing flaw in the experiment setup. Other counter-arguments include the memory loophole [BCH$^+$02], which exploits the assumption that the nth measurement is independent from the first $n-1$ measurements, and the detection loophole [Pea70, Mas02], which is based on the fact that in real experiments, only a fraction of the instances yield a correct answer.

Here, we will address only one such loophole argument, namely the detector efficiency problem: real-world detectors are *noisy* and *inefficient*, thus, in the real-life laboratory, we cannot expect to always witness the results predicted by quantum mechanics.

We want to know how we can work with the noise and inefficiencies to devise an experimental demonstration of Bell's theorem that does not exploit the detection loophole. Of course, the more tolerant to detector noise and inefficiencies our game is, the more convincing it might be.

Taking into account these errors, the experiment must change. It is possible for the quantum players to lose (in the case of an error due to noise), or for the answer to be lost (in the case of an error due to an inefficiency). So, we will run many instances of the game and collect the results (win/lose/draw), until we are satisfied that the classical players would not be able to win *as often* as the quantum players. This experiment will only be convincing if the detector noise and inefficiency rates are small enough. It is not an easy task to devise experiments that are statistically convincing; we only mention here that work on this subject has been done in [Per00, DGG03].

It is important to mention a common mistake in reasoning about experimental realizations of pseudo-telepathy games. Too often, we read that the all-or-nothing effect is to rule out local hidden variables in a *single run*: "The quantum nonlocality can thus, in principle, be manifest in a single run of a certain measurement." [CPZ+03] The fallacy here is that if the players (classical or quantum) win for a single run, we cannot conclude anything, except that they have guessed correctly. It is only by running many instances that we conclude that case 2 of the ideal experiment has been realized. There are many more examples of this mistake in the literature. As Peres wrote, about those who made this mistake: "The list of authors is too long to give explicitly, and it would be unfair to give only a partial list." [Per00].

3.3.1 Noisy Detectors

We consider this error model for binary outputs only. If there is noise, the output bit will be flipped. More formally, each individual player's answer y_i corresponds to the predictions of quantum mechanics (if the apparatus were perfect) with probability p. With complementary probability $1-p$, the player outputs $\overline{y_i}$, the complement of y_i. We say that this is a game with *errors*; $1-p$ is the *noise rate.*

For each game, there is a threshold on p, above which no classical strategy can succeed as well as a quantum strategy. This threshold is defined as $p_*(G_n)$:

Definition 3.3.1. $p_*(G_n)$ is the maximum value of p for which a classical strategy can succeed as well as a quantum strategy, in the game G_n with errors.

In general, we want to upper-bound $p_*(G_n)$.

3.3.2 Inefficient Detectors

Assume that the apparatus gives the correct answer most of the time, but sometimes it fails to give an answer at all. In this model, we enlarge each player's set of outputs Y_i to include the special symbol $\perp$ which means that the player's apparatus fails to give an answer. Formally, we redefine player i's possible outputs in game $G_n = (X, Y, P, W)$ by $Y_i = Y_i \cup \{\perp\}$. If, in the answer $y = y_1, y_2, \ldots, y_n$, we have $y_i = \perp$ for any i, then we say the players neither win nor lose, but that the outcome is a *draw.* If the outcome is not a draw, then we require that it be correct (i.e. it must satisfy the winning condition). We call such a game an error-free game.

For each player, we will assume that the measurement has probability η of giving a result and $1 - \eta$ of not giving a result. So $y_i = \perp$ with probability $1 - \eta$.

As in the case of noisy detectors, we are interested in the threshold of the efficiency rate η, above which no classical strategy can succeed as well as a quantum strategy. This threshold is defined as $\eta_*(G_n)$:

Definition 3.3.2. $\eta_*(G_n)$ is the maximum value of η for which a classical strategy can succeed as well as a quantum strategy, in the error-free game G_n.

If we assume that each apparatus's efficiency η is independent of the others, then η^n is the probability that all players give an answer. We usually calculate this probability, and from there, deduce η.

In general, we want to upper-bound $\eta_*(G_n)$. Some work has been done on this in [MP03]. The error-free model is usually easier to analyze than the model with errors, but it is obviously less realistic. In practice, noise could come from many sources, which means that the model with errors is the more realistic of the two.

3.4 Presentation of the Games

The present document is a collection of pseudo-telepathy games, in which we present many original contributions (see section 1.5). The games are presented in two separate chapters (chapter 4 for games with $n = 2$, called *two-party games* and chapter 5 for games with $n \geq 3$, called *multi-party games*). Each game G_n is presented according to the following format:

1. Background information on the game, as well as historical notes.

2. A table with summary information (table 3.1); some fields may be omitted if no information is known. The promise P and the winning condition W are

given as equations. These should be interpreted as: $P(x) =$ true if and only if x satisfies the given equation, and $(x, y) \in W$ if and only if (x, y) satisfies the given equation.

Name of the game	
n	number of players
X	set of questions
Y	set of answers
P	promise
W	winning condition
$\widetilde{\omega}_c$	maximum classical success proportion
ω_c	maximum classical success probability
p^*	maximum value of p for which a classical strategy can succeed as well as a quantum strategy
η^*	maximum value of η for which a classical strategy can succeed as well as a quantum strategy
$\|\psi\rangle$	quantum state used in the winning strategy

Table 3.1: Presentation of the games

3. Justification of each row of the table by theorems and proofs; we always give the quantum winning strategy, and then justify why $\omega_c(G_n) < 1$. For example, we will usually find a value or an upper bound for $\widetilde{\omega}_c(G_n)$. Then, by theorem 3.2.2, this value gives us an upper bound on $\omega_c(G_n)$.

CHAPTER 4

TWO-PARTY GAMES

In this chapter, we present five two-party pseudo-telepathy games. Among these games, there are three that are *scalable* (we can increase the length of each player's question). We also show that the remaining two games are *equivalent*. Since we consider games with only two players, we will call player 1 Alice and player 2 Bob. We denote a two-party game by G (instead of G_n, $n = 2$), or by G^k where k is a parameter that determines the length of the player's input and output for a scalable game G.

4.1 The Impossible Colouring Game

In response to Einstein, Podolsky and Rosen's argument for hidden variables (section 1.1), Kochen and Specker [KS67] presented an argument against hidden variables. They showed that under *non-contextuality*, hidden variables cannot exist. Briefly stated, non-contextuality is the principle according to which the probability of a given outcome in a measurement does not depend on the choice of the other orthogonal outcomes used to define that measurement. Bell's theorem and the Kochen-Specker theorem differ by their assumptions: Bell's theorem assumes locality, while Kochen-Specker's theorem assumes non-contextuality. Non-contextuality may not be experimentally verified:

> This doctrine, being 'counterfactual', is incapable of empirical verification and hence Bell regarded it, and the BKS[1] theorem to which it lead, as unsatisfactory; he prefered the Bell theorem instead with its reliance upon the much less problematic assumption of locality. [Ara99]

[1] The Kochen-Specker theorem is also known as the Bell-Kochen-Specker (BKS) theorem, due to [Bel66]. To be even more historically accurate, we should note that similar results appeared earlier in [Gle57], and in [Spe60].

In this section, we show how to convert the problematic assumption of non-contextuality from the Kochen-Specker theorem into the assumption of locality, effectively creating a pseudo-telepathy game. Kochen and Specker proved the following theorem:

Theorem 4.1.1 (Kochen-Specker Theorem). *There exists an explicit, finite set of vectors* $\{v_0, v_1, \ldots, v_{n-1}\} \in \mathbb{R}^3$ *that cannot be* $\{0, 1\}$*- coloured so that both of the following conditions hold:*

1. *For every orthogonal pair of vectors* v_i *and* v_j*, they are not both coloured 1.*
2. *For every mutually orthogonal triple of vectors* v_i*,* v_j *and* v_k*, at least one of them is coloured 1.*

Theorem 4.1.1 was originally proven using 117 vectors [KS67], and this has been reduced to 31 (with 17 orthogonal triples) by Conway and Kochen [Per93]. From theorem 4.1.1, it is possible to give an argument against hidden variables by using the non-contextuality assumption. We will not give the details here, since we are interested in showing how theorem 4.1.1 can be turned in to a pseudo-telepathy game, as first shown by [HR83] and then by [Sta83][2]. Here, we use a presentation inspired by [CHTW04]. This is no doubt the earliest example of pseudo-telepathy, which was overlooked by many, since Greenberger, Horne and Zeilinger (section 5.1) got most of the credit for inventing the first pseudo-telepathy game. There is actually an infinite family of pseudo-telepathy games that arises from *Kochen-Specker constructions.* A Kochen-Specker construction, similar from that of theorem 4.1.1, can be constructed in any dimension $d \geq 3$, either by geometric argument, or by extending a construction in dimension d to dimension $d + 1$ [Per93]. Geometric arguments can yield sets with smaller cardinality; for example, the smallest known set in four dimensions has 18 vectors [CEGA96].

[2] Stairs notes that Kochen offered a version of the argument, presumably before Heywood and Redhead, but never published it. He also notes that his own 1978 dissertation presents a similar argument.

A game G^m, for any Kochen-Specker construction of dimension $m \geq 3$ is given in table 4.1, where the following definition is used:

Definition 4.1.1. An *augmented Kochen-Specker construction of dimension* m is a normalized set of vectors $\{v_0, \ldots, v_{n-1}\} \subseteq \mathbb{R}^m$ that cannot be $\{0, 1\}$- coloured so that all of the following conditions hold:

1. For every orthogonal pair of vectors v_i and v_j, they are not both coloured 1.
2. For every mutually orthogonal m-tuple of vectors $v_{i_0}, v_{i_1}, \ldots, v_{i_{m-1}}$, at least one of them is coloured 1.
3. Every orthogonal pair of vectors is part of an orthogonal m-tuple.

Starting from the Kochen-Specker theorem, it is straightforward to find an augmented Kochen-Specker construction of any dimension m. The challenge that Alice and Bob face in the impossible colouring pseudo-telepathy game is given in table 4.1: Alice receives an orthonormal m-tuple of vectors $v_1, v_2, \ldots, v_m$. Bob receives a single vector $v_\ell \in \{v_1, v_2, \ldots, v_m\}$. Alice outputs $y_1 \in \{1, 2, \ldots, m\}$, indicating which of the m vectors of her input is assigned colour 1. Bob outputs a bit assigning a colour to his vector. The winning condition is that Alice and Bob assign the same colour to the vector that they receive in common. It is necessary to use an augmented Kochen-Specker construction of definition 4.1.1 in order to ensure that every vector appears in at least one instance of the game (although a modification of the game, where we can ask Alice to colour an n-tuplet, where $n \leq m$, does not require the use of the augmented Kochen-Specker construction). Unlike other pseudo-telepathy games, it is not straightforward to find $|X_1|$ and $|X_2|$, because it depends on the augmented Kochen-Specker construction that is used. It would be interesting to calculate these values.

As mentioned earlier, the pseudo-telepathy game based on the Kochen-Specker theorem appeared as early as 1983. Since then, other authors have explored the topic: [Ara99], [MA99] and [RW04].

Impossible colouring game	
n	2
X	Let K_m be an augmented Kochen-Specker construction of dimension $m \geq 3$. $X_1 = \{(v_1, \ldots, v_m) \mid (v_1, \ldots, v_m)$ are orthonormal m-tuples in $K_m\}$ $X_2 = \{v_\ell \mid v_\ell \in K_m\}$
Y	$Y_1 = \{1, 2, \ldots, m\}$, $Y_2 = \{0, 1\}$
P	$v_\ell \in \{v_1, \ldots, v_m\}$
W	$y_1 = \ell \Leftrightarrow y_2 = 1$
$\widetilde{\omega}_c$	< 1
ω_c	< 1
$\|\psi\rangle$	$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \|jj\rangle$

Table 4.1: Impossible colouring game

4.1.1 A Quantum Winning Strategy

Theorem 4.1.2. *Let G^m be the impossible colouring game. Then $\omega_q(G^m) = 1$.*

Proof. The player's strategy is to share the state $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jj\rangle$. After receiving their input, Alice and Bob do the following:

1. Alice performs a measurement in the basis $B_a = \{|v_1\rangle, \ldots, |v_m\rangle\}$. She outputs the index i corresponding to the measured vector.

2. Bob augments the set $\{|v_\ell\rangle\}$ to a basis $B_b = \{|v_\ell\rangle, |w_1\rangle, \ldots, |w_{m-1}\rangle\}$ of $\mathbb{R}^m$, and measures in the basis given by B_b. If the outcome is v_ℓ, he outputs 1, and outputs 0 otherwise.

To show that this quantum strategy works, we first remark that since the bases B_a and B_b have real coefficients, for any $|v_a\rangle = |v_{a,0}, v_{a,1}, \ldots, v_{a,m-1}\rangle \in B_a$ and

$|w_b\rangle = |w_{b,0}, w_{b,1}, \ldots, w_{b,m-1}\rangle \in B_b$,

$$\begin{aligned}\sum_{j=0}^{m-1} \langle j|v_a\rangle\langle j|w_b\rangle &= \sum_{j=0}^{m-1} v_{a,j} w_{b,j} && (4.1)\\ &= \sum_{j=0}^{m-1} \overline{v_{a,j}} w_{b,j} && (4.2)\\ &= \langle v_a|w_b\rangle. && (4.3)\end{aligned}$$

The probability that Alice measures v_i and Bob measures v_ℓ is given by:

$$\begin{aligned}\left|\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \langle j|\langle j|v_i\rangle|v_\ell\rangle\right|^2 &= \left|\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \langle j|v_i\rangle\langle j|v_\ell\rangle\right|^2 && (4.4)\\ &= \left|\frac{1}{\sqrt{m}} \langle v_i|v_\ell\rangle\right|^2 && (4.5)\\ &= \begin{cases} \frac{1}{d}, & i = \ell \\ 0, & i \neq \ell \end{cases} && (4.6)\end{aligned}$$

We see that the winning condition $y_1 = \ell \Leftrightarrow y_2 = 1$ is always met. This completes the proof that $\omega_q(G^m) = 1$.

□

4.1.2 Classical Success Proportion

Theorem 4.1.3. *Let G^m be the impossible colouring game. Then $\widetilde{\omega}_c(G^m) < 1$.*

Proof. Any classical deterministic strategy is a colouring with the properties of definition 4.1.1. Yet the set of vectors used, those of an augmented Kochen-Specker construction of dimension m, may not be coloured in this way; so Alice and Bob cannot have a classical winning strategy. □

It follows by theorem 3.2.2 that $\omega_c(G^m) < 1$.

4.1.3 Special Case of the Impossible Colouring Game

We have presented a infinite family of pseudo-telepathy games based on the Kochen-Specker theorem. It is interesting to mention the particular case where $m = 3$ (table 4.2). For the quantum strategy, Alice and Bob share an entangled *qutrit* pair $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$. This is interesting as this entangled state of dimension 9 is the smallest known state used for a two-party pseudo-telepathy game. In fact, we know for sure that this is the smallest possible state for a two-party pseudo-telepathy game [BMT04].

Impossible colouring game ($m = 3$)	
n	2
X	Let K_3 be an augmented Kochen-Specker construction of dimension 3. $X_1 = \{(v_i, v_j, v_k) \mid (v_i, v_j, v_k)$ are orthonormal triples in $K_3\}$ $X_2 = \{v_\ell \mid v_\ell \in K_3\}$
Y	$Y_1 = \{1, 2, 3\}$, $Y_2 = \{0, 1\}$
P	$v_\ell \in \{v_i, v_j, v_k\}$
W	$y_1 = \ell \Leftrightarrow y_2 = 1$
$\widetilde{\omega}_c$	< 1
ω_c	< 1
$\|\psi\rangle$	$\frac{1}{\sqrt{3}}(\|00\rangle + \|11\rangle + \|22\rangle)$

Table 4.2: Impossible colouring game ($m = 3$)

4.2 The Distributed Deutsch-Jozsa Game

This pseudo-telepathy game, based on the Deutsch-Jozsa problem [DJ92], was first presented in [BCT99]. The game uses a parameter k, which determines the size of the game. The task that Alice and Bob face is the following (see table 4.3, which makes use of definition 4.2.1): they each receive an input bit string of length 2^k, with the promise that either their inputs are identical, or they differ in exactly half of the positions. They must each output a bit string of length k, such that their outputs are identical if and only if their inputs are identical. Originally, there was only an *asymptotic* bound known on the amount of communication required for classical players to have a winning strategy; thus we could not say for sure which values of k give rise to a pseudo-telepathy game. A few years later, an analysis showed that for $k = 4$, this game is a pseudo-telepathy game (see section 4.2.2).

Definition 4.2.1. The *Hamming Weight* of a binary string $x = x_1x_2 \ldots x_n \in \{0,1\}^n$ is denoted $\Delta(x)$ and defined as:

$$\Delta(x) = \sum_{i=1}^{n} x_i.$$

As a consequence, we have that $0 \leq \Delta(x) \leq n$.

4.2.1 A Quantum Winning Strategy

Theorem 4.2.1. *Let G^k be the distributed Deutsch-Jozsa game. Then $\omega_q(G^k) = 1$.*

Proof. The player's strategy is to share the state $|\psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |jj\rangle$. After receiving his input $x_i = x_i^0 x_i^1 \ldots x_i^{2^k-1}$, each player i does the following:

1. apply the unitary transformation S_i given by

$$S_i(|j\rangle) = (-1)^{x_i^j} |j\rangle$$

2. apply H to each qubit

3. measure the qubits to obtain $y_i = y_i^0 y_i^1 \ldots y_i^{k-1}$

4. output y_i

To show that this quantum strategy works, we first state and prove a lemma.

Distributed Deutsch-Jozsa game	
n	2
X	$X_1 = X_2 = \{0,1\}^{2^k}$
Y	$Y_1 = Y_2 = \{0,1\}^k$
P	$x_1 = x_2$ or $\Delta(x_1, x_2) = 2^{k-1}$
W	$y_1 = y_2 \Leftrightarrow x_1 = x_2$
$\widetilde{\omega}_c$	$\widetilde{\omega}_c = 1$ $(k = 1,2,3)$, $\widetilde{\omega}_c < 1$ ($k = 4$ and for all sufficiently large m)
ω_c	$\omega_c = 1$ $(k = 1,2,3)$, $\omega_c < 1$ ($k = 4$ and for all sufficiently large m)
$\|\psi\rangle$	$\frac{1}{\sqrt{2^k}} \sum_{i=0}^{2^k-1} \|jj\rangle$

Table 4.3: Distributed Deutsch-Jozsa game

Lemma 4.2.2. *Let $|x\rangle$ be a basis state of n qubits. Then*

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x \cdot z}|z\rangle}{\sqrt{2^n}}, \tag{4.7}$$

where $x \cdot z$ is the bitwise inner product of x and z, modulo 2, and the sum is over all $z \in \{0,1\}^n$.

Proof. For a single qubit, we have $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and so for $|x\rangle$ a single qubit,

$$H|x\rangle = \frac{\sum_z (-1)^{x \cdot z}|z\rangle}{\sqrt{2}}$$

By linearity, for $|x\rangle = |x_1 \dots x_n\rangle$ a basis state,

$$H^{\otimes n}|x_1 \dots x_n\rangle = \frac{\sum_{z_1,\dots,z_n} (-1)^{x_1 \cdot z_1 + \dots + x_n \cdot z_n}|z_1 \dots z_n\rangle}{\sqrt{2^n}},$$

which can be summarized by

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x \cdot z} |z\rangle}{\sqrt{2^n}}.$$

□

Now, consider the resulting state after step 1 of the quantum strategy:

$$|\psi\rangle = \sum_{j=0}^{2^k-1} \frac{1}{\sqrt{2^k}} (-1)^{x_1^j + x_2^j} |jj\rangle$$

In step 2, both players apply H. By lemma 4.2.2, if $|j\rangle$ is a basis state of k qubits:

$$H^{\otimes k}|j\rangle = \frac{1}{\sqrt{2^k}} \sum_{\ell=0}^{2^k-1} (-1)^{j \cdot \ell} |\ell\rangle \tag{4.8}$$

where $\ell \cdot j$ is the bitwise inner product of ℓ and j, modulo 2. So,

$$\begin{aligned} H^{\otimes 2k}|\psi\rangle &= \sum_{j=0}^{2^k-1} \frac{1}{\sqrt{2^k}} (-1)^{x_1^j + x_2^j} \left(\frac{1}{\sqrt{2^k}} \sum_{u=0}^{2^k-1} (-1)^{j \cdot u} |u\rangle \right) \left(\frac{1}{\sqrt{2^k}} \sum_{v=0}^{2^k-1} (-1)^{j \cdot v} |v\rangle \right) \\ &= \frac{1}{2^{\frac{3k}{2}}} \sum_{u=0}^{2^k-1} \sum_{v=0}^{2^k-1} \left(\sum_{j=0}^{2^k-1} (-1)^{x_1^j + x_2^j + j \cdot u + j \cdot v} \right) |u\rangle |v\rangle \end{aligned}$$

The amplitude α of $|u\rangle|v\rangle$ in $H^{\otimes 2^k}|\psi\rangle$ determines the probability that $y_1 = u$ and $y_2 = v$. From here, we have two cases:

- $x_1 = x_2$. Suppose that $u \neq v$. The amplitude α of $|u\rangle|v\rangle$ in $H^{\otimes 2^k}|\psi\rangle$ is:

$$\begin{aligned} \alpha &= \frac{1}{2^{\frac{3k}{2}}} \sum_{j=0}^{2^k-1} (-1)^{x_1^j + x_2^j + j \cdot u + j \cdot v} \\ &= \frac{1}{2^{\frac{3k}{2}}} \sum_{j=0}^{2^k-1} (-1)^{j \cdot u + j \cdot v} \\ &= 0 \end{aligned}$$

Where the last line follows by the following argument: we know that $j \cdot u + j \cdot v \equiv j \cdot u \oplus j \cdot v \pmod 2$ and that $j \cdot u \oplus j \cdot v = j \cdot (u \oplus v)$. Since $u \neq v$, we have that $u \oplus v \neq 0$. Therefore, $j \cdot (u \oplus v) \equiv 0 \pmod 2$ for exactly half the values of j and $j \cdot (u \oplus v) \equiv 1 \pmod 2$ for the other half of the values of j.

Hence the winning condition is always satisfied if $x_1 = x_2$.

- $\Delta(x_1, x_2) = \frac{1}{2}$: Suppose that $u = v$. The amplitude α of $|u\rangle|v\rangle$ in $H^{\otimes 2^k}|\psi\rangle$ is:

$$\begin{aligned}\alpha &= \frac{1}{2^{\frac{3k}{2}}} \sum_{j=0}^{2^k-1} (-1)^{x_1^j + x_2^j + j \cdot u + j \cdot v} \\ &= \frac{1}{2^{\frac{3k}{2}}} \sum_{j=0}^{2^k-1} (-1)^{x_1^j + x_2^j} \\ &= 0\end{aligned}$$

Since $\Delta(x_1, x_2) = 2^{k-1}$ implies that $x_1^j + x_2^j \equiv 0 \pmod 2$ for half values of j and $x_1^j + x_2^j \equiv 1 \pmod 2$ for the other half of the values of j.

Hence the winning condition is always satisfied if $\Delta(x_1, x_2) = 2^{k-1}$.

□

4.2.2 Classical Success Proportion

The following theorem states that if the parameter k is chosen large enough, this game cannot be won with certainty by classical players. It appeared in a slightly different context in [BCW98].

