Symmetric Extendability of Quantum States and the Extreme Limits of Quantum Key Distribution

by

Sumeet Khatri

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Science
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2016

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We investigate QKD protocols with two-way classical post-processing that are based on the well-known six-state and BB84 signal states. In these QKD protocols, the source (Alice) sends quantum signals to the receiver (Bob), who measures them, leaving only classical data on both sides. Our goal is to find the highest value of the quantum bit-error rate (QBER) Q for which two-way classical post-processing protocols on the data can distill secret keys. Using the BB84 signal states, such protocols currently exist for $Q < \frac{1}{5}$. On the other hand, for $Q \geq \frac{1}{4}$ no such protocol can exist as the observed data is compatible with an intercept-resend attack. This leaves the interesting question of whether successful two-way protocols exist in the interval $\frac{1}{5} \leq Q < \frac{1}{4}$. For the six-state signal states, the corresponding interval is known to be $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$.

We search for two-way protocols because it turns out that within these intervals Alice and Bob's correlations are symmetrically extendable, meaning that Bob and the eavesdropper (Eve) are completely indistinguishable from Alice's point of view, making any one-way Alice-to-Bob post-processing protocol insecure. A two-way protocol might be able to break the symmetry between Bob and Eve, and it must do so in order to distill a secret key because any two-way protocol will necessarily terminate with a one-way communication step, at which point the symmetric extendability of Alice and Bob's updated correlations must be checked again.

We first show that the search for two-way protocols breaking the symmetric extendability of Alice and Bob's correlations can be restricted to a search over post-selection protocols if all we care about is whether secret key can at all be distilled and not about the rate of distillation. We then provide strong analytical and numerical evidence to suggest that no two-way classical post-processing protocol exists within the gap when the six-state signal states are used.

Under quantum entanglement distillation protocols, it is known that secret key can be distilled right up to the intercept-resend bounds of $\frac{1}{4}$ and $\frac{1}{3}$ for the BB84 and six-state signal states, respectively. We therefore want to know whether classical post-processing protocols are just as good at distilling secret keys as quantum ones. Our results appear to indicate that they are not.

Acknowledgements

Firstly, I'd like to thank my supervisor Norbert Lütkenhaus for giving me the opportunity to join his Optical Quantum Communication Theory (OQCT) group and to work on this challenging project. His frequent availability and expertise allowed me to progress at a good pace and made working with him very enjoyable.

I would also like to thank all the other members of the OQCT group, past and present, for a wonderful two years: Patrick Coles, Filippo Miatto, Electra Eleftheriadou, Ryo Namiki, Yanbao Zhang, Dave Touchette, Michael Epping, Juan Miguel Arrazola, David Luong, Christian Mastromattei, Benjamin Lovitz, and Jie Lin. I would especially like to thank Juan Miguel Arrazola for his constant encouragement and helpful advice over the past two years.

I am thankful to Hubert Lin for his initial work on this project, which included writing several important `MATLAB` functions and providing preliminary numerical results. I am also grateful for the `MATLAB` code written by Toby Cubitt [Cub] and Nathaniel Johnston [Joh16].

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

The amount of secret key that can be distilled from a quantum key distribution (QKD) protocol is a function of the amount of noise in the channel linking the two parties, Alice and Bob, wishing to establish the secret key in the presence of an eavesdropper, Eve. The amount of noise, as well as the statistics of the resulting measurements performed by Alice and Bob on their physical systems, can be described by a quantum state ρ^{AB}. QKD protocols based on the well-known BB84 [BB84] and six-state [Bru98; BG99] signal states, for example, proceed with Alice sending signals through a quantum channel to Bob, who measures them, leaving both Alice and Bob with classical data. They sacrifice some of their data to estimate a state ρ^{AB} that is consistent with their data. They then decide whether or not the state is too noisy to proceed to distilling a secret key using some classical post-processing protocols, typically error-correction and privacy amplification.

It was proved in Moroder et al. [MCL06] that if ρ^{AB} is symmetrically extendable to a copy of B then it cannot be used to distill a secret key by one-way classical post-processing protocols involving communication from Alice to Bob. The state ρ^{AB} is called *symmetrically extendable to a copy of B* if there exists a tripartite state $\rho^{ABB'}$ such that its marginal density matrices satisfy $\rho^{AB'} = \rho^{AB}$. The system B' is effectively a copy of B, which means that if Alice tries to establish a secret key with Bob by communicating to him, and the system B' is in Eve's possession, then Eve will be just as knowledgeable as Bob is about the key Alice is trying to create, rendering it insecure. Symmetric extendability of ρ^{AB}, therefore, places a fundamental limit on the noise tolerance of QKD protocols under one-way classical post-processing. (Error-correction and privacy amplification, for example, are one-way classical post-processing protocols.) For QKD protocols using the BB84 and six-state signal states in which the noise is characterized by a single quantity called the *quantum bit-error rate (QBER) Q*, it is known from [MCL06] that the corresponding state ρ_Q^{AB} corresponding to Alice and Bob's correlations is symmetrically extendable for all $Q \geq \frac{2-\sqrt{2}}{4} \approx 14.6\%$ when the BB84 signal states are used and for all $Q \geq \frac{1}{6} \approx 16.6\%$ when the six-state signal states are used.