Theorem 4.2.3. *Let G^k be the distributed Deutsch-Jozsa game. Then the amount of communication required for classical players to win the game is in $\Omega(2^k)$.*

But this theorem doesn't help if we want to know which values of k yield a pseudo-telepathy game. Originally, the authors of [BCT99] knew that the game had a classical winning strategy for $k = 1, 2$. They conjectured that this was not the case for $k = 3$. However, in [GW02], the authors prove that there is a classical winning strategy for $k = 3$, hence the following theorem:

Theorem 4.2.4. *Let G^k be the distributed Deutsch-Jozsa game. Then $\widetilde{\omega}_c(G^k) = 1$ if $k \in \{1, 2, 3\}$.*

Then, the idea was to show that for $k = 4$, there was no possibility of a classical winning strategy. By using an argument based on graph theory, as well as a computer-assisted case analysis, it was finally shown in [GWT03] that for $k = 4$, there is no classical winning strategy:

Theorem 4.2.5. *Let G^k be the distributed Deutsch-Jozsa game. Then $\widetilde{\omega}_c(G^k) < 1$ if $k = 4$.*

So we know that for $k = 4$, the distributed Deutsch-Jozsa game is a pseudo-telepathy game. By theorem 4.2.3, we also know that if we choose k larger than a certain threshold k_0, then we have a pseudo-telepathy game. However, it is an open question to determine the value of k_0. In particular, we don't even know if $k = 5$ yields a pseudo-telepathy game!

4.3 The Magic Square Game

The magic square game was presented by Aravind [Ara02, Ara03], who built on work by Mermin [Mer90d]. The game is also presented in [CHTW04].

A *magic square* is a 3×3 binary array that has the property that the sum of each row is even and the sum of each column is odd. Such a square is magic since it cannot exist: suppose we calculate the parity of the nine entries. According to the rows, the parity is even, yet according to the columns, the parity is odd, which is a contradiction.

The task that the players face while playing the game is the following: Alice is asked to give the entries of a row and Bob is asked to give the entries of a column. The winning condition is that the parity of the row must be even, the parity of the column must be odd, and the intersection of the given row and column must agree. Because a classical strategy would have to assign nine entries to a magic square, which is impossible, we know right away that there is no classical winning strategy. The game is described in table 4.4, where $y_1 = r_1r_2r_3$ (r is used for rows) and $y_2 = c_1c_2c_3$ (c is used for columns). It is interesting to note that this game is promise-free according to definition 3.2.5.

Magic square game	
n	2
X	$X_1 = \{1,2,3\}$, $X_2 = \{1,2,3\}$
Y	$Y_1 = Y_2 = \{0,1\}^3$
P	none
W	$\sum_{i=1}^{3} r_i \equiv 0 \pmod 2$, $\sum_{i=1}^{3} c_i \equiv 1 \pmod 2$ $r_{x_2} = c_{x_1}$
$\widetilde{\omega}_c$	$\frac{8}{9}$
ω_c	$\frac{8}{9}$
$\lvert\psi\rangle$	$\frac{1}{2}(\lvert 0011\rangle - \lvert 0110\rangle - \lvert 1001\rangle + \lvert 1100\rangle)$

Table 4.4: Magic square game

4.3.1 A Quantum Winning Strategy

Theorem 4.3.1. *Let G be the magic square game. Then $\omega_q(G) = 1$.*

Proof. The players share the state $|\psi\rangle = \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle)$. After receiving their inputs (x_1 for Alice, x_2 for Bob, the players do the following:

1. Alice performs the unitary transformation given by the matrix A_{x_1} (where $\imath$ denotes $\sqrt{-1}$):

$$A_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} \imath & 0 & 0 & 1 \\ 0 & -\imath & 1 & 0 \\ 0 & \imath & 1 & 0 \\ 1 & 0 & 0 & \imath \end{bmatrix}, \quad A_2 = \frac{1}{2}\begin{bmatrix} \imath & 1 & 1 & \imath \\ -\imath & 1 & -1 & \imath \\ \imath & 1 & -1 & -\imath \\ -\imath & 1 & 1 & -\imath \end{bmatrix}, \quad A_3 = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}$$

2. Bob performs the unitary transformation given by the matrix B_{x_2}:

$$B_1 = \frac{1}{2}\begin{bmatrix} \imath & -\imath & 1 & 1 \\ -\imath & -\imath & 1 & -1 \\ 1 & 1 & -\imath & \imath \\ -\imath & \imath & 1 & 1 \end{bmatrix}, \quad B_2 = \frac{1}{2}\begin{bmatrix} -1 & \imath & 1 & \imath \\ 1 & \imath & 1 & -\imath \\ 1 & -\imath & 1 & \imath \\ -1 & -\imath & 1 & -\imath \end{bmatrix}, \quad B_3 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

3. Alice and Bob measure their system. The result of the measurement gives the first two bits of the output, r_1r_2 for Alice and c_1c_2 for Bob. The third output bit is calculated so that the sum of each row is even and the sum of each column is odd. Hence $r_3 = r_1 + r_2 \pmod 2$ and $c_3 = c_1 + c_2 + 1 \pmod 2$.

To show that this strategy works, we consider nine cases that correspond to the possible questions $x = x_1, x_2$. In each case, we show that the player's final answer satisfies the winning condition. Because of step 3, we know that the row and column parity conditions are satisfied. After some tedious calculations that we omit here, we are able to show that indeed $r_{x_2} = c_{x_1}$ in all nine cases. □

The reader might wonder where the unitary transformations A_1, A_2, A_3, B_1, B_2 and B_3 come from. The answer is that they come from a 3×3 array of *observables* (table 4.5), each observable defining a measurement.

$\sigma_x \otimes \sigma_y$	$\sigma_y \otimes \sigma_x$	$\sigma_z \otimes \sigma_z$
$\sigma_y \otimes \sigma_z$	$\sigma_z \otimes \sigma_y$	$\sigma_x \otimes \sigma_x$
$\sigma_z \otimes \sigma_x$	$\sigma_x \otimes \sigma_z$	$\sigma_y \otimes \sigma_y$

Table 4.5: A 3×3 array of observables

Here, σ_x, σ_y, σ_z denote the Pauli matrices:

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

The measurement outcome for each observable is 0 or 1. The operators in each row and in each column commute pairwise, which means that they can be measured simultaneously, the result being a three-bit string. Since the product along any row is $I \otimes I$, the outcome for any row is even, and since the product along any column is $-I \otimes I$, the outcome for any column is odd.

In order to show that the intersection of Alice's and Bob's answers agree, we first note that the shared entangled state can be re-written as $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, where Alice has the first and third bit, and Bob the second and fourth bit. It is easy to check that the state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ has the property that $(\sigma_i \otimes \sigma_i)|\Psi^-\rangle = -|\Psi^-\rangle$, for any $i \in \{x, y, z\}$. Thus, using superscripts to identify the player's operator,

$$(\sigma_i^A \otimes \sigma_i^B) \otimes (\sigma_j^A \otimes \sigma_j^B)|\Psi^-\rangle \otimes |\Psi^-\rangle = |\Psi^-\rangle \otimes |\Psi^-\rangle. \tag{4.9}$$

So, if Alice and Bob perform an identical measurement corresponding to an entry in table 4.5 on the state $|\psi\rangle = |\Psi^-\rangle \otimes |\Psi^-\rangle$, their outcomes will agree.

Therefore, the quantum strategy is that Alice and Bob share the state $|\psi\rangle$. Alice performs three measurements on her part of the system, corresponding to row x_1 in table 4.5, and Bob performs three measurements, corresponding to column x_2.

The matrices A_1, A_2, A_3, B_1, B_2 and B_3, given in the previous quantum strategy come from table 4.5. We obtained them by simultaneous diagonalization of the rows (A_1, A_2, A_3) and columns (B_1, B_2, B_3) of the table.

4.3.2 Classical Success Proportion

Theorem 4.3.2. *Let G be the magic square game. Then $\widetilde{\omega}_c(G) < 1$.*

Proof. A deterministic strategy assigns values $\{0, 1\}$ to entries of a 3×3 array. Alice answers according to the required row and Bob answers according to the required column. Because of the winning conditions (the sum of the row is even, the sum of the column is even and the intersection of both answers agree), such a strategy would have to correspond to a magic square. No such magic square exists, so $\widetilde{\omega}_c(G) < 1$. □

Theorem 4.3.3. *Let G be the magic square game. Then $\widetilde{\omega}_c(G) = \frac{8}{9}$.*

Proof. By theorem 4.3.2, there is no classical winning strategy. Combining this with lemma 3.2.3, we get that $\widetilde{\omega}_c(G) \leq \frac{8}{9}$. We give a strategy that succeeds on all but one question, say $x_1 = 3$, $x_2 = 3$: Alice answers according to table 4.6, and Bob answers according to table 4.7.

0	0	0
0	0	0
1	1	0

Table 4.6: Alice's strategy

0	0	0
0	0	0
1	1	1

Table 4.7: Bob's strategy

Then the players win on all but one question ($x_1 = 3$, $x_2 = 3$), so $\widetilde{\omega}_c(G) = \frac{8}{9}$. □

Theorem 4.3.4. *Let G be the magic square game. Then $\omega_c(G) = \frac{8}{9}$.*

Proof. We know from the previous theorem and by theorem 3.2.2 that $\omega_c(G) \leq \frac{8}{9}$. Consider a set of nine deterministic strategies $s_{i,j}$ ($i = 1, 2, 3$ $j = 1, 2, 3$) that succeed on all but one question, $x_1 = i$, $x_2 = j$. These strategies can be constructed as in the proof of the previous theorem.

Suppose Alice and Bob use the probabilistic strategy which consists of selecting uniformly at random a strategy $s_{i,j}$. Then for each question, the probability of winning is $\frac{8}{9}$, and so $\omega_c(G) = \frac{8}{9}$. □

4.4 Cabello's Game

Cabello's game (table 4.8) is presented in [Cab01a] and [Cab01b]. Here, we have substantially changed the original notation so as to simplify the presentation. We suppose that, on input $x_1 \in \{1, 2, 3\}$, Alice outputs two bits, $y_1 = a_1 a_2$, and that on input $x_2 \in \{1, 2, 3\}$, Bob outputs two bits, $y_2 = b_1 b_2$.

Cabello's game resembles the magic square game (section 4.3) in many ways: both are promise-free, both have the same input size, the same output size, and even the same entangled state used for the quantum winning strategy. This suspicious resemblance is not a coincidence, since it turns out that the games are *equivalent*, which is the topic of section 4.5.

Cabello's game	
n	2
X	$X_1 = \{1,2,3\}$, $X_2 = \{1,2,3\}$
Y	$Y_1 = Y_2 = \{0,1\}^2$
P	none
W	given in table 4.9
$\widetilde{\omega}_c$	$\frac{8}{9}$
ω_c	$\frac{8}{9}$
$\|\psi\rangle$	$\frac{1}{2}(\|0011\rangle - \|0110\rangle - \|1001\rangle + \|1100\rangle)$

Table 4.8: Cabello's game

x_1	x_2	winning condition
1	1	$a_1 + b_1 \equiv 1$
1	2	$a_2 + b_1 \equiv 1$
1	3	$a_1 + a_2 + b_1 \equiv 0$
2	1	$a_1 + b_2 \equiv 1$
2	2	$a_2 + b_2 \equiv 1$
2	3	$a_1 + a_2 + b_2 \equiv 0$
3	1	$a_1 + b_1 + b_2 \equiv 0$
3	2	$a_2 + b_1 + b_2 \equiv 0$
3	3	$a_1 + a_2 + b_1 + b_2 \equiv 1$

Table 4.9: Winning conditions for Cabello's game

4.4.1 A Quantum Winning Strategy

Theorem 4.4.1. *Let G be Cabello's game. Then $\omega_q(G) = 1$.*

Proof. Let G' be the magic square game. In theorem 4.5.6, we will show that G is equivalent to G'. By theorem 4.3.1, $\omega_q(G') = 1$. By lemma 4.5.5, this implies that $\omega_q(G) = 1$. □

4.4.2 Classical Success Proportion

Theorem 4.4.2. *Let G be Cabello's game. Then $\widetilde{\omega}_c(G) < 1$.*

Proof. To prove this result, we use the fact that by theorem 4.5.6, this game is equivalent to the magic square game, G'. By theorem 4.3.2, $\widetilde{\omega}_c(G') < 1$, hence, by lemma 4.5.3, $\widetilde{\omega}_c(G) < 1$. □

Theorem 4.4.3. *Let G be Cabello's game. Then $\widetilde{\omega}_c(G) = \frac{8}{9}$.*

Proof. Let G' be the magic square game. By theorem 4.3.3, $\widetilde{\omega}_c(G') = \frac{8}{9}$ and since G and G' are equivalent (theorem 4.5.6), lemma 4.5.3 gives us that $\widetilde{\omega}_c(G) = \frac{8}{9}$. □

Theorem 4.4.4. *Let G be Cabello's game. Then $\omega_c(G) = \frac{8}{9}$.*

Proof. Let G' be the magic square game. By theorem 4.3.4, $\omega_c(G') = \frac{8}{9}$ and since G and G' are equivalent (theorem 4.5.6), lemma 4.5.4 gives us that $\omega_c(G) = \frac{8}{9}$. □

4.5 The Magic Square and Cabello's Games Are Equivalent

As mentioned in section 4.4, the magic square and Cabello's game are suspiciously similar. In fact, they are equivalent. This fact is known by Cabello [Cab04]; but it doesn't seem to have appeared in print. In this section, we formally show that the games are equivalent.

First, we must define what we mean when we say that two games are equivalent. For our purposes, the following definition is sufficient:

Definition 4.5.1. Let $G = (X, Y, P, W)$ and $G' = (X', Y', P', W')$, be two player games with $X = X_1 \times X_2$, $Y = Y_1 \times Y_2$, $X' = X_1' \times X_2'$, and $Y' = Y_1' \times Y_2'$. We say that G and G' are *equivalent* if there exist bijections $\sigma_A : X_1 \rightarrow X_1'$ and

$\sigma_B : X_2 \to X_2'$ as well as bijections $\delta_A : Y_1 \to Y_1'$ and $\delta_B : Y_2 \to Y_2'$ such that for all $x_1, x_2 \in X$ and $y_1, y_2 \in Y$, $x_1, x_2 \in P \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2)) \in P'$ and

$$(x_1, x_2, y_1, y_2) \in W \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2), \delta_A(y_1), \delta_B(y_2)) \in W'.$$

The following five lemmas justify the above definition by showing that the properties that we would expect to hold for two equivalent games are indeed true.

Lemma 4.5.1. *Let G and G' be equivalent two-player games. Then for each deterministic strategy s for G, there exists a deterministic strategy s' for G' such that s' has the the same success proportion as s.*

Proof. Let $\sigma_A, \sigma_B, \delta_A$ and δ_B be as in definition 4.5.1. Let s be a strategy for G and suppose that s succeeds in proportion p. Let s' be the following strategy for G': On input $x_1' \in X_1'$, Alice finds $x_1 = \sigma_A^{-1}(x_1')$. Let y_1 be Alice's output on input x_1 according to strategy s. Then in strategy s', Alice outputs $\delta_A(y_1)$. Bob uses a similar strategy for s'. Since

$$(x_1, x_2) \in P \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2)) \in P',$$

we know that $|P| = |P'|$. Furthermore, since

$$(x_1, x_2, y_1, y_2) \in W \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2), \delta_A(y_1), \delta_B(y_2)) \in W',$$

we conclude that strategies s and s' have the same success proportion. □

Given an arbitrary strategy s and a question x, let $\Pr_s(\text{win} \mid x)$ denote the probability that strategy s provides a winning answer on question x.

Lemma 4.5.2. *Let $G = (X, Y, P, W)$ and $G' = (X', Y', P', W')$ be equivalent two-player games. Let s be a probabilistic strategy for G. Then there exists a bijection $\tau : X \to X'$ and s' a probabilistic strategy for G' such that for all $x \in X$,*

$$\Pr_s(win \mid x) = \Pr_{s'}(win \mid \tau(x)).$$

Proof. Let $\sigma_A, \sigma_B, \delta_A$ and δ_B be as in definition 4.5.1.

Since s is a probabilistic strategy for G, it is a probability distribution over a finite set of deterministic strategies for G, say $\{s_1, s_2, \dots s_m\}$. Let $\Pr(s_i)$ be the probability that strategy s_i is chosen.

We can convert each deterministic strategy s_i for G, to a deterministic strategy s'_i for G', as in the proof of lemma 4.5.1. Using this, let s' be the strategy for G' which is a probability distribution over the set of deterministic strategies $\{s'_1, s'_2, \dots s'_m\}$ such that strategy s'_i is chosen with probability $\Pr(s_i)$.

Let $p_{s_i}(x)$ be 1 if strategy s_i yields a winning answer on question x and 0 otherwise.

We define the bijection τ on $x = x_1, x_2 \in X_1 \times X_2$, by $\tau(x) = \sigma_A(x_1), \sigma_B(x_2)$. Since

$$(x_1, x_2, y_1, y_2) \in W \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2), \delta_A(y_1), \delta_B(y_2)) \in W',$$

the deterministic strategy s_i wins on question $x \in X$ if and only if the deterministic strategy s'_i wins on question $\tau(x) \in X'$. In other words, $p_{s_i}(x) = p_{s'_i}(\tau(x))$. Therefore,

$$\begin{aligned}\Pr_s(\text{win} \mid x) &= \sum_{i=1}^{m} \Pr(s_i) p_{s_i}(x) \\ &= \sum_{i=1}^{m} \Pr(s_i) p_{s'_i}(\tau(x)) \\ &= \Pr_{s'}(\text{win} \mid \tau(x)).\end{aligned}$$

□

Lemma 4.5.3. *Let G and G' be equivalent two-player games. Then $\widetilde{\omega}_c(G) = \widetilde{\omega}_c(G')$.*

Proof. By lemma 4.5.1, $\widetilde{\omega}_c(G) \leq \widetilde{\omega}_c(G')$. By symmetry, $\widetilde{\omega}_c(G) \geq \widetilde{\omega}_c(G')$, hence $\widetilde{\omega}_c(G) = \widetilde{\omega}_c(G')$. □

Lemma 4.5.4. *Let G and G' be equivalent two-player games. Then $\omega_c(G) = \omega_c(G')$.*

Proof. By lemma 4.5.2, $\omega_c(G) \leq \omega_c(G')$. By symmetry, $\omega_c(G) \geq \omega_c(G')$, hence $\omega_c(G) = \omega_c(G')$.

□

Lemma 4.5.5. *Let G and G' be equivalent two-player games. Then $\omega_q(G) = \omega_q(G')$.*

Proof. By lemma 4.5.1, $\omega_q(G) \leq \omega_q(G')$. By symmetry, $\omega_q(G) \geq \omega_q(G')$, hence $\omega_q(G) = \omega_q(G')$. □

We now state and prove the main result:

Theorem 4.5.6. *The magic squares game and Cabello's game are equivalent.*

Proof. Let G be the magic square game and G' be Cabello's game. Consider the following bijections: $\sigma_A : X_1 \longrightarrow X_1'$ is the identity map and $\sigma_B : X_2 \longrightarrow X_2'$ is also the identity map. The maps $\delta_A : Y_1 \longrightarrow Y_1'$ and $\delta_B : Y_2 \longrightarrow Y_2'$ are given by the following:

$$\delta_A(r_1r_2r_3) = \overline{r_1r_2}$$
$$\delta_B(c_1c_2c_3) = c_1c_2.$$

Obviously, σ_A and σ_B are bijections. Also, δ_A and δ_B are bijections with inverse maps: $\delta_A^{-1}(a_1a_2) = r_1r_2r_3$ where

$$r_1 = \overline{a_1}$$
$$r_2 = \overline{a_2}$$
$$r_3 \equiv \overline{a_1} + \overline{a_2} \pmod 2$$

and $\delta_B^{-1}(b_1b_2) = c_1c_2c_3$ where

$$c_1 = b_1$$
$$c_2 = b_2$$
$$c_3 \equiv b_1 + b_2 + 1 \pmod 2.$$

All the questions satisfy the promise, so what remains to be shown is that for all $(x_1, x_2) \in X$ and $(y_1, y_2) \in Y$,

$$(x_1, x_2, y_1, y_2) \in W \Leftrightarrow (\sigma_A(x_1), \sigma_B(x_2), \delta_A(y_1), \delta_B(y_2)) \in W'.$$

Since $\sigma_A(x_1)$ and $\sigma_B(x_2)$ are the identity maps, all we need to show is that for any fixed question, y_1, y_2 is a winning answer for G if and only if $\delta_A(y_1), \delta_B(y_2)$ is a winning answer for G'. There are nine cases to check, corresponding to the nine possible questions that Alice and Bob receive. Note that for each question, there is exactly one condition in table 4.9 that must be satisfied. We can also transform the winning condition of the magic square game into equations. For example, if $x_1 = 1$ and $x_2 = 1$, the winning condition is that $r_1 = c_1$ and $r_1 + r_2 + r_3 \equiv 0 \pmod 2$ and $c_1 + c_2 + c_3 \equiv 1 \pmod 2$. A less obvious case is when $x_1 = 3$ and $x_2 = 3$. The parity condition states that:

$$r_1 + r_2 + r_3 \equiv 0 \pmod 2 \tag{4.10}$$

$$c_1 + c_2 + c_3 \equiv 1 \pmod 2. \tag{4.11}$$

Since we must have $c_3 = r_3$, substituting equations 4.10 and 4.11, we get that $c_1 + c_2 \equiv r_1 + r_2 + 1 \pmod 2$.

We summarize the possible questions as well as the winning conditions for both games in table 4.10, where the parity condition for the magic square game is implicit by the fact that r_3 and c_3 are replaced by $r_1 + r_2 \pmod 2$ and $c_1 + c_2 + 1 \pmod 2$, respectively.

Since $\delta_A(r_1r_2r_3) = \overline{r_1r_2}$ and $\delta_B(c_1c_2c_3) = c_1c_2$, it is easy to see that for a fixed question x_1, x_2,

$$(x_1, x_2, y_1, y_2) \in W \Leftrightarrow (x_1, x_2, \delta_A(y_1), \delta_B(y_2)) \in W'.$$

This completes the proof. □

question		winning condition	
x_1	x_2	magic square game	Cabello's game
1	1	$r_1 = c_1$	$a_1 + b_1 \equiv 1$
1	2	$r_2 = c_1$	$a_2 + b_1 \equiv 1$
1	3	$r_1 + r_2 \equiv c_1$	$a_1 + a_2 + b_1 \equiv 0$
2	1	$r_1 = c_2$	$a_1 + b_2 \equiv 1$
2	2	$r_2 = c_2$	$a_2 + b_2 \equiv 1$
2	3	$r_1 + r_2 \equiv c_2$	$a_1 + a_2 + b_2 \equiv 0$
3	1	$r_1 \equiv c_1 + c_2 + 1$	$a_1 + b_1 + b_2 \equiv 0$
3	2	$r_2 \equiv c_1 + c_2 + 1$	$a_2 + b_1 + b_2 \equiv 0$
3	3	$r_1 + r_2 \equiv c_1 + c_2 + 1$	$a_1 + a_2 + b_1 + b_2 \equiv 1$

Table 4.10: Winning conditions for the magic square and Cabello's game

4.6 The Matching Game

This game is the newest to be added to the family of pseudo-telepathy games. In fact, this is probably the first time that it appears in print. It is based on a talk given by Kerenidis at the Quantum Information Processing 2004 conference [BK04], and on [BYJK04].

Definition 4.6.1. A *perfect matching M* on $\{0, 1, \ldots, m-1\}$ (m even) is a partition of $\{0, 1, \ldots m-1\}$ into $\frac{m}{2}$ sets, each of size 2. We define M_m as the set of all perfect matchings on $\{0, 1, \ldots, m-1\}$.

The matching game is presented in table 4.11. Alice receives as input $x = x_1 x_2 \ldots x_m \in \{0,1\}^m$, and Bob receives a perfect matching $M \in M_m$. The task that the players face is for Alice to output a string $y_1 \in \{0,1\}^{\lceil \lg m \rceil}$ (lg is the base-two logarithm), and Bob to output a pair $\{a, b\} \in M$ as well as a string $y_2 \in \{0,1\}^{\lceil \lg m \rceil}$ such that:

$$x_a \oplus x_b = (a \oplus b) \cdot (y_1 \oplus y_2) \,,$$

where $(y_1 \oplus y_2)$ is the bit by bit exclusive or of y_1 and y_2, and $x \cdot a$ is the bitwise inner product, modulo 2. This game is promise-free according to definition 3.2.5.

The game scales with parameter m. For now, we are only able to say that there is no classical winning strategy if m is chosen large enough; we are currently investigating in order to find exactly which values of m yield a pseudo-telepathy game, more details are given in section 4.6.3.

Matching game	
n	2
X	$X_1 = \{0,1\}^m$ (m even) $X_2 = \{M \mid M \in M_m\}$
Y	$Y_1 = \{0,1\}^{\lceil \lg m \rceil}$ $Y_2 = \{\{a,b\} \mid \{a,b\} \in M\} \times \{0,1\}^{\lceil \lg m \rceil}$
P	none
W	$x_a \oplus x_b = (a \oplus b) \cdot (y_1 \oplus y_2)$
$\widetilde{\omega}_c$	< 1 for all sufficiently large m
ω_c	< 1 for all sufficiently large m
$\vert\psi\rangle$	$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \vert jj\rangle$

Table 4.11: Matching game

4.6.1 A Quantum Winning Strategy

Theorem 4.6.1. *Let G^m be the matching game. Then $\omega_q(G^m) = 1$.*

Proof. The player's strategy is to share the state $|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jj\rangle$. After Alice receives her input $x = x_1 x_2 \dots x_m$ and Bob his input $M \in M_m$, the players do the following:

1. Alice applies to her quantum register the unitary transformation that maps

$$|j\rangle \mapsto (-1)^{x_j} |j\rangle$$

for all j between 0 and $m-1$.

2. Bob performs a projective partial measurement onto subspaces of dimension 2. Each subspace of the measurement is spanned by vectors $|k\rangle$ and $|\ell\rangle$, where $\{k,\ell\} \in M$. Bob outputs the classical outcome of this measurement, which is a pair $\{a,b\} \in M$.

3. Both Alice and Bob perform the Hadamard transform $H^{\otimes \lceil \lg m \rceil}$

4. Alice measures in the computational basis and outputs a, the result of her measurement

5. Bob measures in the computational basis and outputs b, the result of his measurement

We now show that this quantum strategy always succeeds. After step 1, the state is:

$$|\psi_1\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} (-1)^{x_j} |jj\rangle.$$

Suppose that in step 2, Bob measures and outputs $\{a,b\} \in M$. The measurement causes the quantum state shared with Alice to collapse to $\frac{1}{\sqrt{2}}(-1)^{x_a}|aa\rangle + \frac{1}{\sqrt{2}}(-1)^{x_b}|bb\rangle$. In step 3, both players apply $H^{\otimes \lceil \lg m \rceil}$. Let the result be $|\psi_3\rangle$. By lemma 4.2.2:

$$\begin{aligned}
|\psi_3\rangle =&(-1)^{x_a}\frac{1}{8}\left(\sum_x (-1)^{x\cdot a}|x\rangle \sum_y (-1)^{y\cdot a}|y\rangle\right) + \\
&(-1)^{x_b}\frac{1}{8}\left(\sum_x (-1)^{x\cdot b}|x\rangle \sum_y (-1)^{y\cdot b}|y\rangle\right) \\
=&\frac{1}{8}\sum_{xy}(-1)^{x_a \oplus (x\oplus y)\cdot a}|x\rangle|y\rangle + \frac{1}{8}\sum_{xy}(-1)^{x_b \oplus (x\oplus y)\cdot b}|x\rangle|y\rangle \\
=&\frac{1}{8}\sum_{xy}\left((-1)^{x_a \oplus (x\oplus y)\cdot a} + (-1)^{x_b \oplus (x\oplus y)\cdot b}\right)|x\rangle|y\rangle.
\end{aligned}$$

Alice and Bob then measure (steps 4 and 5), and output their result, y_1 and y_2. We know that the winning condition is satisfied, since

$$x_a \oplus x_b \neq (a \oplus b) \cdot (x \oplus y)$$

implies that $x_a \oplus (x \oplus y) \cdot a \neq x_b \oplus (x \oplus y) \cdot b$, so the outcome $y_1 = x$, $y_2 = y$ has zero probability of being observed, hence the outcomes will always satisfy the winning condition. □

4.6.2 The Hidden Matching Problem

The above game is inspired by a *one-way communication problem* called the *hidden matching problem* [BYJK04] defined as the following:

1. Alice receives as input a string $x \in \{0,1\}^m$.

2. Bob receives a perfect matching $M \in M_m$.

3. Alice sends a message to Bob.

4. Bob's goal is to output a tuple (a, b, c) such that $\{a, b\} \in M$ and $c = x_a \oplus x_b$.

In the hidden matching problem, if Alice is allowed to send quantum information (but not to share entanglement with Bob), then the quantum one-way communication complexity is in $O(\log m)$, yet any randomized one-way protocol with bounded error must use $\Omega(\sqrt{m})$ bits of communication. This last result is useful in the next section.

4.6.3 Classical Success Proportion

Theorem 4.6.2. *Let G^m be the matching game. Then $\widetilde{\omega}_c(G^m) < 1$ provided m is chosen large enough.*

Proof. Suppose that Alice and Bob have a winning classical strategy for the matching game. So Alice is able to find a y_1 and Bob is able to find $\{a, b\} \in M$ and y_2 such that:

$$x_a \oplus x_b = (a \oplus b) \cdot (y_1 \oplus y_2)$$

If we allow one-way communication (i.e. we allow Alice to send a message to Bob), then if Alice sends y_1 (a $\lceil \lg m \rceil$ bit message) to Bob, he can calculate

$$(a \oplus b) \cdot (y_1 \oplus y_2) = x_a \oplus x_b$$

This tells him which value of $c = x_a \oplus x_b$ to output in his tuple (a, b, c). Hence, Alice and Bob always succeed at the hidden matching problem with $\lceil \lg m \rceil$ bits of communication. However, we know from [BYJK04], that any randomized protocol with bounded error for the hidden matching problem must use $\Omega(\sqrt{m})$ bits of communication; hence if m is chosen large enough, it is impossible for Alice and Bob to always succeed at the hidden matching problem with $\lg m$ bits of communication, and so $\widetilde{\omega}_c(G^m) < 1$ for large enough values of m. □

Of course, the above theorem does not tell us exactly which values of m yield a pseudo-telepathy game G^m. If $m = 2$, there is an obvious classical winning strategy. We conjecture that for any other even m, there is no winning strategy:

Conjecture 4.6.3. Let G^m be the matching game. Then for all even $m \geq 4$, $\widetilde{\omega}_c(G^m) < 1$.

The apparent difficulty for classical players in the matching game leads us to believe that $\widetilde{\omega}_c(G^m)$ goes quickly towards $\frac{1}{2}$ as m increases. It is therefore possible that this game satisfies the following open problem:

> it would be nice to find a *two*-party pseudo-telepathy problem that admits a perfect quantum solution, yet any classical protocol would have a small probability of success [3] even for inputs of small or moderate size. [BBT03]

[3] In this context, "small probability of success" means a small advantage compared to random outputs.

CHAPTER 5

MULTI-PARTY GAMES

In this chapter, we present three pseudo-telepathy games with three or more players. It so happens that the first game is a special case of the second game, which, in turn, is a special case of the third game. Historically, however, these games appeared separately; it is probably more instructive to present them as we do here, as separate games.

5.1 The Mermin-GHZ Three-Party Game

This pseudo-telepathy game is probably the most famous as its discovery surprised many researchers as it did Mermin (section 3.3). Contrary to conventional wisdom, it is not the first pseudo-telepathy game, since Heywood and Redhead had suggested using the Kochen-Specker theorem to create a pseudo-telepathy game (section 4.1) more than 5 years before.

The original version was given in [GHZ88], and presented as a four-player game (although it was noted that a three player game would be possible). Later, the game was presented as a three-player version in [GHSZ90]. Non-trivial decoding of the two previous references allowed Mermin to popularize the game [Mer90c, Mer90e]. From Mermin's work, it is relatively straightforward to deduce a pseudo-telepathy game.

The game (table 5.1) is very simple. Each player receives as input a single bit x_i $(i = 1, 2, 3)$. The promise guarantees that $x_1 + x_2 + x_3$ is even. Each player outputs a single bit y_i, and the winning condition is that the *parity* of $y_1 + y_2 + y_3$ must equal the parity of $\frac{x_1+x_2+x_3}{2}$.

Mermin-GHZ game	
n	$n = 3$
X	$X_i = \{0, 1\}$ $(i = 1, 2, 3)$
Y	$Y_i = \{0, 1\}$ $(i = 1, 2, 3)$
P	$\sum_i^3 x_i \equiv 0 \pmod 2$
W	$\sum_i^3 y_i \equiv \frac{\sum_i^3 x_i}{2} \pmod 2$
$\widetilde{\omega}_c$	$\frac{3}{4}$
ω_c	$\frac{3}{4}$
$\lvert\psi\rangle$	$\frac{1}{\sqrt{2}}(\lvert 000\rangle + \lvert 111\rangle)$

Table 5.1: Mermin-GHZ game

5.1.1 A Quantum Winning Strategy

Before presenting the quantum winning strategy, we present a lemma that is useful for demonstrating the validity of the strategy. The lemma is more general than necessary here, this is because we will use the result in sections 5.2 and 5.3.

We denote S to be the unitary transformation given by:

$$S|0\rangle = |0\rangle$$
$$S|1\rangle = \imath|1\rangle.$$

Lemma 5.1.1. *Let* $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$ *and* $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$. *Let* S_m *represent the unitary transformation obtained by applying* S *to any* m *qubits and leaving the rest undisturbed. Then*

$$S_m|\Phi^+\rangle = \begin{cases} |\Phi^+\rangle & , m \equiv 0 \pmod 4 \\ |\Phi^-\rangle & , m \equiv 2 \pmod 4, \end{cases} \tag{5.1}$$

and

$$(H^{\otimes n})|\Phi^+\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(x)\equiv 0 \\ (\text{mod } 2)}} |x\rangle \tag{5.2}$$

$$(H^{\otimes n})|\Phi^-\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(x)\equiv 1 \\ (\text{mod } 2)}} |x\rangle. \tag{5.3}$$

Proof. It is easy to see that equation 5.1 holds. To show equation 5.2, we apply lemma 4.2.2 to get the following:

$$\begin{aligned}
(H^{\otimes n})\tfrac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle) &= \tfrac{1}{\sqrt{2}}((H^{\otimes n})|0^n\rangle + (H^{\otimes n})|1^n\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\frac{\sum_x (-1)^{0\ldots0\cdot x}|x\rangle}{\sqrt{2^n}} + \frac{\sum_x (-1)^{1\ldots1\cdot x}|x\rangle}{\sqrt{2^n}}\right) \\
&= \frac{1}{\sqrt{2}}\left(\frac{\sum_x |x\rangle}{\sqrt{2^n}} + \frac{\sum_x (-1)^{\Delta(x)}|x\rangle}{\sqrt{2^n}}\right) \\
&= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_x 1 + (-1)^{\Delta(x)}\right)|x\rangle \\
&= \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(x)\equiv 0 \\ (\text{mod } 2)}} |x\rangle.
\end{aligned}$$

A similar reasoning is used to show equation 5.3. □

Theorem 5.1.2. *Let G_n be the Mermin-GHZ game. Then $\omega_q(G_n) = 1$.*

Proof. The player's strategy is to share the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. After receiving his input x_i, each player i does the following:

1. if $x_i = 1$, apply the unitary transformation S
2. apply H
3. measure the qubit to obtain y_i
4. output y_i

The resulting state after step 1 is:

$$
\begin{aligned}
|\psi\rangle &= \tfrac{1}{\sqrt{2}}\left(|000\rangle + \imath^{\sum_{i=1}^{3} x_i}|111\rangle\right) \\
&= \begin{cases} \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) & , \sum_{i=1}^{3} x_i = 0 \\ \tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle) & , \sum_{i=1}^{3} x_i = 2 \end{cases}
\end{aligned}
$$

By lemma 5.1.1, the resulting state after step 2 is:

$$
\begin{aligned}
&\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle), \sum_{i=1}^{3} x_i = 0 \\
&\frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle), \sum_{i=1}^{3} x_i = 2
\end{aligned}
$$

And so after the measurement at step 3, the output of step 4 will satisfy:

$$
\sum_{i=1}^{3} y_i \equiv \frac{\sum_{i=1}^{3} x_i}{2} \pmod 2
$$

so the players always win. □

5.1.2 Classical Success Proportion

Theorem 5.1.3. *Let G_n be the Mermin-GHZ game. Then $\widetilde{\omega}_c(G_n) < 1$.*

To prove this theorem, we could try all deterministic classical strategies, as there are only 4^3 such strategies, but here we give a more elegant proof.

Proof. We represent the set P of questions satisfying the promise in the following way:

$$
\begin{array}{ccccccc}
x^1 & = & x_1^1, & x_2^1, & x_3^1 & = & 0, \; 1, \; 1 \\
x^2 & = & x_1^2, & x_2^2, & x_3^2 & = & 1, \; 0, \; 1 \\
x^3 & = & x_1^3, & x_2^3, & x_3^3 & = & 1, \; 1, \; 0 \\
x^4 & = & x_1^4, & x_2^4, & x_3^4 & = & 0, \; 0, \; 0
\end{array}
\tag{5.4}
$$

Suppose that the players' answers for questions x^1, x^2, x^3, x^4 are y^1, y^2, y^3, y^4 respectively. Represent player i's output on input 0 by y_i^0 and his output on input 1 by y_i^1.

Consider how the players will answer for all four possible questions:

$$\begin{array}{rcl} y^1 & = & y_1^0,\ y_2^1,\ y_3^1 \\ y^2 & = & y_1^1,\ y_2^0,\ y_3^1 \\ y^3 & = & y_1^1,\ y_2^1,\ y_3^0 \\ y^4 & = & y_1^0,\ y_2^0,\ y_3^0 \end{array} \tag{5.5}$$

The winning condition W states that, in order for the players to win, we must have:

$$\Delta(y^1) \equiv \Delta(y^2) \equiv \Delta(y^3) \equiv 1 \pmod 2 \tag{5.6}$$

and

$$\Delta(y^4) \equiv 0 \pmod 2. \tag{5.7}$$

Suppose that the classical players have a winning strategy. If we add (modulo 2) the 12 bits of the right-hand side of equation 5.5, we must get 1 since equations 5.6 and 5.7 state that $\Delta(y^1)+\Delta(y^2)+\Delta(y^3)+\Delta(y^4) \equiv 1 \pmod 2$. But if we take the column-wise sum of the same elements, we get 0 since each element appears exactly twice. This is a contradiction, so $\widetilde{\omega}_c(G_n) < 1$. □

Theorem 5.1.4. *Let G_n be the Mermin-GHZ game. Then $\widetilde{\omega}_c(G_n) = \frac{3}{4}$.*

Proof. Thanks to theorem 5.1.3, we know that there is no classical winning strategy. By lemma 3.2.3, $\widetilde{\omega}_c(G_n) \le \frac{3}{4}$. The following strategy succeeds in proportion $\frac{3}{4}$: the players always give an odd answer, say $y^i = 0,0,1$ ($i = 1,2,3,4$). Then they win for questions $x_1 = 0,1,1$, $x_2 = 1,0,1$, $x_3 = 1,1,0$ and lose on question $x_4 = 0,0,0$. The success proportion is therefore $\widetilde{\omega}_c(G_n) = \frac{3}{4}$. □

Theorem 5.1.5. *Let G_n be the Mermin-GHZ game. Then $\omega_c(G_n) = \frac{3}{4}$.*

Proof. We know by theorems 5.1.4 and 3.2.2 that $\omega_c(G_n) \le \frac{3}{4}$. In the next section, we will consider a generalization of the Mermin-GHZ game to an n-player version. By considering the case $n = 3$ of theorem 5.2.6, we get that $\omega_c(G_n) = \frac{3}{4}$. □

5.2 The Parity Game

This game was presented for the first time in [Mer90b] and in [PRC91]. As these physics references were unknown to the authors, the same game was presented in [BBT03], but this time from a QIP point of view. As in the case of the Mermin-GHZ game, a certain amount of decoding is necessary to extract a pseudo-telepathy game from [Mer90b] or [PRC91].

The game is a generalization of the Mermin-GHZ game (section 5.1), as it extends the 3-player version to an n-player game. In this game (table 5.2), we have $n \geq 3$ players. Each player receives as input a single bit x_i. The promise guarantees that $\sum x_i$ is even. Each player outputs a single bit y_i, and the winning condition is that the *parity* of $\sum y_i$ must equal the parity of $\frac{\sum x_i}{2}$.

5.2.1 A Quantum Winning Strategy

Theorem 5.2.1. *Let G_n be the parity game. Then $\omega_q(G_n) = 1$.*

Proof. The player's strategy is to share the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$. After receiving his input x_i, each player i does the following:

1. if $x_i = 1$, apply the unitary transformation S from section 5.1.1
2. apply H
3. measure the qubit to obtain y_i
4. output y_i

Parity Game	
n	$n \geq 3$
X	$X_i = \{0,1\}$ $(i = 1 \dots n)$
Y	$Y_i = \{0,1\}$ $(i = 1 \dots n)$
P	$\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$
W	$\sum_{i=1}^{n} y_i \equiv \frac{\sum_{i=1}^{n} x_i}{2} \pmod 2$
ω_c	$\frac{1}{2} + 2^{-\lceil n/2 \rceil}$
$\widetilde{\omega}_c$	$\frac{1}{2} + 2^{-\lceil n/2 \rceil}$
p^*	$\frac{1}{2} + 2^{\frac{2-3n}{2n}}$ $(n$ even$)$; $\frac{1}{2} + 2^{\frac{1-3n}{2n}}$ $(n$ odd$)$
η^*	$\frac{1}{2}\sqrt[n]{4}$
$\lvert\psi\rangle$	$\frac{1}{\sqrt{2}}\left(\lvert 0^n\rangle + \lvert 1^n\rangle\right)$

Table 5.2: Parity game

The resulting state after step 1 is:

$$\begin{aligned}\lvert\psi\rangle &= \tfrac{1}{\sqrt{2}}\left(\lvert 0^n\rangle + \imath^{\sum_{i=1}^{n} x_i}\lvert 1^n\rangle\right)\\ &= \begin{cases} \tfrac{1}{\sqrt{2}}\left(\lvert 0^n\rangle + \lvert 1^n\rangle\right) & , \sum_{i=1}^{n} x_i \equiv 0 \pmod 4 \\ \tfrac{1}{\sqrt{2}}\left(\lvert 0^n\rangle - \lvert 1^n\rangle\right) & , \sum_{i=1}^{n} x_i \equiv 2 \pmod 4 \end{cases}\end{aligned}$$

By proposition 5.1.1, the resulting state after step 2 is:

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(y)\equiv 0 \\ (\text{mod } 2)}} |y\rangle \,, \sum_{i=1}^{n} x_i \equiv 0 \pmod 4$$
$$\frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(y)\equiv 1 \\ (\text{mod } 2)}} |y\rangle \,, \sum_{i=1}^{n} x_i \equiv 2 \pmod 4$$

After the measurement of step 4, the output of step 5 will satisfy:

$$\sum_{i}^{n} y_i \equiv \frac{\sum_{i=1}^{n} x_i}{2} \pmod 2$$

so the players always win.

□

5.2.2 Classical Success Proportion

It is easy to see that $\widetilde{\omega}_c(G_n) < 1$ for the parity game, since a classical deterministic winning strategy for the parity game would entail a classical deterministic winning strategy for the Mermin-GHZ game by the following argument: if there is a classical deterministic winning strategy for the parity game, then in particular, there is a deterministic winning strategy if $x_1, x_2, x_3 \in \{0, 1\}$ and $x_4, x_5, \ldots, x_n = 0$. This strategy, restricted to players 1, 2 and 3 (with player 3 possibly responding with $\overline{y_3}$ instead of y_3, to take into account the parity of $y_4, y_5, \ldots, y_n$) is a winning strategy for the Mermin-GHZ game.

The following theorem gives an exact value for $\widetilde{\omega}_c(G_n)$, and the proof also yields a set of strategies that succeed with this optimal proportion. In [Mer90b], an upper bound for $\widetilde{\omega}_c(G_n)$ is given. Here, we prove that the upper bound is tight.

Theorem 5.2.2. *Let G_n be the parity game. Then*

$$\widetilde{\omega}_c(G_n) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

To prove the result, we will show that for any deterministic strategy, the success proportion is $\leq \frac{1}{2} + 2^{-\lceil n/2 \rceil}$, and that we can reach this proportion. Hence $\widetilde{\omega}_c(G_n) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$. The rest of section 5.2.2 (including 5.2.2.1, 5.2.2.2 and 5.2.2.3) is dedicated to proving theorem 5.2.2.

Let S_d be the set of deterministic strategies. Since no information may be communicated during the game, the best the players can do is agree on a strategy before the game starts. Any such strategy will be such that player i's answer depends only on his input, x_i. Each player may have one of the following four strategies:

$$\begin{aligned} f_0 &: y_i = 0 \\ f_1 &: y_i = 1 \\ v_0 &: y_i = x_i \\ v_1 &: y_i = \overline{x}_i \end{aligned}$$

Here, $F = \{f_0, f_1\}$ is the set of *fixed* strategies (the output is independent of x_i), and $V = \{v_0, v_1\}$ is the set of *variable* strategies (the output depends on x_i).

This gives a way to represent a strategy as an ordered list $s = s_1, s_2, \ldots, s_n$ where $s_i \in V \cup F$, $(1 \leq i \leq n)$, is player i's strategy.

Without loss of generality, we may assume that the ℓ, $(0 \leq \ell \leq n)$ first players choose a strategy in F (this amounts to saying that *order* doesn't matter, which is indeed true if all we want to know is the winning proportion). So in fact we can write any strategy $s \in S_d$ as

$$s = \overbrace{s_1, s_2, \ldots, s_\ell}^{\in F}, \overbrace{s_{\ell+1}, s_{\ell+2}, \ldots, s_n}^{\in V}.$$

What's more, without loss of generality, we may suppose that the first $\ell - \alpha$ $(0 \leq \alpha \leq \ell)$ players have the strategy f_0, it follows that the following α players have the strategy f_1, and we suppose that the next $n - \ell - \beta$ $(0 \leq \beta \leq n - \ell)$

players have the strategy v_0, so the next β players have the strategy v_1:

$$s = \overbrace{f_0, f_0, \ldots, f_0}^{\ell-\alpha}, \overbrace{f_1, f_1, \ldots, f_1}^{\alpha}, \overbrace{v_0, v_0, \ldots, v_0}^{n-\ell-\beta}, \overbrace{v_1, v_1, \ldots, v_1}^{\beta}.$$

Since the winning proportion depends only on the parameters ℓ, α and β of the given strategy (again, because order doesn't matter), we may represent each strategy s as $s = (\ell, \alpha, \beta)$. We now examine the winning proportion, given such a strategy s.

Lemma 5.2.3. *Let $x = x_1, x_2, \ldots, x_n \in \{0,1\}^n$. Then*

$$\Delta(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) \equiv \begin{cases} \Delta(x_1, x_2, \ldots, x_n) \pmod 2 & , n \equiv 0 \pmod 2 \\ \Delta(x_1, x_2, \ldots, x_n) + 1 \pmod 2 & , n \equiv 1 \pmod 2 \end{cases}$$

Proof. The proof follows directly from the fact that

$$\Delta(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) + \Delta(x_1, x_2, \ldots, x_n) = n.$$

□

As defined in chapter 3, let P be the set of questions that satisfy the promise. For the parity game,

$$P = \{x \in \{0,1\}^n \mid \Delta(x) \equiv 0 \pmod 2\}. \tag{5.8}$$

The winning proportion p_s, for a given strategy $s = (\ell, \alpha, \beta)$, depends only on the number of questions $x = x_1, x_2, \ldots, x_n$ that yield a correct answer:

$$p_s = \frac{|\{x \in P \mid \text{strategy } s \text{ applied to } x \text{ yields a winning answer}\}|}{|P|}$$

We note that $|P| = 2^{n-1}$ (since there are the same amount of even and odd binary strings of length n), and we ask: how many $x \in P$ will yield a winning answer?

Consider a partition of P:

$$A_n = \{x \in P \mid \Delta(x) \equiv 0 \pmod 4\} = \{x \in P \mid \frac{\Delta(x)}{2} \equiv 0 \pmod 2\}$$
$$B_n = \{x \in P \mid \Delta(x) \equiv 2 \pmod 4\} = \{x \in P \mid \frac{\Delta(x)}{2} \equiv 1 \pmod 2\}$$

The participant's answer $y = y_1, y_2, \dots, y_n$ is a winning answer if and only if:

$$(x \in A_n \wedge \Delta(y) \equiv 0 \pmod 2) \vee (x \in B_n \wedge \Delta(y) \equiv 1 \pmod 2). \tag{5.9}$$

We introduce more notation:

$$A_n^{\ell,E} = \{x \in A_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 0 \pmod 2\}$$
$$A_n^{\ell,O} = \{x \in A_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 1 \pmod 2\}$$
$$B_n^{\ell,E} = \{x \in B_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 0 \pmod 2\}$$
$$B_n^{\ell,O} = \{x \in B_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 1 \pmod 2\}$$

Here, E stands for even and O stands for odd. Note that $A_n = A_n^{\ell,E} \cup A_n^{\ell,O}$ and that $B_n = B_n^{\ell,E} \cup B_n^{\ell,O}$. And of course, $P = A_n \cup B_n$.

This notation is useful because, given a strategy $s \in S_d$, and supposing that we know in which set, $A_n^{\ell,E}, A_n^{\ell,O}, B_n^{\ell,E}$ or $B_n^{\ell,O}$ the question $x \in P$ belongs, then we have sufficient information to determine whether or not the game is won. The next section explains how this is done.

5.2.2.1 Counting Winning Questions

Suppose $s = (\ell, \alpha, \beta) \in S_d$. Let $x \in P$ be the given question, and suppose y is the answer.

Working mod 2, and using lemma 5.2.3, we find that

$$\begin{aligned}
\Delta(y) &\equiv \Delta(y_1, y_2, \dots, y_{\ell-\alpha}) + \Delta(y_{\ell-\alpha+1}, y_{\ell-\alpha+1}, \dots, y_\ell) + \Delta(y_{\ell+1}, y_{\ell+2}, \dots, y_n) \\
&\equiv \Delta(\overbrace{0, 0, \dots, 0}^{\ell-\alpha}) + \Delta(\overbrace{1, 1, \dots, 1}^{\alpha}) + \Delta(y_{\ell+1}, y_{\ell+2}, \dots, y_n) \\
&\equiv \begin{cases} \Delta(y_\ell, y_{\ell+1}, \dots, y_n) & , \alpha \equiv 0 \pmod 2 \\ 1 + \Delta(y_\ell, y_{\ell+1}, \dots, y_n) & , \alpha \equiv 1 \pmod 2 \end{cases} \\
&\equiv \begin{cases} \Delta(y_{\ell+1}, y_{\ell+2}, \dots, y_{n-\beta}) + \Delta(y_{n-\beta+1}, y_{n-\beta+2}, \dots, y_n) & , \alpha \equiv 0 \pmod 2 \\ 1 + \Delta(y_{\ell+1}, y_{\ell+2}, \dots, y_{n-\beta}) + \Delta(y_{n-\beta+1}, y_{n-\beta+2}, \dots, y_n) & , \alpha \equiv 1 \pmod 2 \end{cases} \\
&\equiv \begin{cases} \Delta(x_{\ell_1}, x_{\ell+2}, \dots, x_{n-\beta}) + \Delta(\overline{x_{n-\beta+1}}, \overline{x_{n-\beta+2}}, \dots, \overline{x_n}) & , \alpha \equiv 0 \pmod 2 \\ 1 + \Delta(x_{\ell_1}, x_{\ell+2}, \dots, x_{n-\beta}) + \Delta(\overline{x_{n-\beta+1}}, \overline{x_{n-\beta+2}}, \dots, \overline{x_n}) & , \alpha \equiv 1 \pmod 2 \end{cases} \\
&\equiv \begin{cases} \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_{n-\beta}) + \Delta(x_{n-\beta+1}, x_{n-\beta+2}, \dots, x_n) & , \alpha + \beta \equiv 0 \pmod 2 \\ 1 + \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_{n-\beta}) + \Delta(x_{n-\beta+1}, x_{n-\beta+2}, \dots, x_n) & , \alpha + \beta \equiv 1 \pmod 2 \end{cases} \\
&\equiv \begin{cases} \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) & , \alpha + \beta \equiv 0 \pmod 2 \\ 1 + \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) & , \alpha + \beta \equiv 1 \pmod 2 \end{cases}
\end{aligned}$$

In order for the game to be won, equation 5.9 must be satisfied. We must have either:

$$\begin{aligned}
& x \in A_n \text{ and } \Delta(y) \equiv 0 \pmod 2 \\
\iff & \begin{cases} x \in A_n \text{ and } \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 0 \pmod 2 & , \alpha + \beta \equiv 0 \pmod 2 \\ x \in A_n \text{ and } \Delta(x_{\ell+1}, x_{\ell+2}, \dots, x_n) \equiv 1 \pmod 2 & , \alpha + \beta \equiv 1 \pmod 2 \end{cases} \\
\iff & \begin{cases} x \in A_n^{\ell,E} & , \alpha + \beta \equiv 0 \pmod 2 \\ x \in A_n^{\ell,O} & , \alpha + \beta \equiv 1 \pmod 2 \end{cases}
\end{aligned}$$

or

$$
\begin{aligned}
& x \in B_n \text{ and } \Delta(y) \equiv 1 \pmod 2 \\
\iff & \begin{cases} x \in B_n \text{ and } \Delta(x_{\ell+1}, x_{\ell+2}, \ldots, x_n) \equiv 1 \pmod 2 & , \alpha + \beta \equiv 0 \pmod 2 \\ x \in B_n \text{ and } \Delta(x_{\ell+1}, x_{\ell+2}, \ldots, x_n) \equiv 0 \pmod 2 & , \alpha + \beta \equiv 1 \pmod 2 \end{cases} \\
\iff & \begin{cases} x \in B_n^{\ell,O} & , \alpha + \beta \equiv 0 \pmod 2 \\ x \in B_n^{\ell,E} & , \alpha + \beta \equiv 1 \pmod 2 \end{cases}
\end{aligned}
$$

We conclude that there are exactly $|A_n^{\ell,E}| + |B_n^{\ell,O}|$ or $|A_n^{\ell,O}| + |B_n^{\ell,E}|$ questions that will yield a winning answer, depending on $\alpha + \beta \pmod 2$. The results are summarized in table 5.3.

$\alpha + \beta \pmod 2$	Number of questions that yield a winning answer
0	$\lvert A_n^{\ell,E}\rvert + \lvert B_n^{\ell,O}\rvert$
1	$\lvert A_n^{\ell,O}\rvert + \lvert B_n^{\ell,E}\rvert$

Table 5.3: Number of questions that yield a winning answer

5.2.2.2 Combinatorial Lemmas

Before going any further, we must state and prove some lemmas.

Lemma 5.2.4 ([Gou72], [GJ83]). *Let n, a, i be integers, with $n \neq 0$. Then:*

$$
\sum_{i \equiv 0 \pmod 4} \binom{n}{a+i} = \begin{cases} 2^{n-2} + 2^{\frac{n}{2}-1} & , n - 2a \equiv 0 \pmod 8 \\ 2^{n-2} - 2^{\frac{n}{2}-1} & , n - 2a \equiv 4 \pmod 8 \\ 2^{n-2} & , n - 2a \equiv 2, 6 \pmod 8 \\ 2^{n-2} + 2^{\frac{n-3}{2}} & , n - 2a \equiv 1, 7 \pmod 8 \\ 2^{n-2} - 2^{\frac{n-3}{2}} & , n - 2a \equiv 3, 5 \pmod 8 \end{cases}
$$

Lemma 5.2.5.

Let $n \equiv 1 \pmod 2$. *Then*

$$|A_n^{\ell,E}| + |B_n^{\ell,O}| = \begin{cases} 2^{n-2} + 2^{\frac{n-3}{2}} & ,(n-1)/2 + 3\ell \equiv 0,3 \pmod 4 \\ 2^{n-2} - 2^{\frac{n-3}{2}} & ,(n-1)/2 + 3\ell \equiv 1,2 \pmod 4 \end{cases}$$

Let $n \equiv 0 \pmod 2$. *Then*

$$|A_n^{\ell,E}| + |B_n^{\ell,O}| = \begin{cases} 2^{n-2} & ,n/2 + 3\ell \equiv 1,3 \pmod 4 \\ 2^{n-2} + 2^{\frac{n}{2}-1} & ,n/2 + 3\ell \equiv 0 \pmod 4 \\ 2^{n-2} - 2^{\frac{n}{2}-1} & ,n/2 + 3\ell \equiv 2 \pmod 4 \end{cases}$$

Proof. Recall that

$$\begin{aligned} A_n &= \{x \in P \mid \Delta(x) \equiv 0 \pmod 4\} \\ B_n &= \{x \in P \mid \Delta(x) \equiv 2 \pmod 4\} \\ A_n^{\ell,E} &= \{x \in A_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \ldots, x_n) \equiv 0 \pmod 2\} \\ B_n^{\ell,O} &= \{x \in B_n \mid \Delta(x_{\ell+1}, x_{\ell+2}, \ldots, x_n) \equiv 1 \pmod 2\} \end{aligned}$$

If $\ell = 0$ or $\ell = n$, then

$$|A_n^{\ell,E}| = |A_n| = \sum_{\substack{i \equiv 0 \\ (\text{mod } 4)}} \binom{n}{i}$$

and

$$|B_n^{\ell,O}| = 0.$$

Otherwise, if $0 < \ell < n$,

$$\begin{aligned}|A_n^{\ell,E}| =& \binom{n-\ell}{0}\left(\binom{\ell}{0}+\binom{\ell}{4}+\dots\right)+\binom{n-\ell}{2}\left(\binom{\ell}{4-2}+\binom{\ell}{8-2}+\dots\right)\\ &+\binom{n-\ell}{4}\left(\binom{\ell}{4-4}+\binom{\ell}{8-4}+\dots\right)+\dots\\ =& \binom{n-\ell}{0}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j}+\binom{n-\ell}{2}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j-2}+\dots\\ =& \sum_{\substack{i\equiv 0\\ (\text{mod } 2)}}\binom{n-\ell}{i}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j-i}\end{aligned}$$

So

$$|A_n^{\ell,E}| = \sum_{\substack{i\equiv 0\\ (\text{mod } 4)}}\binom{n-\ell}{i}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j}+\sum_{\substack{i\equiv 0\\ (\text{mod } 4)}}\binom{n-\ell}{i+2}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j+2} \tag{5.10}$$

and similarly,

$$|B_n^{\ell,O}| = \sum_{\substack{i\equiv 0\\ (\text{mod } 4)}}\binom{n-\ell}{i+1}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j+1}+\sum_{\substack{i\equiv 0\\ (\text{mod } 4)}}\binom{n-\ell}{i+3}\sum_{\substack{j\equiv 0\\ (\text{mod } 4)}}\binom{\ell}{j+3} \tag{5.11}$$

Hence we have the equation:

$$|A_n^{\ell,E}|+|B_n^{\ell,O}| = \begin{cases}\sum_{\substack{i\equiv 0\\ (\text{mod } 4)}}\binom{n}{i} & \ell=0 \text{ or } \ell=n\\ (5.10)+(5.11) & \textit{otherwise}\end{cases} \tag{5.12}$$

We will now use equation 5.12 to conclude that lemma 5.2.5 is true.

Suppose $\ell \neq 0$ and $\ell \neq n$. The simplification of equation 5.12 using lemma 5.2.4 depends on the values of n and $\ell \pmod 8$. Hence, we have 8 cases to check for n and 8 cases for ℓ, for a total of 64 cases. Here, we check one case:

Suppose $n \equiv 1 \pmod 8$ and $\ell \equiv 0 \pmod 8$. Using lemma 5.2.4, equation 5.12

becomes:

$$\begin{aligned}|A_n^{\ell,E}|+|B_n^{\ell,O}| =&(2^{n-\ell-2}+2^{\frac{n-\ell-3}{2}})(2^{\ell-2}+2^{\frac{\ell}{2}-1})+\\ &(2^{n-\ell-2}-2^{\frac{n-\ell-3}{2}})(2^{\ell-2}-2^{\frac{\ell}{2}-1})+\\ &(2^{n-\ell-2}+2^{\frac{n-\ell-3}{2}})(2^{\ell-2})+\\ &(2^{n-\ell-2}-2^{\frac{n-\ell-3}{2}})(2^{\ell-2})\\ =&2^{n-2}+2^{\frac{n-3}{2}}.\end{aligned}$$

For this case, the lemma is verified, since $(n-1)/2+3\ell \equiv 0 \pmod 4$. The other cases can be checked in a similar way. In fact, a *Mathematica* worksheet was used to complete the proof (see appendix I).

We must verify the case $\ell = 0$ and $\ell = n$ of equation (5.12) separately. Using lemma 5.2.4:

If $\ell = 0$,

$$\frac{n-1}{2} \equiv 0,3 \pmod 4 \Rightarrow n \equiv 1,7 \pmod 8$$

$$\Rightarrow |A_n^{\ell,E}|+|B_n^{\ell,O}| = 2^{n-2}+2^{\frac{n-3}{2}}$$

$$\frac{n-1}{2} \equiv 1,2 \pmod 4 \Rightarrow n \equiv 3,5 \pmod 8$$

$$\Rightarrow |A_n^{\ell,E}|+|B_n^{\ell,O}| = 2^{n-2}-2^{\frac{n-3}{2}}$$

$$\frac{n}{2} \equiv 1,3 \pmod 4 \Rightarrow n \equiv 2,6 \pmod 8$$

$$\Rightarrow |A_n^{\ell,E}|+|B_n^{\ell,O}| = 2^{n-2}$$

$$\frac{n}{2} \equiv 0 \pmod 4 \Rightarrow n \equiv 0 \pmod 8$$

$$\Rightarrow |A_n^{\ell,E}|+|B_n^{\ell,O}| = 2^{n-2}+2^{\frac{n}{2}-1}$$

$$\frac{n}{2} \equiv 2 \pmod 4 \Rightarrow n \equiv 4 \pmod 8$$

$$\Rightarrow |A_n^{\ell,E}|+|B_n^{\ell,O}| = 2^{n-2}-2^{\frac{n}{2}-1}$$

If $\ell = n$,

$$\begin{aligned}
\frac{n-1}{2} + 3\ell \equiv 0,3 \pmod 4 &\Rightarrow n \equiv 1,7 \pmod 8 \\
&\Rightarrow |A_n^{\ell,E}| + |B_n^{\ell,O}| = 2^{n-2} + 2^{\frac{n-3}{2}} \\
\frac{n-1}{2} + 3\ell \equiv 1,2 \pmod 4 &\Rightarrow n \equiv 3,5 \pmod 8 \\
&\Rightarrow |A_n^{\ell,E}| + |B_n^{\ell,O}| = 2^{n-2} - 2^{\frac{n-3}{2}} \\
\frac{n}{2} + 3\ell \equiv 1,3 \pmod 4 &\Rightarrow n \equiv 2,6 \pmod 8 \\
&\Rightarrow |A_n^{\ell,E}| + |B_n^{\ell,O}| = 2^{n-2} \\
\frac{n}{2} + 3\ell \equiv 0 \pmod 4 &\Rightarrow n \equiv 0 \pmod 8 \\
&\Rightarrow |A_n^{\ell,E}| + |B_n^{\ell,O}| = 2^{n-2} + 2^{\frac{n}{2}-1} \\
\frac{n}{2} + 3\ell \equiv 2 \pmod 4 &\Rightarrow n \equiv 4 \pmod 8 \\
&\Rightarrow |A_n^{\ell,E}| + |B_n^{\ell,O}| = 2^{n-2} - 2^{\frac{n}{2}-1}
\end{aligned}$$

Together with appendix I, this completes the proof of lemma 5.2.5. □

5.2.2.3 Proof of theorem 5.2.2

We are now ready to give the proof of the main theorem for the success proportion.

Proof of theorem 5.2.2. Recall that the success proportion p_s of a deterministic strategy $s \in S_d$ is:

$$p_s = \frac{|\{x \in P \mid \text{strategy } s \text{ applied to } x \text{ yields a winning answer}\}|}{|P|}$$

By section 5.2.2.1, if $s = (\ell, \alpha, \beta) \in S_d$ and $\alpha + \beta \equiv 0 \pmod 2$,

$$p_s = \frac{|A_n^{\ell,E}| + |B_n^{\ell,O}|}{|P|}$$

and if $\alpha + \beta \equiv 1 \pmod 2$,

$$p_s = \frac{|A_n^{\ell,O}| + |B_n^{\ell,E}|}{|P|}$$

Note that $|A_n^{\ell,O}| + |B_n^{\ell,E}| = |P| - (|A_n^{\ell,E}| + |B_n^{\ell,O}|)$.

We will treat the case of even and odd n separately.

- Case 1: n odd

If $\alpha + \beta \equiv 0 \pmod 2$, then

$$p_s = \frac{|A_n^{\ell,E}| + |B_n^{\ell,O}|}{|P|}$$

$$\frac{|A_n^{\ell,E}| + |B_n^{\ell,O}|}{|P|} = \begin{cases} \frac{2^{n-2}+2^{\frac{n-3}{2}}}{|P|}, (n-1)/2 + 3\ell \equiv 0, 3 \pmod 4 \\ \frac{2^{n-2}-2^{\frac{n-3}{2}}}{|P|}, (n-1)/2 + 3\ell \equiv 1, 2 \pmod 4 \end{cases} \quad \text{(by lemma 5.2.5)}$$

$$= \begin{cases} \frac{2^{n-2}+2^{\frac{n-3}{2}}}{2^{n-1}}, (n-1)/2 + 3\ell \equiv 0, 3 \pmod 4 \\ \frac{2^{n-2}-2^{\frac{n-3}{2}}}{2^{n-1}}, (n-1)/2 + 3\ell \equiv 1, 2 \pmod 4 \end{cases}$$

$$= \begin{cases} \frac{1}{2} + 2^{-\lceil n/2 \rceil}, (n-1)/2 + 3\ell \equiv 0, 3 \pmod 4 \\ \frac{1}{2} - 2^{-\lceil n/2 \rceil}, (n-1)/2 + 3\ell \equiv 1, 2 \pmod 4 \end{cases}$$

If $\alpha + \beta \equiv 1 \pmod 2$, then

$$\begin{aligned} p_s =& \frac{|A_n^{\ell,O}| + |B_n^{\ell,E}|}{|P|} \\ =& \frac{|P| - (|A_n^{\ell,E}| + |B_n^{\ell,O}|)}{|P|} \\ =& 1 - \frac{|A_n^{\ell,E}| + |B_n^{\ell,O}|}{|P|} \\ =& \begin{cases} \frac{1}{2} - 2^{-\lceil n/2 \rceil}, (n-1)/2 + 3\ell \equiv 0, 3 \pmod 4 \\ \frac{1}{2} + 2^{-\lceil n/2 \rceil}, (n-1)/2 + 3\ell \equiv 1, 2 \pmod 4 \end{cases} \qquad \text{(by above)} \end{aligned}$$

Since $\frac{1}{2} - 2^{-\lceil n/2 \rceil} < \frac{1}{2} + 2^{-\lceil n/2 \rceil}$, we conclude that for odd n,

$$\max_{s \in S_d} \{p_s\} \leq \frac{1}{2} + 2^{-\lceil n/2 \rceil}$$

To show equality, we must show that every odd $n \geq 3$ admits a strategy that succeeds with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

This is indeed the case. If $n \equiv 1 \pmod 4$, we can choose $\ell = n$ and $\alpha = 0$, and if $n \equiv 3 \pmod 4$, we can choose $\ell = n$ and $\alpha = n$. These strategies are surprisingly simple. They amount to choosing a strategy that doesn't depend on the question (since $\ell = n$). In the first case, all players answer 0, and in the second, all players answer 1 (see table 5.5).

Hence, for the case when n is odd,

$$\max_{s \in S_d} \{p_s\} = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$$

- Case 2: n even

  If $\alpha + \beta \equiv 0 \pmod 2$, then

$$p_s = \frac{|A_n^{\ell,E}| + |B_n^{\ell,O}|}{|P|}$$

$$\frac{|A_n^{\ell,E}|+|B_n^{\ell,O}|}{|P|} = \begin{cases} \frac{2^{n-2}}{|P|} & ,n/2+3\ell \equiv 1,3 \pmod 4 \\ \frac{2^{n-2}+2^{\frac{n}{2}-1}}{|P|} & ,n/2+3\ell \equiv 0 \pmod 4 \\ \frac{2^{n-2}-2^{\frac{n}{2}-1}}{|P|} & ,n/2+3\ell \equiv 2 \pmod 4 \end{cases} \quad \text{(by lemma 5.2.5)}$$

$$= \begin{cases} \frac{2^{n-2}}{2^{n-1}} & ,n/2+3\ell \equiv 1,3 \pmod 4 \\ \frac{2^{n-2}+2^{\frac{n}{2}-1}}{2^{n-1}} & ,n/2+3\ell \equiv 0 \pmod 4 \\ \frac{2^{n-2}-2^{\frac{n}{2}-1}}{2^{n-1}} & ,n/2+3\ell \equiv 2 \pmod 4 \end{cases}$$

$$= \begin{cases} \frac{1}{2} & ,n/2+3\ell \equiv 1,3 \pmod 4 \\ \frac{1}{2}+2^{-\lceil n/2 \rceil} & ,n/2+3\ell \equiv 0 \pmod 4 \\ \frac{1}{2}-2^{-\lceil n/2 \rceil} & ,n/2+3\ell \equiv 2 \pmod 4 \end{cases}$$

If $\alpha+\beta \equiv 1 \pmod 2$, then

$$\begin{aligned} p_s =& \frac{|A_n^{\ell,O}|+|B_n^{\ell,E}|}{|P|} \\ =& \frac{|P|-(|A_n^{\ell,E}|+|B_n^{\ell,O}|)}{|P|} \\ =& 1-\frac{|A_n^{\ell,E}|+|B_n^{\ell,O}|}{|P|} \\ =& \begin{cases} \frac{1}{2} & ,n/2+3\ell \equiv 1,3 \pmod 4 \\ \frac{1}{2}-2^{-\lceil n/2 \rceil} & ,n/2+3\ell \equiv 0 \pmod 4 \\ \frac{1}{2}+2^{-\lceil n/2 \rceil} & ,n/2+3\ell \equiv 2 \pmod 4 \end{cases} \quad \text{(by above)} \end{aligned}$$

Since $\frac{1}{2} - 2^{-\lceil n/2 \rceil} < \frac{1}{2} + 2^{-\lceil n/2 \rceil}$, we conclude that for even n,

$$\max_{s \in S_d}\{p_s\} \leq \frac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

To show equality, we must show that every even $n \geq 4$ admits a strategy that succeeds with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. This is indeed the case. Consider table 5.4:

$n \pmod 8$	$n/2 + 3n \pmod 4$
0	0
2	3
4	2
6	1

Table 5.4: Values of $n/2 + 3n \pmod 4$ for even n

If $n \equiv 0 \pmod 8$, we can choose $\ell = n$ and $\alpha = \beta = 0$. If $n \equiv 4 \pmod 8$, we can choose $\ell = n$, $\alpha = 1$ and $\beta = 0$. These two cases amount to choosing a strategy that doesn't depend on the question (since $\ell = n$). In the first case, all players answer 0, and in the second, all players answer 0, except for one player that answers 1.

However, if $n \equiv 2 \pmod 4$, and if we choose again a strategy where $n = \ell$, then the game is won with probability 1/2. This shows that it is necessary for at least one player to look at his input. To succeed with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$, use the following strategy: If $n \equiv 2 \pmod 8$, choose $\ell = n - 1$ and $\alpha = \beta = 0$. If $n \equiv 6 \pmod 8$, choose $\ell = n - 1$ and $\alpha = 0, \beta = 1$. These two cases amount to choosing a strategy in which all players but one answer 0. There is a single player i who looks at his input x_i, and answers $y_i = x_i$ (first case) or $y_i = \overline{x_i}$ (second case). See table 5.5.

Hence, for the case when n is even,

$$\max_{s \in S_d}\{p_s\} = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$$

$n \pmod 8$	first $n-1$ players' strategy	last player's strategy
0	f_0	f_0
1	f_0	f_0
2	f_0	v_0
3	f_1	f_1
4	f_0	f_1
5	f_0	f_0
6	f_0	v_1
7	f_1	f_1

Table 5.5: Optimal strategies

It follows that

$$\widetilde{\omega}_c(G_n) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$$

for all even and odd n.

□

5.2.3 Classical Success Probability

In this section, we find a value for $\omega_c(G_n)$. From theorems 3.2.2 and 5.2.2, we know that $\omega_c(G_n) \leq \frac{1}{2} + 2^{-\lceil n/2 \rceil}$. The following theorem states that we can reach this bound, and specifies what type of strategy is used to do so.

We call a deterministic strategy *optimal* for the game G_n if it succeeds in proportion $\widetilde{\omega}_c(G_n)$. Let S_o be the set of optimal strategies.

Theorem 5.2.6. *Let G_n be the parity game. Suppose that the n players use the strategy s that consists of choosing an* optimal *strategy in S_o at random according to the uniform distribution. Then for all $x \in P$,*

$$\Pr(\text{win} \mid \text{strategy } s \text{ is used and question } x \text{ is asked}) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

The proof of the theorem follows directly from the next seven lemmas.

Lemma 5.2.7. *Let $n \equiv 1 \pmod 2$. The number of optimal strategies is 2^{2n-1}.*

To prove this lemma and the next one, we could use a counting method, but instead we present more succinct proofs based on mappings.

Proof. There are 2^{2n} deterministic strategies. To show that exactly half are optimal, we define a map $\mathcal{M}$ from the set of optimal strategies to the set of non-optimal strategies. Let $s = (\ell, \alpha, \beta)$ be an optimal strategy. Let $\mathcal{M}$ be defined as the following: change the first player's strategy, according to:

$$f_0 \mapsto f_1$$
$$f_1 \mapsto f_0$$
$$v_0 \mapsto v_1$$
$$v_1 \mapsto v_0$$

Suppose that $\mathcal{M}(s) = s'$, where $s' = (\ell, \alpha', \beta')$: Using results of section 5.2.2.3, a strategy $s = (\ell, \alpha, \beta)$ is optimal if and only if one of the two following conditions hold:

$$\alpha + \beta \equiv 0 \pmod 2 \text{ and } \frac{n-1}{2} + 3\ell \equiv 0, 3 \pmod 4 \tag{5.13}$$
$$\alpha + \beta \equiv 1 \pmod 2 \text{ and } \frac{n-1}{2} + 3\ell \equiv 1, 2 \pmod 4 \tag{5.14}$$

We see that s' is not optimal since under $\mathcal{M}$, n and ℓ are unchanged and $\alpha' + \beta' \equiv \alpha + \beta + 1 \pmod 2$. $\mathcal{M}$ is its own inverse, hence a bijection between the set of optimal strategies and the set of non-optimal strategies exists, these sets are finite, so their cardinality is the same, and the number of optimal strategies is 2^{2n-1}. □

Lemma 5.2.8. *Let* $n \equiv 0 \pmod 2$. *The number of optimal strategies is* 2^{2n-2}.

Proof. There are 2^{2n} deterministic strategies. To show that exactly one quarter are optimal, we define a map $\mathcal{M}$ from the set of non-optimal strategies to the set of optimal strategies. Let $s = (\ell, \alpha, \beta)$ be a non-optimal strategy. Let $\mathcal{M}$ be defined by the following: change the first player's strategy to one of f_0, f_1, v_0, v_1, such that the result is an optimal strategy.

Using results of section 5.2.2.3, a strategy $s = (\ell, \alpha, \beta)$ is optimal if and only if one of the two following conditions hold:

$$\alpha + \beta \equiv 0 \pmod 2 \text{ and } \frac{n}{2} + 3\ell \equiv 0 \pmod 4 \tag{5.15}$$

$$\alpha + \beta \equiv 1 \pmod 2 \text{ and } \frac{n}{2} + 3\ell \equiv 2 \pmod 4 \tag{5.16}$$

For a given s, there are three candidates for its image under $\mathcal{M}$. But only one choice will yield a optimal strategy, since it is always the case that changing the first player's strategy to one of f_0, f_1, v_0, v_1 gives a strategy $s' = (\ell', \alpha', \beta')$ with one of:

1. $\alpha' + \beta' \equiv \alpha + \beta + 1 \pmod 2$
2. $\ell' = \ell + 1$ or $\ell' = \ell - 1$
3. both 1 and 2

Given a non-optimal strategy, there is only one of the above three choices that is optimal. Further, $\mathcal{M}$ is onto. $\mathcal{M}$ is a three-to-one onto map on two finite sets, so $\frac{1}{4}$ of the strategies are optimal. Hence, the number of optimal strategies is 2^{2n-2}. □

Lemma 5.2.9.

$$\sum_{k=1}^{n} \binom{n}{k} = 2^n$$

Proof. By the binomial theorem,

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Substituting $x = 1$, we get

$$2^n = \sum_{k=0}^{n} \binom{n}{k},$$

which is what we wanted to prove. □

Lemma 5.2.10.

$$\sum_{\substack{k\equiv 0\\(\text{mod }2)}} \binom{n}{k} = \sum_{\substack{k\equiv 1\\(\text{mod }2)}} \binom{n}{k} = 2^{n-1}$$

Proof. By the binomial theorem,

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Substituting $x = -1$, we get

$$\begin{aligned} 0 &= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \\ &= \sum_{\substack{k\equiv 0\\(\text{mod }2)}} \binom{n}{k} - \sum_{\substack{k\equiv 1\\(\text{mod }2)}} \binom{n}{k} \end{aligned}$$

And so

$$\sum_{\substack{k\equiv 0\\(\text{mod }2)}} \binom{n}{k} = \sum_{\substack{k\equiv 1\\(\text{mod }2)}} \binom{n}{k}.$$

Since $\sum_{\substack{k\equiv 0\\(\text{mod }2)}} \binom{n}{k} + \sum_{\substack{k\equiv 1\\(\text{mod }2)}} \binom{n}{k} = 2^n$ (by lemma 5.2.9), we conclude that

$$\sum_{\substack{k\equiv 0\\(\text{mod }2)}} \binom{n}{k} = \sum_{\substack{k\equiv 1\\(\text{mod }2)}} \binom{n}{k} = 2^{n-1}.$$

□

Lemma 5.2.11.

$$\sum_{\substack{\alpha+\beta\equiv 0\\(\text{mod }2)}} \binom{n}{\alpha}\binom{r}{\beta} = \sum_{\substack{\alpha+\beta\equiv 1\\(\text{mod }2)}} \binom{n}{\alpha}\binom{r}{\beta} = 2^{n+r-1}$$

Proof. Using lemma 5.2.10,

$$\begin{aligned}\sum_{\substack{\alpha+\beta\equiv 0 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} &= \sum_{\substack{\alpha\equiv 0 \\ \pmod 2}} \sum_{\substack{\beta\equiv 0 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} + \sum_{\substack{\alpha\equiv 1 \\ \pmod 2}} \sum_{\substack{\beta\equiv 1 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} \\ &= 2^{n-1}2^{r-1} + 2^{n-1}2^{r-1} \\ &= 2^{n+r-1}\end{aligned}$$

And similarly,

$$\begin{aligned}\sum_{\substack{\alpha+\beta\equiv 1 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} &= \sum_{\substack{\alpha\equiv 1 \\ \pmod 2}} \sum_{\substack{\beta\equiv 0 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} + \sum_{\substack{\alpha\equiv 0 \\ \pmod 2}} \sum_{\substack{\beta\equiv 1 \\ \pmod 2}} \binom{n}{\alpha}\binom{r}{\beta} \\ &= 2^{n-1}2^{r-1} + 2^{n-1}2^{r-1} \\ &= 2^{n+r-1}\end{aligned}$$

□

Lemma 5.2.12. *Let $n \equiv 1 \pmod 2$. Given any question x that satisfies the promise P in the parity game, the number of optimal strategies that win on x is $2^{2n-2} + 2^{\frac{3n-3}{2}}$.*

Proof. Suppose that the question contains r 1s (by the promise, we have that $r \equiv 0 \pmod 2$). We can assume without loss of generality that the input is ordered, so that

$$x = \overbrace{1, 1, \ldots, 1}^{r}, \overbrace{0, 0, \ldots, 0}^{n-r}$$

Consider the following strategy s:

- Within all the n players:
  - ℓ have strategy f_0 or f_1
  - α have strategy f_1
  - β have strategy v_1

- In particular, within the first r players:
  - ℓ' have strategy f_0 or f_1
  - α' have strategy f_1
  - β' have strategy v_1

If $r \equiv 0 \pmod 4$, then the game is won if and only if the answer is even, otherwise, if $r \equiv 2 \pmod 4$, then the game is won if and only if the answer is odd. By knowing the number of even answers, and the total number of questions, we can deduce the number of odd answers, hence we will count the number of even answers. The number we are looking for is the number of players with strategy f_1 (α) plus the number of players with strategy v_0 that receive 1 as input ($r - \beta' - \ell'$) plus the number of players strategy v_1 that receive 0 as input ($\beta - \beta'$).

Hence, the players' answer will be even if and only if

$$\alpha + (r - \beta' - \ell') + (\beta - \beta') \equiv 0 \pmod 2 \tag{5.17}$$

We already have that

$$r \equiv 0 \pmod 2$$

so equation 5.17 becomes:

$$\ell' \equiv \alpha + \beta \pmod 2 \tag{5.18}$$

Suppose we are given a strategy s and we want to determine if it is optimal. To do this, we use the results of section 5.2.2.3. If $\alpha + \beta \equiv 0 \pmod 2$, s is optimal if and only if $(n-1)/2 + 3\ell \equiv 0, 3 \pmod 4$. Solving this equation, we get two solutions for $\ell \pmod 4$, say ℓ_1, ℓ_2, depending on the value of $n \pmod 8$. If $\alpha + \beta \equiv 1 \pmod 2$, s is optimal if and only if $(n-1)/2 + 3\ell \equiv 1, 2 \pmod 4$. Again, depending on $n \pmod 8$, we get two solutions for $\ell \pmod 4$, say ℓ_3, ℓ_4, depending on the value of $n \pmod 8$. Table 5.6 gives the values of ℓ_1, ℓ_2, ℓ_3, and ℓ_4.

We want to count the number of optimal strategies that yield an even answer.

$n \pmod 8$	ℓ_1	ℓ_2	ℓ_3	ℓ_4
1	0	1	2	3
3	1	2	3	0
5	2	3	0	1
7	3	0	1	2

Table 5.6: Values of $\ell \pmod 4$ for odd n

This is the number of ordered strategies that satisfy equation 5.18 and table 5.6, i.e. one of the following holds:

1. $\ell' \equiv 0 \pmod 2 \wedge \alpha + \beta \equiv 0 \pmod 2 \wedge \ell \pmod 4 \in \{\ell_1, \ell_2\}$

2. $\ell' \equiv 1 \pmod 2 \wedge \alpha + \beta \equiv 1 \pmod 2 \wedge \ell \pmod 4 \in \{\ell_1, \ell_2\}$

So, as long as 1 or 2 is satisfied, we know that we are dealing with an optimal strategy that yields an even answer. We want to count the number of such strategies. One way to do this is to count the number of ways of choosing:

- ℓ' among r
- α' among ℓ'
- β' among $r - \ell'$
- $\ell - \ell'$ among $n - r$
- $\alpha - \alpha'$ among $\ell - \ell'$
- $\beta - \beta'$ among $n - r - (\ell - \ell')$

If $r = 0$, then $\ell' = \alpha' = \beta' = 0$, and the sum we are looking for is:

$$\begin{aligned}
\sum_{\substack{\ell \pmod 4 \\ \in\{\ell_1,\ell_2\}}} \sum_{\substack{\alpha+\beta\equiv 0 \\ \pmod 2}} \binom{n}{\ell}\binom{\ell}{\alpha}\binom{n-\ell}{\beta} &= 2^{n-1} \sum_{\substack{\ell \pmod 4 \\ \in\{\ell_1,\ell_2\}}} \binom{n}{\ell} \quad \text{(by lemma 5.2.11)} \\
&= 2^{n}\left(2^{n-1} + 2^{\frac{n-3}{2}}\right) \quad \text{(by table 5.7 and lemma 5.2.4)} \\
&= 2^{2n-2} + 2^{\frac{3n-3}{2}}
\end{aligned}$$

$n \pmod 8$	$n-2\ell_1$	$n-2\ell_2$
1	1	7
3	1	7
5	1	7
7	1	7

Table 5.7: Values of $n-2\ell \pmod 8$ for odd n

The case where $n = r$ is impossible, since n is odd and r is even.

Otherwise, as long as $r \neq 0$ and $r \neq n$, the sum that we are looking for is:

$$\begin{aligned}&\sum_{\substack{\ell'\equiv 0\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in\{\ell_1,\ell_2\}}} \sum_{p'} \sum_{\beta'} \sum_{\substack{\alpha+\beta\equiv 0\\ \pmod 2}} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\binom{\ell-\ell'}{\alpha-\alpha'}\binom{n-r-(\ell-\ell')}{\beta-\beta'}\\ &+\sum_{\substack{\ell'\equiv 1\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in\{\ell_3,\ell_4\}}} \sum_{\alpha'} \sum_{\beta'} \sum_{\substack{\alpha+\beta\equiv 1\\ \pmod 2}} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\binom{\ell-\ell'}{\alpha-\alpha'}\binom{n-r-(\ell-\ell')}{\beta-\beta'}\end{aligned} \tag{5.19}$$

Using lemma 5.2.11,

$$\begin{aligned}&= 2^{n-r-1} \sum_{\substack{\ell'\equiv 0\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in\{\ell_1,\ell_2\}}} \sum_{\alpha'} \sum_{\beta'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\\ &\qquad + 2^{n-r-1} \sum_{\substack{\ell'\equiv 1\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in\{\ell_3,\ell_4\}}} \sum_{\alpha'} \sum_{\beta'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\end{aligned} \tag{5.20}$$

Using lemma 5.2.9,

$$\begin{aligned}&= 2^{n-r-1}2^{r-\ell'} \sum_{\substack{\ell'\equiv 0\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in\{\ell_1,\ell_2\}}} \sum_{\alpha'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{n-r}{\ell-\ell'}\\ &\qquad + 2^{n-r-1}2^{r-\ell'} \sum_{\substack{\ell'\equiv 1\\ \pmod 2}} \sum_{\substack{\ell \pmod 4\\ \in \ell_3,\ell_4}} \sum_{\alpha'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{n-r}{\ell-\ell'}\end{aligned} \tag{5.21}$$

Again, by lemma 5.2.9,

$$= 2^{n-1} \sum_{\substack{\ell' \equiv 0 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell \pmod 4 \\ \in\{\ell_1,\ell_2\}}} \binom{r}{\ell'}\binom{n-r}{\ell-\ell'} + 2^{n-1} \sum_{\substack{\ell' \equiv 1 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell \pmod 4 \\ \in\{\ell_3,\ell_4\}}} \binom{r}{\ell'}\binom{n-r}{\ell-\ell'} \tag{5.22}$$

Which is equal to:

$$\begin{aligned}
= 2^{n-1} \sum_{\substack{\ell' \equiv 0 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'} &\left(\sum_{\substack{\ell \equiv \ell_1 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} + \sum_{\substack{\ell \equiv \ell_2 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} \right) \\
+ 2^{n-1} \sum_{\substack{\ell' \equiv 2 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'} &\left(\sum_{\substack{\ell \equiv \ell_1 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} + \sum_{\substack{\ell \equiv \ell_2 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} \right) \\
+ 2^{n-1} \sum_{\substack{\ell' \equiv 1 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'} &\left(\sum_{\substack{\ell \equiv \ell_3 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} + \sum_{\substack{\ell \equiv \ell_4 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} \right) \\
+ 2^{n-1} \sum_{\substack{\ell' \equiv 3 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'} &\left(\sum_{\substack{\ell \equiv \ell_3 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} + \sum_{\substack{\ell \equiv \ell_4 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'} \right)
\end{aligned} \tag{5.23}$$

We can simplify equation 5.23 by repeatedly applying lemma 5.2.4. We have 4 cases for $n \pmod 8$ (which yield $\ell_1, \ell_2, \ell_3, \ell_4$) and 4 cases for $r \pmod 8$, hence 16 cases. We have used a *Mathematica* worksheet (appendix II) to do these simplifications, the result is:

$$= \begin{cases} 2^{2n-2} + 2^{\frac{3n-3}{2}} & , r \equiv 0 \pmod 4 \\ 2^{2n-2} - 2^{\frac{3n-3}{2}} & , r \equiv 2 \pmod 4 \end{cases}$$

So if $r \equiv 0 \pmod 4$, the number of winning optimal strategies is the number of optimal strategies that yield an even answer, hence $2^{2n-2} + 2^{\frac{3n-3}{2}}$ winning answers, and otherwise if $r \equiv 2 \pmod 4$, there are $2^{2n-1} - \left(2^{2n-2} - 2^{\frac{3n-3}{2}}\right) = 2^{2n-2} + 2^{\frac{3n-3}{2}}$

optimal strategies that yield an odd, hence winning, answer (using lemma 5.2.7).

□

Lemma 5.2.13. *Let* $n \equiv 0 \pmod{2}$. *Given any question* x *that satisfies the promise* P *in the parity game, the number of optimal strategies that win on* x *is* $2^{\frac{3n}{2}-2} + 2^{2n-3}$

Proof. We use the same argument as in the proof of lemma 5.2.13, except that there are only two values of ℓ, ℓ_1, ℓ_3, that yield an optimal strategy (table 5.8).

$n \pmod 8$	ℓ_1	ℓ_3
0	0	2
2	1	3
4	2	0
6	3	1

Table 5.8: Values of $\ell \pmod 4$ for even n

If $r = 0$, then $\ell' = \alpha' = \beta' = 0$, and the sum we are looking for is:

$$\sum_{\substack{\ell\equiv\ell_1 \\ \pmod 4}} \sum_{\substack{\alpha+\beta\equiv 0 \\ \pmod 2}} \binom{n}{\ell}\binom{\ell}{\alpha}\binom{n-\ell}{\beta} = 2^{n-1} \sum_{\substack{\ell\equiv\ell_1 \\ \pmod 4}} \binom{n}{\ell} \text{ (by lemma 5.2.11)}$$

$$= 2^{n-1}\left(2^{n-2} + 2^{\frac{n}{2}-1}\right) \text{ (by table 5.9 and lemma 5.2.4)}$$

$$= 2^{2n-3} + 2^{\frac{3n-3}{2}-2}$$

$n \pmod 8$	ℓ_1	$n - 2\ell_1$
0	0	0
2	1	0
4	2	0
6	3	0

Table 5.9: Values of $n - 2\ell_1 \pmod 8$ for even n

If $n = r$, then $\ell' = \ell, \alpha' = p, \beta' = \beta$ and we consider the cases $n \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$ separately.

If $n \equiv 0 \pmod 4$, the number we are looking for is:

$$\sum_{\substack{\ell \equiv \ell_1 \\ \pmod 4}} \sum_{\substack{\alpha+\beta\equiv 0 \\ \pmod 2}} \binom{n}{\ell}\binom{\ell}{\alpha}\binom{n-\ell}{\beta} = 2^{2n-3} + 2^{\frac{3n-3}{2}-2} \text{ (by above).}$$

If $n \equiv 2 \pmod 4$, the number we are looking for is:

$$\begin{aligned}\sum_{\substack{\ell \equiv \ell_3 \\ \pmod 4}} \sum_{\substack{\alpha+\beta\equiv 1 \\ \pmod 2}} \binom{n}{\ell}\binom{\ell}{\alpha}\binom{n-\ell}{\beta} &= 2^{n-1} \sum_{\substack{\ell \equiv \ell_1 \\ \pmod 4}} \binom{n}{\ell} \text{ (by lemma 5.2.11)} \\ &= 2^{n-1}\left(2^{n-2} - 2^{\frac{n}{2}-1}\right) \text{ (by table 5.10 and lemma 5.2.4)} \\ &= 2^{2n-3} - 2^{\frac{3n-3}{2}-2}\end{aligned}$$

$n \pmod 8$	ℓ_3	$n - 2\ell_3$
2	3	4
6	1	4

Table 5.10: Values of $n - 2\ell_3 \pmod 8$ for even n

Otherwise, as long as $r \neq 0$ and $r \neq n$, the sum that we are looking for is:

$$\begin{aligned}&\sum_{\substack{\ell' \equiv 0 \\ \pmod 2}} \sum_{\substack{\ell \equiv \ell_1 \\ \pmod 4}} \sum_{\alpha'} \sum_{\beta'} \sum_{\substack{\alpha+\beta\equiv 0 \\ \pmod 2}} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\binom{\ell-\ell'}{\alpha-\alpha'}\binom{n-r-(\ell-\ell')}{\beta-\beta'} \\ +&\sum_{\substack{\ell' \equiv 1 \\ \pmod 2}} \sum_{\substack{\ell \equiv \ell_3 \\ \pmod 4}} \sum_{\alpha'} \sum_{\beta'} \sum_{\substack{\alpha+\beta\equiv 1 \\ \pmod 2}} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\binom{\ell-\ell'}{\alpha-\alpha'}\binom{n-r-(\ell-\ell')}{\beta-\beta'}\end{aligned}$$

Using lemma 5.2.11,

$$\begin{aligned}&= 2^{n-r-1} \sum_{\substack{\ell' \equiv 0 \\ \pmod 2}} \sum_{\substack{\ell \equiv \ell_1 \\ \pmod 4}} \sum_{\alpha'} \sum_{\beta'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'} \\ &\qquad + 2^{n-r-1} \sum_{\substack{\ell' \equiv 1 \\ \pmod 2}} \sum_{\substack{\ell \equiv \ell_3 \\ \pmod 4}} \sum_{\alpha'} \sum_{\beta'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{r-\ell'}{\beta'}\binom{n-r}{\ell-\ell'}\end{aligned}$$

Using lemma 5.2.9,

$$= 2^{n-r-1}2^{r-\ell'} \sum_{\substack{\ell'\equiv 0 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell\equiv\ell_1 \\ (\mathrm{mod}\ 4)}} \sum_{\alpha'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{n-r}{\ell-\ell'}$$
$$+ 2^{n-r-1}2^{r-\ell'} \sum_{\substack{\ell'\equiv 1 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell\equiv\ell_3 \\ (\mathrm{mod}\ 4)}} \sum_{\alpha'} \binom{r}{\ell'}\binom{\ell'}{\alpha'}\binom{n-r}{\ell-\ell'}$$

Again, by lemma 5.2.9,

$$= \quad 2^{n-1} \sum_{\substack{\ell'\equiv 0 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell\equiv\ell_1 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\binom{n-r}{\ell-\ell'} + 2^{n-1} \sum_{\substack{\ell'\equiv 1 \\ (\mathrm{mod}\ 2)}} \sum_{\substack{\ell\equiv\ell_3 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\binom{n-r}{\ell-\ell'}$$

Which is equal to:

$$= 2^{n-1}\left(\sum_{\substack{\ell'\equiv 0 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\left(\sum_{\substack{\ell\equiv\ell_1 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'}\right) + \sum_{\substack{\ell'\equiv 2 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\left(\sum_{\substack{\ell\equiv\ell_1 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'}\right)\right)$$
$$+ 2^{n-1}\left(\sum_{\substack{\ell'\equiv 1 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\left(\sum_{\substack{\ell\equiv\ell_3 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'}\right) + \sum_{\substack{\ell'\equiv 3 \\ (\mathrm{mod}\ 4)}} \binom{r}{\ell'}\left(\sum_{\substack{\ell\equiv\ell_3 \\ (\mathrm{mod}\ 4)}} \binom{n-r}{\ell-\ell'}\right)\right) \tag{5.24}$$

We can simplify 5.24 by repeatedly applying lemma 5.2.4. We have 4 cases for $n \pmod 8$ (which yield ℓ_1 and ℓ_3) and 4 cases for $r \pmod 8$, hence 16 cases. We have used a *Mathematica* worksheet (appendix II) to do these simplifications, the result is:

$$= \begin{cases} 2^{2n-3} + 2^{\frac{3n}{2}-2}, & r \equiv 0 \pmod 4 \\ 2^{2n-3} - 2^{\frac{3n}{2}-2}, & r \equiv 2 \pmod 4. \end{cases}$$

So if $r \equiv 0 \pmod 4$, the number of winning optimal strategies is the number of optimal strategies that yield an even answer, hence $2^{\frac{3n}{2}-2} + 2^{2n-3}$ winning answers, and otherwise if $r \equiv 0 \pmod 4$, there are $2^{2n-2} - \left(2^{2n-3} - 2^{\frac{3n}{2}-2}\right) = 2^{\frac{3n}{2}-2} + 2^{2n-3}$

strategies that yield an odd, hence winning, answer (using lemma 5.2.8). □

We are now ready to give the main proof for this section.

Proof of theorem 5.2.6. If n is odd, by lemma 5.2.7, there are 2^{2n-1} optimal strategies. By lemma 5.2.12, given any question x that satisfies the promise P in the parity game, the number of optimal strategies that win on x is $2^{2n-2} + 2^{\frac{3n-3}{2}}$. Therefore, the probability is

$$\frac{2^{2n-2} + 2^{\frac{3n-3}{2}}}{2^{2n-1}} = \frac{1}{2} + 2^{-(\frac{n+1}{2})} = \frac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

If n is even, by lemma 5.2.8, there are 2^{2n-2} optimal strategies. By lemma 5.2.13, given any question x that satisfies the promise P in the parity game, the number of optimal strategies that win on x is $2^{2n-3} + 2^{\frac{3n}{2}-2}$. Therefore, the probability is

$$\frac{2^{2n-3} + 2^{\frac{3n}{2}-2}}{2^{2n-2}} = \frac{1}{2} + 2^{-\frac{n}{2}} = \frac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

□

5.2.4 Towards Closing the Detection Loophole

In this section, we analyze the tolerance to detector errors and inefficiencies.

5.2.4.1 Noisy Detectors

In section 3.3.1, we defined p as the probability that a player's answer corresponds to the predictions of quantum mechanics in a game with errors. We wish to find the value of $p_*(G_n)$, that is, the maximum value of p for which a classical strategy can succeed as well as a quantum strategy. The following lemma is useful for the proof of theorem 5.2.15.

Lemma 5.2.14. *Consider the parity game with errors. The probability of having an even number of errors is given by:*

$$p_n = \frac{1}{2} + \frac{(2p-1)^n}{2}.$$

Proof. The proof is by induction on n. The base case is $n = 1$. The probability of having an even number of errors is p, hence $p_1 = p$, which is what we needed to show.

For the induction hypothesis, suppose that

$$p_k = \frac{1}{2} + \frac{(2p-1)^k}{2}.$$

Consider p_{k+1}:

$$\begin{aligned} p_{k+1} =& p_k(p) + (1-p_k)(1-p) \\ =& 1 - p - p_k + 2pp_k \\ =& 1 - p - \frac{1}{2} - \frac{(2p-1)^k}{2} + 2p\left(\frac{1}{2} + \frac{(2p-1)^k}{2}\right) \\ =& \frac{1}{2} - \frac{(2p-1)^k}{2} + 2p\frac{(2p-1)^k}{2} \\ =& \frac{1}{2} + \frac{(2p-1)^{k+1}}{2}. \end{aligned}$$

Hence, $p_n = \frac{1}{2} + \frac{(2p-1)^n}{2}$ for all n. □

The following theorem and proof are from [BBT03]; a similar result with a very different proof appears in [BM93].

Theorem 5.2.15. *Let G_n be the parity game. Then*

$$p_*(G_n) = \begin{cases} \frac{1}{2} + 2^{\frac{1-3n}{2n}} & , n \equiv 1 \pmod 2 \\ \frac{1}{2} + 2^{\frac{2-3n}{2n}} & , n \equiv 0 \pmod 2 \end{cases}$$

Proof. Let p be the probability that a player's answer corresponds to the predictions of quantum mechanics in a game with errors. The probability p_n that the game is won is given by the probability of having an even number of errors. By lemma 5.2.14,

$$p_n = \frac{1}{2} + \frac{(2p-1)^n}{2}$$

By theorem 5.2.2 $\omega_c(G_n) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$. For any fixed odd n, define

$$e_n = \frac{1}{2} + 2^{\frac{1-3n}{2n}}$$

Suppose that $p > e_n$. Then

$$\begin{aligned} p_n &= \frac{1}{2} + \frac{(2p-1)^n}{2} \\ &> \frac{1}{2} + \frac{(2e_n-1)^n}{2} \\ &= \frac{1}{2} + \frac{\left(2\left(\frac{1}{2} + 2^{\frac{1-3n}{2n}}\right) - 1\right)^n}{2} \\ &= \frac{1}{2} + \frac{\left(2^{\frac{1-n}{2n}}\right)^n}{2} \\ &= \frac{1}{2} + 2^{-\frac{n+1}{2}} \\ &= \frac{1}{2} + 2^{-\lceil n/2 \rceil} \end{aligned}$$

And so if $p > e_n$, no classical strategy exists. Hence for odd n, $p_*(G_n) = e_n$. For any fixed even n, define

$$e_n = \frac{1}{2} + 2^{\frac{2-3n}{2n}}$$

Suppose that $p > e_n$. Then

$$\begin{aligned} p_n &= \frac{1}{2} + \frac{(2p-1)^n}{2} \\ &> \frac{1}{2} + \frac{(2e_n-1)^n}{2} \\ &= \frac{1}{2} + \frac{\left(2\left(\frac{1}{2}+2^{\frac{2-3n}{2n}}\right)-1\right)^n}{2} \\ &= \frac{1}{2} + \frac{\left(2^{\frac{2-n}{2n}}\right)^n}{2} \\ &= \frac{1}{2} + 2^{-\frac{n}{2}} \\ &= \frac{1}{2} + 2^{-\lceil n/2 \rceil} \end{aligned}$$

And so if $p > e_n$, no classical strategy exists. Hence for even n, $p_*(G_n) = e_n$. □

As a consequence of theorem 5.2.15, and since for both odd and even n,

$$\lim_{n\to\infty} p_*(G_n) = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 85\%,$$

we conclude that if $p > \frac{1}{2} + \frac{\sqrt{2}}{4}$ and as long as n is sufficiently large, classical players cannot succeed as well as quantum players in the game G_n.

5.2.4.2 Inefficient Detectors

Let $G_n^0 = (X, Y, P, W)$ be the parity game. We define $G_n^1 = (X, Y, P', W')$ to be a game similar to G_n^0, but with a slight variation on the promise and on the winning condition:

$$P' : \sum_i^n x_i \equiv 1 \pmod 2$$

$$W' : \sum_i^n y_i \equiv \frac{(\sum_i^n x_i) + 1}{2} \pmod 2$$

By applying an argument similar to theorem 5.1.3, it is easy to see that $\widetilde{\omega}_c(G_3^0) < 1$.

Using the same reasoning as in beginning of section 5.2.2, it follows that $\widetilde{\omega}_c(G_n^0) < 1$ for all $n \geq 3$. We will not study G_n^1 for its own sake, but it is useful to have such a definition for the proof of theorem 5.2.16. Recall that in the error-free model, defined in section 3.3.2, we enlarge each player's set of outputs Y_i to include the special symbol $\perp$ which means that the player's apparatus fails to give an answer. The outcome is a draw if $y_i = \perp$ for any player i. If the outcome is not a draw, we require that it be correct.

Theorem 5.2.16. *For the parity game, and in the error-free model, the best the players can do using a deterministic strategy is answer correctly for 2 questions.*

Proof. Let G_n^0 be the parity game and G_n^1 as defined above. We will prove by induction on n, the number of players, that they cannot answer correctly (in the error-free model) for more than 2 questions for the game G_n^0 as well as for G_n^1. Then, we give a simple strategy for G_n^1 that succeeds for 2 questions.

The base case is $n = 3$. In the game G_3^0, the valid questions are:

$$\begin{aligned} x^1 &= 0,0,0 \\ x^2 &= 0,1,1 \\ x^3 &= 1,0,1 \\ x^4 &= 1,1,0. \end{aligned}$$

Recall from section 3.1 that x_i represents player i's input and y_i his output. In the game G_3^0, and in the error-free model, at least one player i must answer $y_i = \perp$ for an input $x_i = 0$ or $x_i = 1$, since, otherwise, all players would always answer correctly and so $\omega_c(G_n^0) = 1$, which contradicts theorem 5.2.2. Each player j has input $x_j = 0$ and $x_j = 1$ exactly twice, hence there are at least two questions that yield a draw and at most two questions are correctly answered.

For the game G_3^1, the valid questions are:

$$\begin{aligned} q^1 &= 1,1,1 \\ q^2 &= 1,0,0 \\ q^3 &= 0,1,0 \\ q^4 &= 0,0,1. \end{aligned}$$

If we complement each bit of $x^1, \ldots, x^4$ in G_3^0, we get $q^1, \ldots, q^4$, and an answer is correct for x^ℓ if and only if it is correct for q^ℓ ($\ell = 1, \ldots, 4$). Suppose that there exists an error-free strategy s that answers correctly for m ($m = 0, \ldots, 4$) questions in the game G_3^1. Then we have an error-free strategy that answers correctly for m questions in the game G_3^0, since the players can use the following strategy: each player complements his input bit, and then applies his individual strategy that is part of s. Since at most two questions are correctly answered for the game G_3^0, then the same holds for the game G_3^1. This completes the base case.

The inductive hypothesis is the following: suppose that for any $k \geq 3$, in the game G_k^0 and G_k^1, the players can answer correctly for at most 2 questions.

For the inductive step, consider the game G_{k+1}^j ($j \in \{0,1\}$). We will prove by contradiction that at most two questions may be correctly answered. Suppose that at least 3 questions may be correctly answered, let $S = \{x^1, x^2, x^3\}$ be a set of questions that are correctly answered, where $x^\ell = x_1^\ell, x_2^\ell, \ldots, x_n^\ell$ ($\ell \in \{1,2,3\}$). As in the base case, at least one player, i, must answer $y_i = \perp$ for an input $x_i = 0$ or $x_i = 1$ since otherwise, the game would always be won. Suppose, without loss of generality, that $i = 1$, so the first player answers $\perp$ on input $x_\perp \in \{0,1\}$, and answers $y \in \{0,1\}$ otherwise. We have 4 cases to consider, depending on $x_\perp$ and y.

1. $x_\perp = 1$, $y = 0$: We have $x_1^\ell = 0$ ($x^\ell \in S$), since otherwise the answer to one or more of the questions in S would be a draw. If we remove the first player from the game, keeping players' $2, \ldots, k+1$ questions and strategies intact, we have the game G_k^j with a strategy that answers correctly on 3 or more questions.

2. $x_\perp = 1$, $y = 1$: We have $x_1^\ell = 0$ ($x^\ell \in S$) since otherwise the answer to one or more of the questions in S would be a draw. Remove the first player from the game, keeping players' $3, \ldots, k+1$ questions and strategies intact. Keep player 2's questions, but change his strategy so that he outputs the complement of the bit he was to output. Then we have the game G_k^j with a strategy that answers correctly for 3 or more questions.

3. $x_\perp = 0$, $y = 0$: We have $x_1^\ell = 1$ ($x^\ell \in S$) since otherwise the answer to one or more of the questions in S would be a draw. If we remove the first player from the game, keeping players' $2, \ldots, k+1$ questions and strategies intact, we have the game $G_k^{j\oplus 1}$ with a strategy that answers correctly for 3 or more questions.

4. $x_\perp = 0$, $y = 1$: We have $x_1^\ell = 1$ ($x^\ell \in S$) since otherwise the answer to one or more of the questions in S would be a draw. Remove the first player from the game, keeping players' $3, \ldots, k+1$ questions and strategies intact. Keep player 2's questions, but change his strategy so that he outputs the complement of the bit he was to output. Then we have the game $G_k^{j\oplus 1}$ with a strategy that answers correctly for 3 or more questions.

In all cases, we contradict the inductive hypothesis that for the game G_k^0 and G_k^1, the players can answer correctly for at most 2 questions. So, by the principle of mathematical induction we know that for all $n \geq 3$, and for the games G_n^0 and G_n^1, the best the players can do is answer correctly for at most 2 questions.

We give a simple strategy that succeeds for 2 questions for the game G_n^0: all players answer 0 on input 0 and $\perp$ otherwise, except for the first two players. Player 1 always outputs 0, and player 2 outputs 0 on input 0 and 1 on input 1. Then all questions that satisfy the promise lead to a draw, except questions $0, 0, 0, \ldots, 0$ and $1, 1, 0, \ldots, 0$, which are correctly answered. Hence, the best the players can do is answer correctly for exactly two questions. □

The following improves on the results of [BBT03] and [BM93].

Corollary 5.2.17. *Let G_n be the parity game. Then $\eta_*(G_n) = \frac{1}{2}\sqrt[n]{4}$.*

Proof. By theorem 5.2.16, the best the classical players can do in the error-free model (using a deterministic strategy) is to answer correctly for 2 questions. Using reasoning similar to theorems 3.2.1 and 3.2.2, we conclude that no probabilistic strategy can succeed in the error-free model with probability strictly greater than $\frac{2}{2^{n-1}}$.

Since we assume that the detector efficiencies are independent,

$$\eta_*^n = \frac{2}{2^{n-1}}$$

and so

$$\begin{aligned}\eta_* &= \sqrt[n]{\frac{2}{2^{n-1}}}\\ &= \frac{1}{2}\sqrt[n]{4}\end{aligned}$$

□

As a consequence of corollary 5.2.17, and since

$$\lim_{n\to\infty} \frac{1}{2}\sqrt[n]{4} = \frac{1}{2},$$

we conclude that if $\eta \geq 50\%$ and as long as n is sufficiently large, classical players cannot succeed as well as quantum players in the game G_n.

5.3 The Extended Parity Game

The following game, proposed by Buhrman, Høyer, Massar and Röhrig [BHMR03], is a generalization of the parity game presented in section 5.2, in the sense that each player's input is a *string* of bits (of length approximately $\lg n$), instead of a single bit as in the parity game. In the extended parity game (table 5.11), each player i receives as input a bit-string of length $\lceil \lg_2 n \rceil - 1$; we also interpret x_i as an integer in base 2. The promise is that $\sum_{i=1}^{n} x_i$ is divisible by 2^ℓ. Each player then outputs a single bit y_i. The players win if and only if $\sum_{i=1}^{n} y_i \equiv \frac{\sum_{i=1}^{n} x_i}{2^\ell} \pmod 2$.

The advantage of this game over the parity game is that it is "harder" to win classically. We will explain what we mean by this shortly.

Extended parity game	
n	$n \geq 3$
X	$X_i = \{0,1\}^\ell$ $(i = 1 \ldots n)$, $\ell = \lceil \lg_2 n \rceil - 1$
Y	$Y_i = \{0,1\}$ $(i = 1 \ldots n)$
P	$\sum_{i=1}^{n} x_i \equiv 0 \pmod{2^\ell}$
W	$\sum_{i=1}^{n} y_i \equiv \frac{\sum_{i=1}^{n} x_i}{2^\ell} \pmod 2$
ω_c	< 1
$\widetilde{\omega}_c$	< 1
η^*	$\leq \frac{8}{n}$
$\vert\psi\rangle$	$\frac{1}{\sqrt{2}}(\vert 0^n\rangle + \vert 1^n\rangle)$

Table 5.11: Extended parity game

5.3.1 A Quantum Winning Strategy

Theorem 5.3.1. *Let G_n be the extended parity game. Then $\omega_q(G_n) = 1$.*

Proof. The player's strategy is to share a state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$. After receiving his input x_i, each player i does the following:

1. if $x_i \neq 0$, apply the unitary transformation S given by

$$|0\rangle \rightarrow |0\rangle$$
$$|1\rangle \rightarrow e^{\frac{\pi i x_i}{2^\ell}} |1\rangle,$$

2. apply H

3. measure the qubit to obtain y_i

4. output y_i

Then the resulting state after step 1 is:

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}}\left(|0^n\rangle + e^{\pi i \frac{\sum_i^n x_i}{2^\ell}}|1^n\rangle\right)\\ &= \begin{cases} \frac{1}{\sqrt{2}}\left(|0^n\rangle + |1^n\rangle\right) & , \frac{\sum_i^n x_i}{2^\ell} \equiv 0 \pmod 2\\ \frac{1}{\sqrt{2}}\left(|0^n\rangle - |1^n\rangle\right) & , \frac{\sum_i^n x_i}{2^\ell} \equiv 1 \pmod 2\end{cases}\end{aligned}$$

We know by the promise P that $\frac{\sum_i^n x_i}{2^\ell}$ is an integer, so by proposition 5.1.1, the resulting state after step 2 is:

$$\begin{aligned}&\frac{1}{\sqrt{2^{n-1}}}\sum_{\substack{\Delta(y)\equiv 0\\ \pmod 2}} |y\rangle \ , \frac{\sum x_i}{2^\ell} \equiv 0 \pmod 2\\ &\frac{1}{\sqrt{2^{n-1}}}\sum_{\substack{\Delta(y)\equiv 1\\ \pmod 2}} |y\rangle \ , \frac{\sum x_i}{2^\ell} \equiv 1 \pmod 2.\end{aligned}$$

And so after the measurement of step 3, the output of step 4 will satisfy:

$$\sum_i^n y_i \equiv \frac{\sum_i^n x_i}{2^\ell} \pmod 2$$

so the players always win. □

5.3.2 Classical Success Proportion

The following theorem shows that the extended parity game is a pseudo-telepathy game. Its proof shows that the parity game is a subset of the extended parity game.

Theorem 5.3.2. *Let G_n be the extended parity game. Then $\widetilde{\omega}_c(G_n) < 1$.*

Proof. Suppose for a contradiction that $\widetilde{\omega}_c(G_n) = 1$ for any n. This means that classical players always have a deterministic winning strategy. In particular, the players have a winning strategy on all questions of the form $x_i = b_i00\ldots0$, where $b_i \in \{0,1\}$. But this subset of questions constitutes the parity game, since the promise becomes:

$$\begin{aligned}\sum_{i=1}^{n} x_i \equiv 0 \pmod{2^\ell} &\Leftrightarrow \sum_{i=1}^{n} b_i 2^{\ell-1} \equiv 0 \pmod{2^\ell} \\ &\Leftrightarrow \sum_{i=1}^{n} b_i \equiv 0 \pmod{2}\end{aligned}$$

And for the same reason, the winning condition becomes

$$\sum_{i=1}^{n} y_i \equiv \frac{\sum_{i=1}^{n} b_i}{2} \pmod{2}$$

Since the players have a winning strategy on all questions of the form $x_i = b_i00\ldots0$, then they have a winning strategy for the parity game, which contradicts theorem 5.2.2. □

Using theorem 3.2.2, we get the following corollary:

Corollary 5.3.3. *Let G_n be the extended parity game. Then $\omega_c(G_n) < 1$.*

5.3.3 Towards Closing the Detection Loophole

5.3.3.1 Error-Free Model

We have just seen that the parity game is a subset of the extended parity game. This gives us the intuition that classically, the extended parity game should not be any easier to win than the parity game. The following theorem confirms this in the error-free model.

Theorem 5.3.4. *Let G_n be the extended parity game. Then $\eta_*(G_n) \leq \frac{8}{n}$.*

The proof of this theorem, which appears in [BHMR03], is too involved to reproduce here. It is based on previous results from [BCT99].

Although this bound is interesting, we would like to know an exact value for $\eta_*(G_n)$. So far, we have only been able to come up with an educated guess:

Conjecture 5.3.5. Let G_n be the extended parity game. Then

$$\eta_*(G_n) = \sqrt[n]{\frac{2^{2^\ell - 1}}{2^{\ell(n-1)}}}. \tag{5.25}$$

The idea behind conjecture 5.3.5 is that there exists a strategy that can answer correctly at most $2^{2^\ell-1}$ out of a total of $2^{\ell(n-1)}$ questions. We conjecture that this is the best classical players can do.

To support the hypothesis, we give an error-free strategy that succeeds on $2^{2^\ell-1}$ questions:

- Players $1, 2, \ldots 2^\ell - 1$ answer 0 on input $00\ldots0$ and $00\ldots01$, and $\perp$ otherwise.
- Player 2^ℓ answers 0 on input $00\ldots0$ and 1 otherwise.
- The remaining $n - 2^\ell$ players answer 0 on $00\ldots0$ and $\perp$ otherwise.

Suppose that the players produce an answer other than $\perp$. We show here that the answer satisfies the winning condition W:

Since the $n - 2^\ell$ last players must have input $00\ldots0$,

$$\sum_{i=1}^{2^\ell-1} x_i + x_{2^\ell} \equiv 0 \pmod{2^\ell}.$$

And since

$$\sum_{i=1}^{2^\ell-1} x_i \leq 2^\ell - 1,$$

we must have that

$$x_{2^\ell} = 2^\ell - \sum_{i=1}^{2^\ell-1} x_i.$$

In particular, if

$$\sum_{i=1}^{2^\ell-1} x_i = 0,$$

then $x_{2^\ell} = 0$ and the output is $y = 0, 0, \ldots 0$, which satisfies the winning condition W. If

$$\sum_{i=1}^{2^\ell-1} x_i > 0,$$

then

$$x_{2^\ell} = 2^\ell - \sum_{i=1}^{2^\ell-1} x_i \neq 0,$$

and the output is $y = 0, 0, \ldots 0, 1, 0, 0, \ldots 0$, which satisfies the winning condition W, since

$$\sum_{i=1}^{n} y_i = 1$$

and

$$\begin{aligned}\frac{\sum_{i=1}^{n} x_i}{2^\ell} &= \frac{\sum_{i=1}^{2^\ell-1} x_i + 2^\ell - \sum_{i=1}^{2^\ell-1} x_i}{2^\ell} \\ &= \frac{2^\ell}{2^\ell} \\ &= 1.\end{aligned}$$

So the winning condition is satisfied.

Then the players answer correctly on $2^{2^\ell-1}$ questions (since players $1, 2, \ldots, 2^\ell - 1$

answer on two questions, and the 2^ℓth players' input is fixed, once the questions to players $1, 2, \ldots, 2^\ell - 1$ have been fixed), and otherwise the outcome is a draw.

5.3.3.2 Model With Errors

No results for the extended parity game are known in the model with errors, although the authors of [BHMR03] give a hint as to an upcoming paper with results in this model. Here, we give a conjecture that is mostly a shot in the dark, but is based on rudimentary numerical simulations and on extrapolations from the parity game analysis.

Conjecture 5.3.6. Let G_n be the extended parity game, with $\widetilde{\omega}_c(G_n) = p$. Then there exists a deterministic strategy that succeeds in proportion p and in which a single player gives an answer that may depend on his input (so all but one player always output 0)!

CHAPTER 6

CONCLUSION

In this thesis, we presented a total of seven pseudo-telepathy games (eight if we distinguish the two equivalent games of sections 4.3 and 4.4). These games appear in the physics and quantum information processing literature; their unified presentation is the author's work.

In chapter 3, we gave formal definitions that describe the characteristics of the games, including a definition for a *promise-free* game, which is new. The two-party games of chapter 4 are: the impossible colouring game, the distributed Deutsch-Jozsa game, the magic square game, Cabello's game, and the matching game. It is shown that the magic square game and Cabello's game are equivalent; this is original work of the author.

The multi-party games of chapter 5 are: the Mermin-GHZ game, the parity game and the extended parity game. For the parity game, we have given exact values for the maximum success proportion and probability for classical players. These two results are original contributions. Also for the parity game, we have improved previous results by giving the exact detector efficiency rate required in the error-free model in order to close the detection loophole.

It is interesting to compare the various characteristics of the pseudo-telepathy games. Tables 6.1 and 6.2 compare the two-party pseudo-telepathy games and table 6.3 compares the multi-party pseudo-telepathy games.

With the help of pseudo-telepathy, we have confirmed the power of the quantum theory over its classical counterpart. The key to the success of the quantum players is one of the most mysterious and powerful resources of the quantum theory: entanglement.

name of the game	**Impossible Colouring Game**	**Distributed Deutsch-Jozsa Game**
input X	Let K_m be an augmented Kochen-Specker construction of dimension $m \geq 3$. $X_1 = \{(v_1, \dots v_m) \mid (v_1, \dots v_m)$ are orthonormal m-tuples in $K_m\}$ $X_2 = \{v_\ell \mid v_\ell \in K_m\}$	$X_1 = X_2 = \{0,1\}^{2^k}$
output Y	$Y_1 = \{1, 2, \dots, m\}$, $Y_2 = \{0,1\}$	$Y_1 = Y_2 = \{0,1\}^k$
promise P	$v_\ell \in \{v_1, \dots v_m\}$	$x_1 = x_2$ or $\Delta(x_1, x_2) = 2^{k-1}$
winning condition W	$y_1 = \ell \Leftrightarrow y_2 = 1$	$y_1 = y_2 \Leftrightarrow x_1 = x_2$
maximum classical success proportion $\widetilde{\omega}_c$	< 1	$\widetilde{\omega}_c = 1$ $(k = 1, 2, 3)$, $\widetilde{\omega}_c < 1$ ($k = 4$ and for all sufficiently large m)
maximum classical success probability ω_c	< 1	$\omega_c = 1$ $(k = 1, 2, 3)$, $\omega_c < 1$ ($k = 4$ and for all sufficiently large m)
shared entangled state $\lvert\psi\rangle$	$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \lvert jj\rangle$	$\frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} \lvert jj\rangle$

Table 6.1: Two-party games: comparison table part I

name of the game	**Magic Square Game**	**Matching Game**
input X	$X_1 = \{1, 2, 3\}$, $X_2 = \{1, 2, 3\}$	$X_1 = \{0,1\}^m$ (m even) $X_2 = \{M \mid M \in M_m\}$
output Y	$Y_1 = Y_2 = \{0,1\}^3$	$Y_1 = \{0,1\}^{\lceil \lg m \rceil}$ $Y_2 = \{\{a,b\} \mid \{a,b\} \in M\} \times \{0,1\}^{\lceil \lg m \rceil}$
promise P	none	none
winning condition W	$\sum_{i=1}^{3} r_i \equiv 0 \pmod 2$, $\sum_{i=1}^{3} c_i \equiv 1 \pmod 2$ $r_{x_2} = c_{x_1}$	$x_a \oplus x_b = (a \oplus b) \cdot (y_1 \oplus y_2)$
maximum classical success proportion $\widetilde{\omega}_c$	$\frac{8}{9}$	< 1 for all sufficiently large m
maximum classical success probability ω_c	$\frac{8}{9}$	< 1 for all sufficiently large m
shared entangled state $\|\psi\rangle$	$\frac{1}{2}(\|0011\rangle - \|0110\rangle - \|1001\rangle + \|1100\rangle)$	$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \|jj\rangle$

Table 6.2: Two-party games: comparison table part II

name of the game	**Parity Game** [1] $(n \geq 3)$	**Extended Parity Game** $(n \geq 3)$
input X	$X_i = \{0,1\}\ (i = 1 \ldots n)$	$X_i = \{0,1\}^\ell\ (i = 1 \ldots n)$, $\ell = \lceil \lg n \rceil - 1$
output Y	$Y_i = \{0,1\}\ (i = 1 \ldots n)$	$Y_i = \{0,1\}\ (i = 1 \ldots n)$
promise P	$\sum_{i=1}^n x_i \equiv 0 \pmod 2$	$\sum_{i=1}^n x_i \equiv 0 \pmod{2^\ell}$
winning condition W	$\sum_{i=1}^n y_i \equiv \frac{\sum_i^n x_i}{2} \pmod 2$	$\sum_{i=1}^n y_i \equiv \frac{\sum_{i=1}^n x_i}{2^\ell} \pmod 2$.
maximum classical success proportion, $\widetilde{\omega}_c$	$\frac{1}{2} + 2^{-\lceil n/2 \rceil}$	< 1
maximum classical success probability, ω_c	$\frac{1}{2} + 2^{-\lceil n/2 \rceil}$	< 1
maximum value of p, p^*	$\frac{1}{2} + 2^{\frac{2-3n}{2n}}$ (n even) ; $\frac{1}{2} + 2^{\frac{1-3n}{2n}}$ (n odd)	unknown
maximum value of η, η^*	$\frac{1}{2} \sqrt[n]{4}$	$\leq \frac{8}{n}$
shared entangled state $\|\psi\rangle$	$\frac{1}{\sqrt{2}} (\|0^n\rangle + \|1^n\rangle)$	$\frac{1}{\sqrt{2}} (\|0^n\rangle + \|1^n\rangle)$

Table 6.3: Multi-party games: comparison table

[1] The Mermin-GHZ game is obtained by setting $n = 3$.

6.1 Future Work

As research often goes, we have encountered more open questions along the way than we have been able to solve. Here is a partial list of tasks that are of interest:

- Where it has not already been done, find exact values of or good approximations for $\widetilde{\omega}_c(G)$, $\omega_c(G)$, $p_*(G)$ and $\eta_*(G)$, where G is a pseudo-telepathy game.
- Find new pseudo-telepathy games.
- Implement games experimentally.
- Prove conjectures 5.3.5 and 5.3.6 that concern the extended parity game.
- Prove that for the distributed Deutsch-Jozsa game (section 4.2), there is no classical winning strategy for all $k > 4$.
- Find a pseudo-telepathy game that satisfies any of the restrictions on W and P from section 3.2.1. Otherwise, show that none exists.
- Show that some games are equivalent, perhaps in a similar or a different way than section 4.5 ("The Magic Square and Cabello's Game Are Equivalent").
- Find minimum values of $|X_1|$ and $|X_2|$ for the impossible colouring game, in any dimension (section 4.1).
- The matching game of section 4.6 comes from a one-way communication complexity problem. Show how it is possible to transform other one-way communication complexity problems into pseudo-telepathy games. Find other links between one-way communication problems and pseudo-telepathy.
- Prove conjecture 4.6.3, i.e. that the matching game G^m is a pseudo-telepathy game for all even $m \geq 4$. Show that $\widetilde{\omega}_c(G^m)$ is close to $\frac{1}{2}$.

BIBLIOGRAPHY

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804–1807, 1982.

[AGR82] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities. *Physical Review Letters*, 49:91–94, 1982.

[Ara99] P. K. Aravind. Impossible colorings and Bell's theorem. *Physics Letters A*, 262(4-5):282–286, 1999.

[Ara02] P. K. Aravind. Bell's theorem without inequalities and only two distant observers. *Foundations of Physics Letters*, 15(4):397–405, 2002.

[Ara03] P. K. Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities, revised January 2003. Available as `arXiv:quant-ph/0206070`.

[BBT03] G. Brassard, A. Broadbent, and A. Tapp. Multi-party pseudo-telepathy. In F. Dehne, J. R. Sack, and M. Smid, editors, *Proceedings of the 8th International Workshop on Algorithms and Data Structures*, volume 2748 of *Lecture Notes in Computer Science*, pages 1–11, 2003.

[BBT04a] G. Brassard, A. Broadbent, and A. Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, to appear, 2004. Available as `arXiv:quant-ph/0407221`.

[BBT04b] G. Brassard, A. Broadbent, and A. Tapp. Recasting Mermin's multi-player game into the framework of pseudo-telepathy. *Manuscript*, August 2004. Available as `arXiv:quant-ph/0408052`.

[BCH$^+$02] J. Barrett, D. Collins, L. Hardy, A. Kent, and S. Popescu. Quantum nonlocality, Bell inequalities and the memory loophole. *Physical Review A*, 66(042111), 2002. Available as `arXiv:quant-ph/0105016`.

[BCT99] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1878, 1999.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 63–68, 1998.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.

[Bel66] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447–452, 1966.

[BHMR03] H. Buhrman, P. Høyer, S. Massar, and H. Röhrig. Combinatorics and quantum nonlocality. *Physical Review Letters*, 91(4):047903.1–047903.4, 2003.

[BK04] H. Buhrman and I. Kerenidis. Personal communication, January 2004.

[BM93] S. L. Braunstein and A. Mann. Noise in Mermin's n-particle Bell inequality. *Physical Review A*, 47, 1993.

[BMT04] G. Brassard, A. Méthot, and A. Tapp. Minimal state dimension for pseudo-telepathy. In preparation, 2004.

[Bra03] G. Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003.

[BYJK04] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Pro-*

ceedings of the 36th Annual ACM Symposium on Theory of Computing, pages 128–137, 2004.

[Cab01a] A. Cabello. "All versus nothing" inseparability for two observers. *Physical Review Letters*, 87(1):010403.1–010430.4, 2001.

[Cab01b] A. Cabello. Bell's theorem without inequalities and without probabilities for two observers. *Physical Review Letters*, 86(10):1911–1914, 2001.

[Cab04] A. Cabello. Personal communication, April 2004.

[CEGA96] A. Cabello, J. M. Estebaranz, and G. García-Alcaine. Bell-Kochen-Specker theorem: A proof with 18 vectors. *Physics Letters A*, 212:183–187, 1996.

[CHSH69] J. F. Clauser, M. A. Horner, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Conference on Computational Complexity (CCC)*, pages 236–249, 2004.

[CPZ+03] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, C. Brukner, and A. Zeilinger. All-versus-nothing violation of local realism for two entangled photons. *Physical Review Letters*, 90:160408.1–160408.4, 2003.

[DGG03] W. van Dam, R. D. Gill, and P. D. Grünwald. The statistical strength of nonlocality proofs, 2003. Available as `arXiv:quant-ph/0307125`.

[DJ92] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London, Series A*, 439:553–558, 1992.

[EBB71] A. Einstein, H. Born, and M. Born. *The Born-Einstein letters: correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955.* Walker, 1971.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[Fra85] J. D. Franson. Bell's theorem and delayed determinism. *Physical Review D*, 31:2529–2532, 1985.

[GHSZ90] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990.

[GHZ88] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Kluwer Academic Publishers, 1988.

[GJ83] I. P. Goulden and D. M. Jackson. *Combinatorial Enumeration.* John Wiley & Sons, 1983.

[Gle57] A. Gleason. Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics*, 6:885–893, 1957.

[Gou72] H. W. Gould. *Combinatorial Identities.* Morgantown, 1972.

[GW02] V. Galliard and S. Wolf. Pseudo-telepathy, entanglement and graph colorings. In *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, pages 101–101, 2002.

[GWT03] V. Galliard, S. Wolf, and A. Tapp. The impossibility of pseudotelepathy without quantum entanglement. In *Proceedings of IEEE In-*

ternational Symposium on Information Theory (ISIT), pages 457–457, 2003.

[GZ99] N. Gisin and H. Zbinden. Bell inequality and the locality loophole: Active versus passive switches. *Physics Letters A*, 264(2-3):103–107, 1999.

[HR83] P. Heywood and M. L. G. Redhead. Nonlocality and the Kochen-Specker paradox. *Foundations of Physics*, 13(5):481–499, 1983.

[Jam74] M. Jammer. *The Philosophy of Quantum Mechanics.* John Wiley & Sons, 1974.

[KS67] S. Kochen and E.P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967.

[MA99] J. E. Massad and P. K. Aravind. The Penrose dodecahedron revisited. *American Journal of Physics*, 67(7):631–638, 1999.

[Mas02] S. Massar. Nonlocality, closing the detection loophole, and communication complexity. *Physical Review A*, 65:032121.1–032121.5, 2002.

[Mer81a] N. D. Mermin. Bringing home the atomic world: Quantum mysteries for anybody. *American Journal of Physics*, 49:940–943, 1981.

[Mer81b] N. D. Mermin. Quantum mysteries for anyone. *Journal of Philosophy*, 78(10):397–408, 1981.

[Mer90a] N. D. Mermin. *Boojums all the way through.* Cambridge University Press, 1990.

[Mer90b] N. D. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838–1849, 1990.

[Mer90c] N. D. Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58(8):731–734, 1990.

[Mer90d] N. D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373–3376, 1990.

[Mer90e] N. D. Mermin. What's wrong with these elements of reality? *Physics Today*, 43:9–11, June 1990.

[MP03] S. Massar and S. Pironio. Violation of local realism versus detection efficiency. *Physical Review A*, 68:062109.1–062109.7, 2003.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[NM44] J. von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior.* Princeton University Press, 1944.

[Pea70] P. M. Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2:1418–1425, 1970.

[Per93] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 1993.

[Per00] A. Peres. Bayesian analysis of Bell inequalities. *Fortschritte der Physik*, 48(5-7):531–535, 2000.

[PRC91] C. Pagonis, M. L. G. Redhead, and R. K. Clifton. The breakdown of quantum non-locality in the classical limit. *Physics Letters A*, 155(8,9):441–444, 1991.

[RW04] R. Renner and S. Wolf. Quantum pseudo-telepathy and the Kochen-Specker theorem. In *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, pages 322–322, 2004.

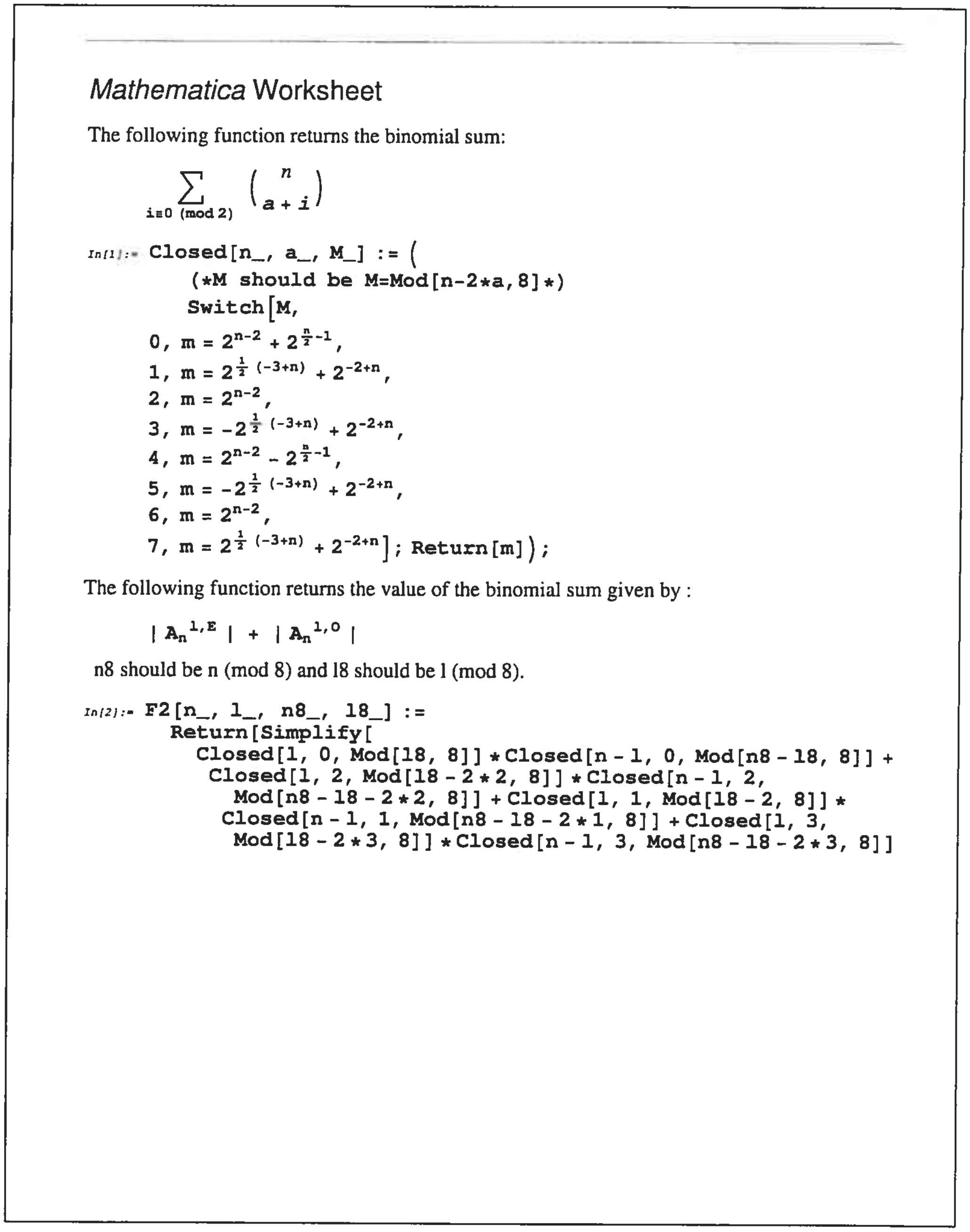
[Spe60] E. Specker. Die Logik nicht gleichzeitig entscheidbarer Aussagen. *Dialectica*, 14:239–246, 1960.

[Sta75] H. P. Stapp. Bell's theorem and world process. *Il Nuovo Cimento*, 29B(2):270–276, 1975.

[Sta83] A. Stairs. Quantum logic, realism, and value definiteness. *Philosophy of Science*, 50(4):578–602, 1983.

Appendix I

Proof of lemma 5.2.5



Mathematica Worksheet

The following function returns the binomial sum:

$$\sum_{i\equiv 0\ (\mathrm{mod}\ 2)} \binom{n}{a+i}$$

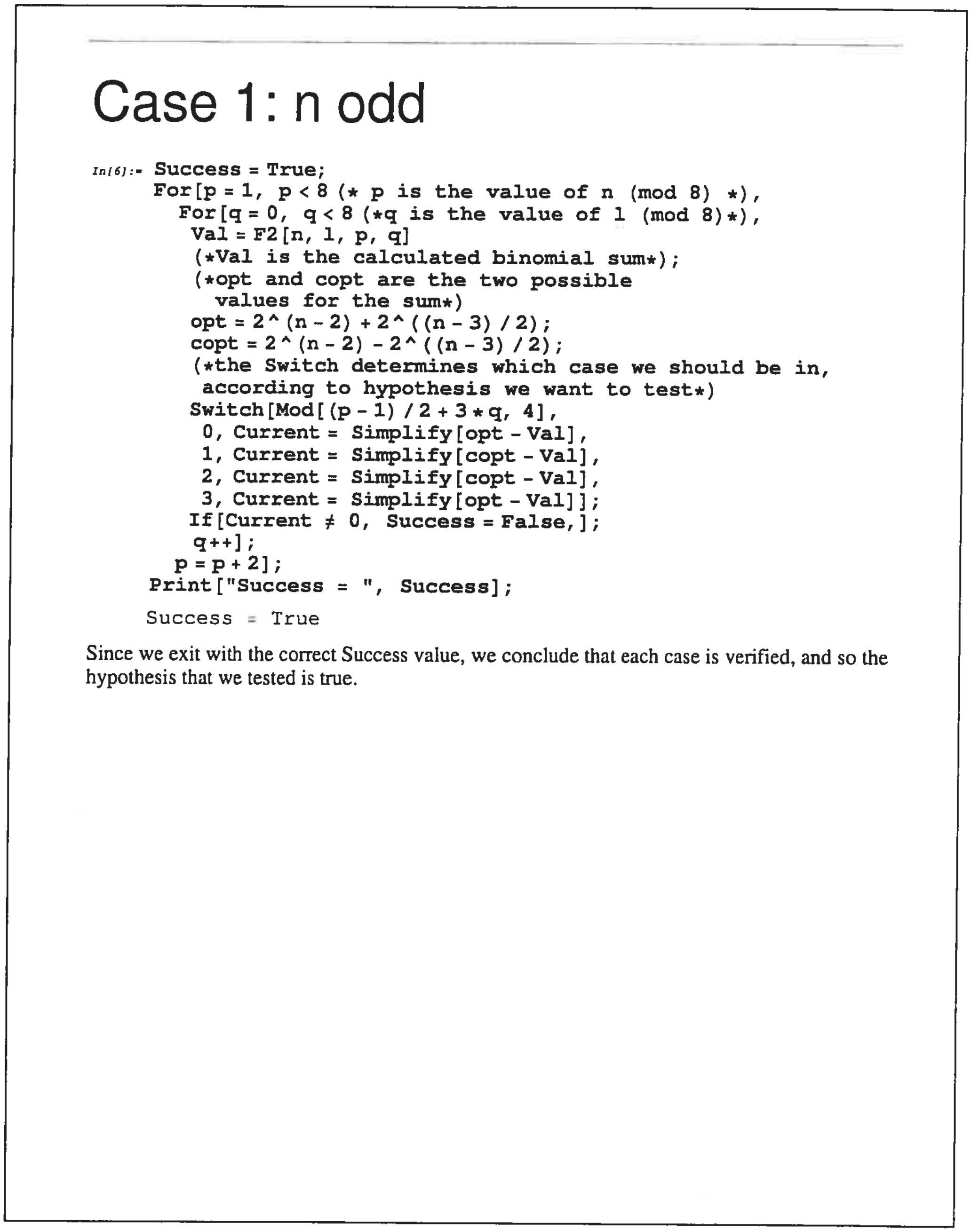
```
In[1]:= Closed[n_, a_, M_] := (
          (*M should be M=Mod[n-2*a,8]*)
          Switch[M,
        0, m = 2^(n-2) + 2^(n/2-1),
        1, m = 2^(1/2 (-3+n)) + 2^(-2+n),
        2, m = 2^(n-2),
        3, m = -2^(1/2 (-3+n)) + 2^(-2+n),
        4, m = 2^(n-2) - 2^(n/2-1),
        5, m = -2^(1/2 (-3+n)) + 2^(-2+n),
        6, m = 2^(n-2),
        7, m = 2^(1/2 (-3+n)) + 2^(-2+n)]; Return[m]);
```

The following function returns the value of the binomial sum given by :

$$| A_n{}^{1,E} | + | A_n{}^{1,O} |$$

n8 should be n (mod 8) and l8 should be l (mod 8).

```
In[2]:= F2[n_, l_, n8_, l8_] :=
          Return[Simplify[
            Closed[l, 0, Mod[l8, 8]] * Closed[n - l, 0, Mod[n8 - l8, 8]] +
             Closed[l, 2, Mod[l8 - 2 * 2, 8]] * Closed[n - l, 2,
               Mod[n8 - l8 - 2 * 2, 8]] + Closed[l, 1, Mod[l8 - 2, 8]] *
              Closed[n - l, 1, Mod[n8 - l8 - 2 * 1, 8]] + Closed[l, 3,
               Mod[l8 - 2 * 3, 8]] * Closed[n - l, 3, Mod[n8 - l8 - 2 * 3, 8]]
```

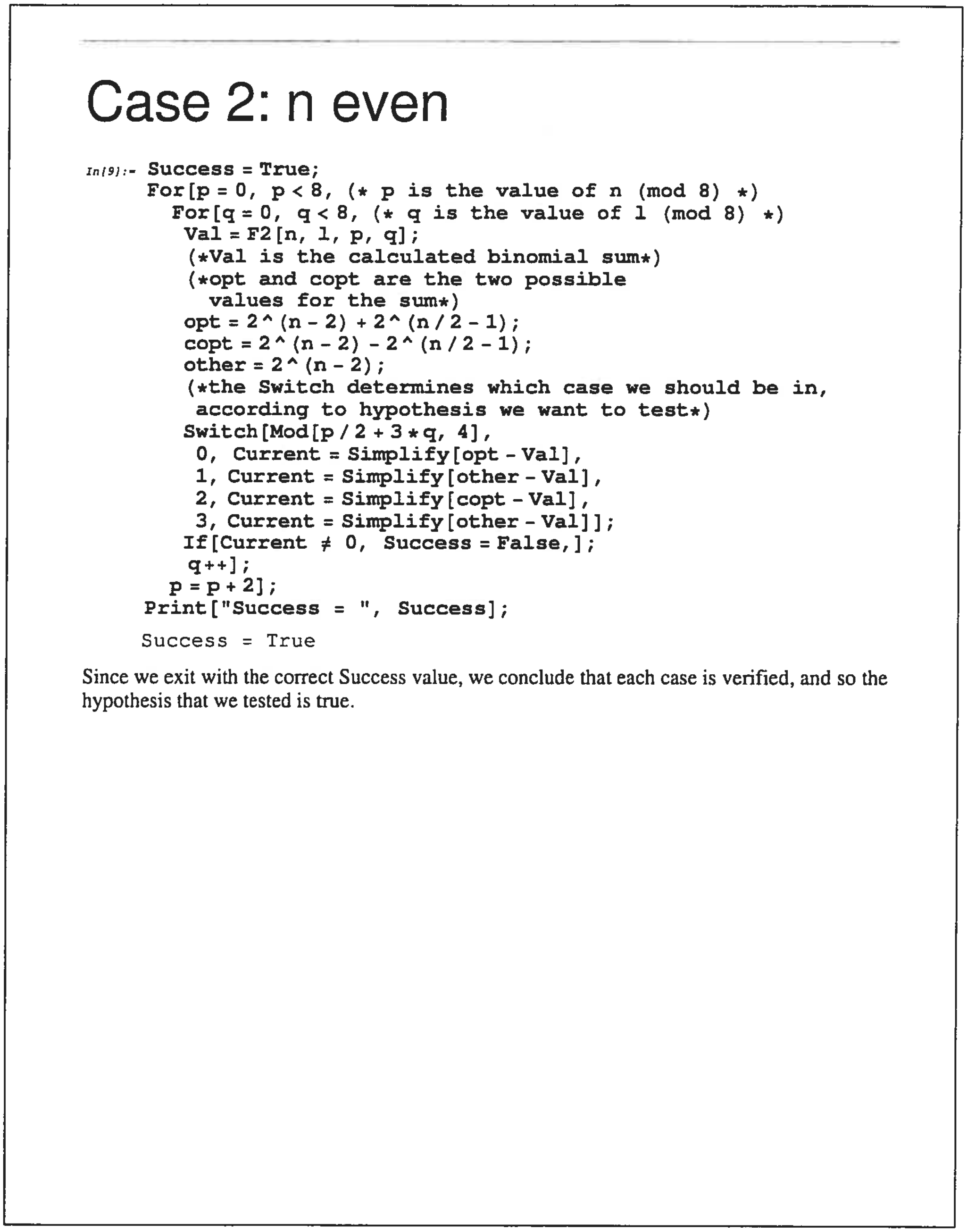


Case 1: n odd

```
In[6]:= Success = True;
     For[p = 1, p < 8 (* p is the value of n (mod 8) *),
       For[q = 0, q < 8 (*q is the value of l (mod 8)*),
        Val = F2[n, l, p, q]
        (*Val is the calculated binomial sum*);
        (*opt and copt are the two possible
          values for the sum*)
        opt = 2^(n - 2) + 2^((n - 3) / 2);
        copt = 2^(n - 2) - 2^((n - 3) / 2);
        (*the Switch determines which case we should be in,
         according to hypothesis we want to test*)
        Switch[Mod[(p - 1) / 2 + 3 * q, 4],
         0, Current = Simplify[opt - Val],
         1, Current = Simplify[copt - Val],
         2, Current = Simplify[copt - Val],
         3, Current = Simplify[opt - Val]];
        If[Current ≠ 0, Success = False,];
        q++];
      p = p + 2];
     Print["Success = ", Success];

     Success = True
```

Since we exit with the correct Success value, we conclude that each case is verified, and so the hypothesis that we tested is true.



Case 2: n even

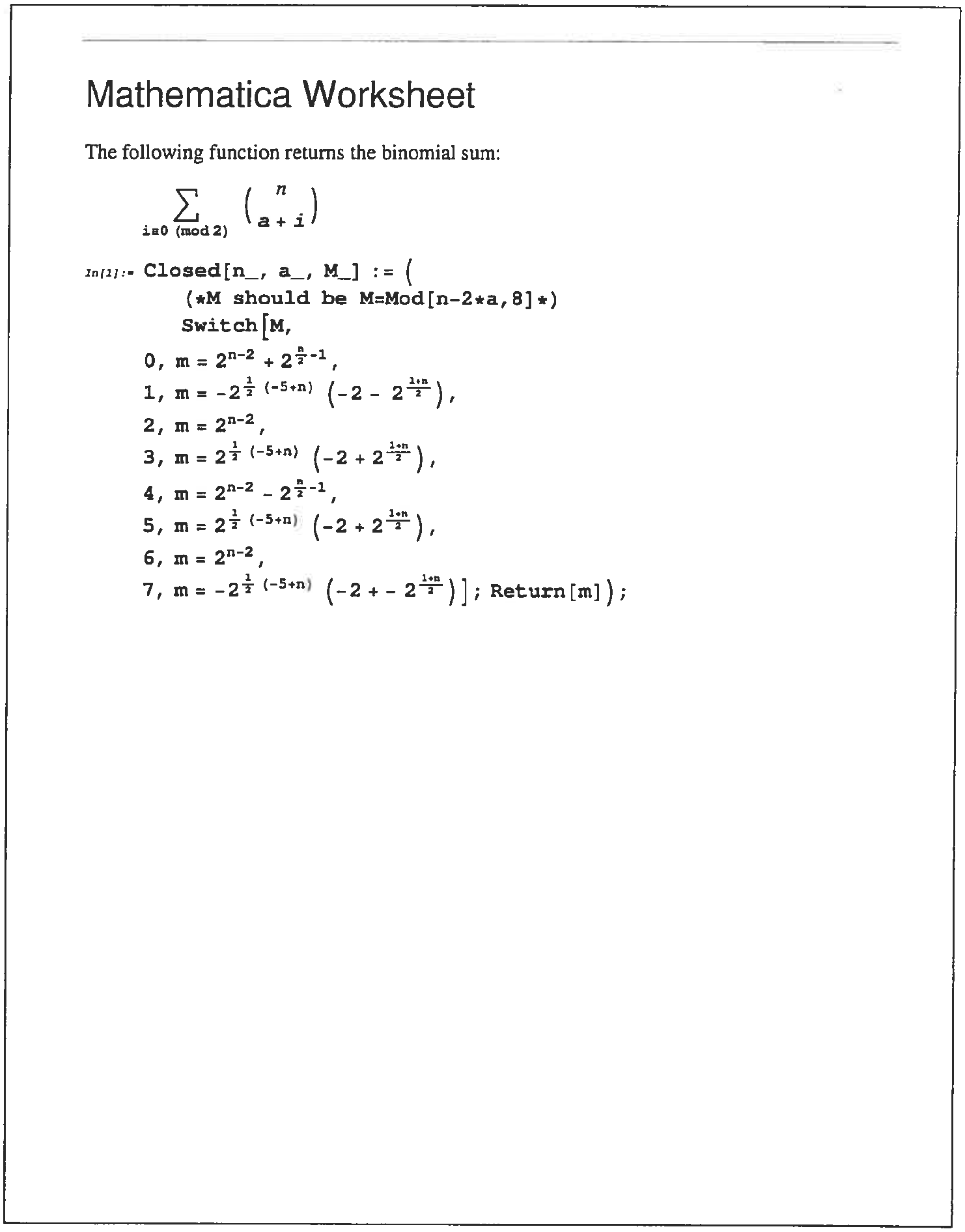
```
In[9]:= Success = True;
        For[p = 0, p < 8, (* p is the value of n (mod 8) *)
          For[q = 0, q < 8, (* q is the value of l (mod 8) *)
           Val = F2[n, l, p, q];
           (*Val is the calculated binomial sum*)
           (*opt and copt are the two possible
             values for the sum*)
           opt = 2^(n - 2) + 2^(n / 2 - 1);
           copt = 2^(n - 2) - 2^(n / 2 - 1);
           other = 2^(n - 2);
           (*the Switch determines which case we should be in,
            according to hypothesis we want to test*)
           Switch[Mod[p / 2 + 3 * q, 4],
            0, Current = Simplify[opt - Val],
            1, Current = Simplify[other - Val],
            2, Current = Simplify[copt - Val],
            3, Current = Simplify[other - Val]];
           If[Current ≠ 0, Success = False,];
           q++];
          p = p + 2];
        Print["Success = ", Success];

        Success = True
```

Since we exit with the correct Success value, we conclude that each case is verified, and so the hypothesis that we tested is true.

Appendix II

Proof of lemmas 5.2.12 and 5.2.13



Mathematica Worksheet

The following function returns the binomial sum:

$$\sum_{i\equiv 0\ (\mathrm{mod}\ 2)} \binom{n}{a+i}$$

In[1]:= Closed[n_, a_, M_] := (

    (*M should be M=Mod[n-2*a,8]*)

    Switch[M,

0, $m = 2^{n-2} + 2^{\frac{n}{2}-1}$,

1, $m = -2^{\frac{1}{2}(-5+n)} \left(-2 - 2^{\frac{1+n}{2}}\right)$,

2, $m = 2^{n-2}$,

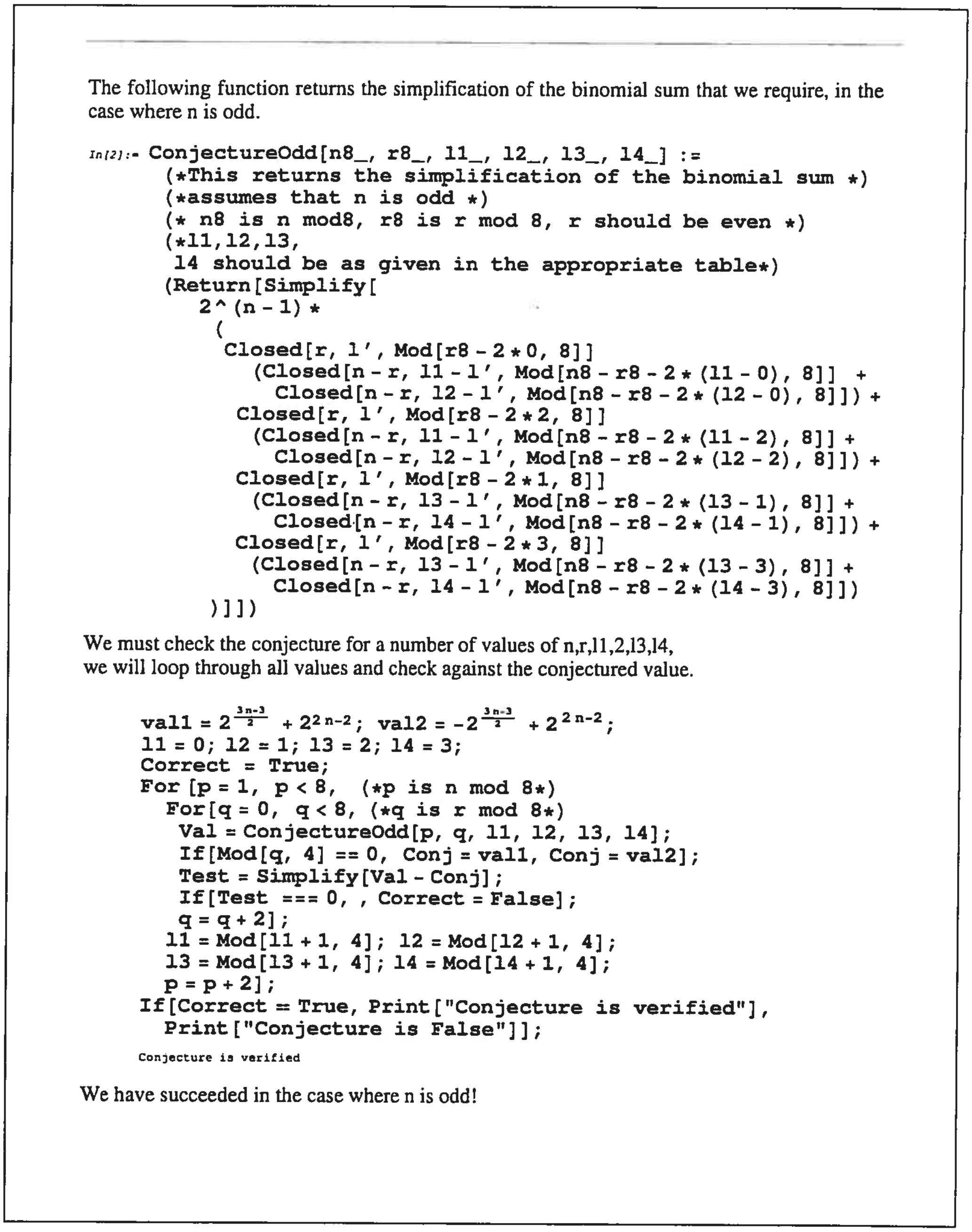
3, $m = 2^{\frac{1}{2}(-5+n)} \left(-2 + 2^{\frac{1+n}{2}}\right)$,

4, $m = 2^{n-2} - 2^{\frac{n}{2}-1}$,

5, $m = 2^{\frac{1}{2}(-5+n)} \left(-2 + 2^{\frac{1+n}{2}}\right)$,

6, $m = 2^{n-2}$,

7, $m = -2^{\frac{1}{2}(-5+n)} \left(-2 + - 2^{\frac{1+n}{2}}\right)$]; Return[m]);



The following function returns the simplification of the binomial sum that we require, in the case where n is odd.

```
In[2]:= ConjectureOdd[n8_, r8_, l1_, l2_, l3_, l4_] :=
      (*This returns the simplification of the binomial sum *)
      (*assumes that n is odd *)
      (* n8 is n mod8, r8 is r mod 8, r should be even *)
      (*l1,l2,l3,
       l4 should be as given in the appropriate table*)
      (Return[Simplify[
         2^(n - 1) *
          (
           Closed[r, 1', Mod[r8 - 2 * 0, 8]]
              (Closed[n - r, l1 - 1', Mod[n8 - r8 - 2 * (l1 - 0), 8]]  +
                Closed[n - r, l2 - 1', Mod[n8 - r8 - 2 * (l2 - 0), 8]]) +
            Closed[r, 1', Mod[r8 - 2 * 2, 8]]
             (Closed[n - r, l1 - 1', Mod[n8 - r8 - 2 * (l1 - 2), 8]] +
                Closed[n - r, l2 - 1', Mod[n8 - r8 - 2 * (l2 - 2), 8]]) +
            Closed[r, 1', Mod[r8 - 2 * 1, 8]]
             (Closed[n - r, l3 - 1', Mod[n8 - r8 - 2 * (l3 - 1), 8]] +
                Closed[n - r, l4 - 1', Mod[n8 - r8 - 2 * (l4 - 1), 8]]) +
            Closed[r, 1', Mod[r8 - 2 * 3, 8]]
             (Closed[n - r, l3 - 1', Mod[n8 - r8 - 2 * (l3 - 3), 8]] +
                Closed[n - r, l4 - 1', Mod[n8 - r8 - 2 * (l4 - 3), 8]])
          )]])
```

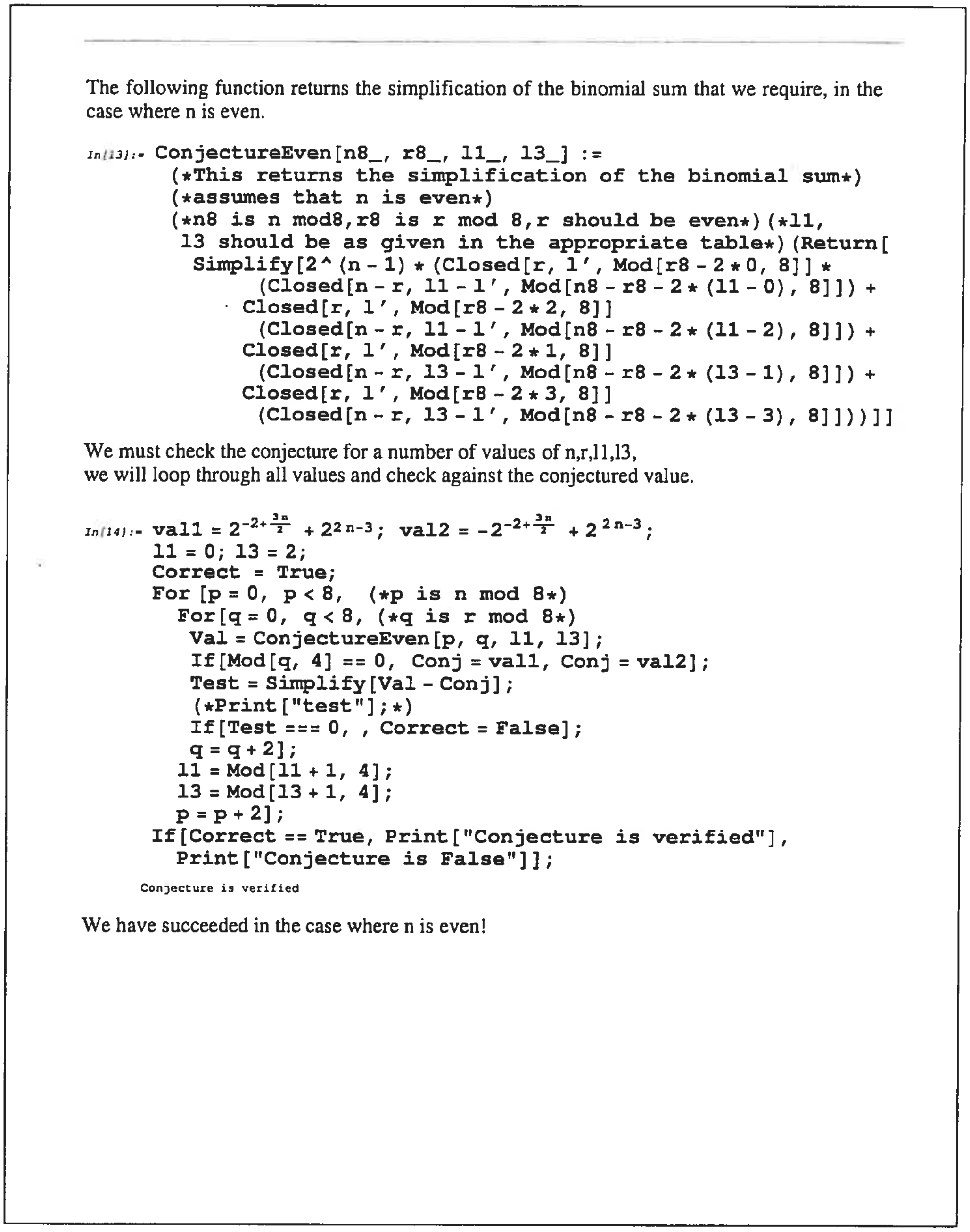
We must check the conjecture for a number of values of n,r,l1,2,l3,l4, we will loop through all values and check against the conjectured value.

$$\texttt{val1} = 2^{\frac{3n-3}{2}} + 2^{2n-2};\ \texttt{val2} = -2^{\frac{3n-3}{2}} + 2^{2n-2};$$

```
     l1 = 0; l2 = 1; l3 = 2; l4 = 3;
     Correct = True;
     For [p = 1, p < 8,  (*p is n mod 8*)
       For[q = 0,  q < 8, (*q is r mod 8*)
        Val = ConjectureOdd[p, q, l1, l2, l3, l4];
        If[Mod[q, 4] == 0, Conj = val1, Conj = val2];
        Test = Simplify[Val - Conj];
        If[Test === 0, , Correct = False];
        q = q + 2];
       l1 = Mod[l1 + 1, 4]; l2 = Mod[l2 + 1, 4];
       l3 = Mod[l3 + 1, 4]; l4 = Mod[l4 + 1, 4];
       p = p + 2];
     If[Correct = True, Print["Conjecture is verified"],
       Print["Conjecture is False"]];

     Conjecture is verified
```

We have succeeded in the case where n is odd!



The following function returns the simplification of the binomial sum that we require, in the case where n is even.

```
In[13]:= ConjectureEven[n8_, r8_, l1_, l3_] :=
           (*This returns the simplification of the binomial sum*)
           (*assumes that n is even*)
           (*n8 is n mod8,r8 is r mod 8,r should be even*)(*l1,
            l3 should be as given in the appropriate table*)(Return[
             Simplify[2^(n - 1) * (Closed[r, 1', Mod[r8 - 2 * 0, 8]] *
                  (Closed[n - r, l1 - 1', Mod[n8 - r8 - 2 * (l1 - 0), 8]]) +
                Closed[r, 1', Mod[r8 - 2 * 2, 8]]
                  (Closed[n - r, l1 - 1', Mod[n8 - r8 - 2 * (l1 - 2), 8]]) +
                Closed[r, 1', Mod[r8 - 2 * 1, 8]]
                  (Closed[n - r, l3 - 1', Mod[n8 - r8 - 2 * (l3 - 1), 8]]) +
                Closed[r, 1', Mod[r8 - 2 * 3, 8]]
                  (Closed[n - r, l3 - 1', Mod[n8 - r8 - 2 * (l3 - 3), 8]]))]]
```

We must check the conjecture for a number of values of n,r,l1,l3,
we will loop through all values and check against the conjectured value.

```
In[14]:= val1 = 2^(-2+3n/2) + 2^(2 n-3); val2 = -2^(-2+3n/2) + 2^(2 n-3);
         l1 = 0; l3 = 2;
         Correct = True;
         For [p = 0, p < 8,  (*p is n mod 8*)
           For[q = 0, q < 8, (*q is r mod 8*)
            Val = ConjectureEven[p, q, l1, l3];
            If[Mod[q, 4] == 0, Conj = val1, Conj = val2];
            Test = Simplify[Val - Conj];
            (*Print["test"];*)
            If[Test === 0, , Correct = False];
            q = q + 2];
           l1 = Mod[l1 + 1, 4];
           l3 = Mod[l3 + 1, 4];
           p = p + 2];
         If[Correct == True, Print["Conjecture is verified"],
           Print["Conjecture is False"]];

    Conjecture is verified
```

We have succeeded in the case where n is even!