Gottesman and Lo [GL03], however, established that Alice and Bob can still create a secret key beyond these values if they execute a *two-way* post-processing protocol, and that they can do so up to $Q = 18.9\%$ with the BB84 signal states and up to $Q = 26.4\%$ with the six-state signal states. Chau [Cha02] improved the Gottesman-Lo protocol to increase the threshold up to the current values of 20% for the BB84 signal states and $\frac{5-\sqrt{5}}{10} \approx 27.6\%$ for the six-state signal states; see Figure 1.1. Later, Acin et al. [Ací+06] and Bae and Acin [BA07] proved that secret key cannot be distilled beyond the Chau bounds using the two-way *advantage distillation* protocol [Mau93] before error-correction and privacy amplification since in such cases there is an eavesdropping attack that compromises the security of the key. Advantage distillation is a purely classical post-selection protocol acting on blocks of data defined as follows: for each block of Alice and Bob's data of

some pre-defined size,

1. Alice checks if her block of data is one of the strings $00\cdots00$ or $11\cdots11$, telling Bob "yes" or "no" (but not the string she has);
2. Bob similarly checks if his data is one of the strings $00\cdots00$ or $11\cdots11$, telling Alice "yes" or "no".

If both Alice and Bob announce "yes", then they keep the first bit of the string they obtained and move to the next block; if not, then they both discard the entire block and move the next block. Note that advantage distillation is a two-way protocol. Its goal, intuitively, is to reduce Eve's information about Alice and Bob's data by only retaining data on which Alice and Bob are highly correlated and discarding the rest. Myhr et al. [Myh+09] showed that the current bounds obtained from advantage distillation correspond precisely to the symmetric extendability bounds of the effective quantum state after it. In other words, advantage distillation is able to "break" the symmetric extendability of Alice and Bob's correlations beyond the one-way upper bounds up to the current bounds, but not beyond them.

Now, it is known that neither a one-way nor a two-way protocol can be used to distill a secret key whenever the channel linking Alice and Bob is entanglement-breaking [CLL04] (see also [AMG03; AG05]). This fact is often stated as Eve performing an intercept-resend attack. As indicated in Figure 1.1 below, this means that for the BB84 and six-state signal states secret key cannot be distilled beyond $Q = \frac{1}{4}$ and $Q = \frac{1}{3}$, respectively. This leaves the question of whether there exists a two-way classical post-processing protocol allowing secret key to be distilled in the yellow interval $\frac{1}{5} \leq Q < \frac{1}{4}$ with the BB84 signal states and $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$ with the six-state signal states. The goal of this thesis is to try to answer this question.

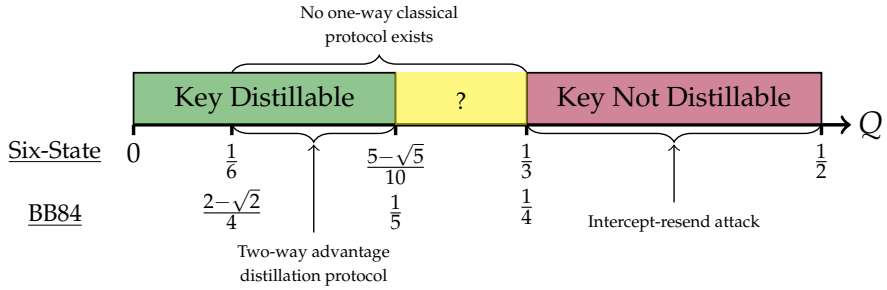


Figure 1.1: Key distillability by classical post-processing as a function of the QBER Q for QKD with the BB84 and six-state signal states. The ability to distill secret key in the yellow region is the subject of this thesis.

The fact that symmetric extendability prevents secret key distillation by one-way classical post-processing is crucial in the quest for a two-way protocol since any two-way protocol must eventually terminate with a one-way communication step. Since the state ρ_Q^{AB} is initially symmetrically extendable for all Q in the yellow region, any successful two-way post-processing protocol must "break" the symmetric extendability of ρ_Q^{AB} before the final round of one-way communication.

The yellow region of Figure 1.1 currently represents a *gap* between classical post-processing protocols (acting on data arising from measurement of quantum states) and quantum post-processing protocols operating on the quantum states themselves. It is known that as long as the state ρ^{AB} is entangled, Alice and Bob can execute the (quantum) entanglement distillation protocol to distill a secret key. (See [Ben+96b; Ben+96a] for

a full description of entanglement distillation and [BB85; Deu+96] for a related protocol called quantum privacy amplification and its application to QKD.) This means that, using the BB84 and six-state signal states, respectively, secret key can be distilled for all $0 \leq Q < \frac{1}{4}$ and $0 \leq Q < \frac{1}{3}$. If there does exist a two-way classical post-processing protocol that can be used to distill a key within the gap, then we will have that classical protocols are just as good as quantum protocols for QKD, while if there does not exist a successful two-way protocol within the gap then there is an advantage to performing quantum post-processing. In particular, the latter would imply the existence of "bound information"—the classical analogue of bound entanglement[1]—which is classical information that contains secret correlations but from which no secret key can be distilled; see [GW00; GRW01; GRW02; CP02; RW03; AG05] for more information. A previous comparison between classical and quantum post-processing protocols has been done in [GW99; Bru+03] for a more restricted class of eavesdropping attacks than those considered here[2] in which it was found that classical and quantum protocols do equally well for distilling secret keys.

This thesis provides strong evidence, consisting of analytical and numerical results, to believe that there does *not* exist a two-way post-processing protocol that can be used to distill a secret key within the gap. We do this by first reducing the search for two-way protocols that might break the symmetric extendability of ρ_Q^{AB} to protocols involving only one round of independent post-selection by Alice and Bob on a block of their data. We then analyze the symmetric extendability of the post-selected states both analytically and numerically over many classes of post-selection. This leads to updated threshold QBERs beyond which secret key cannot be distilled. We show that for the post-selection classes tested none of these updated thresholds are inside the gap.

1.1 Outline of the Thesis & Summary of Results

Chapter 2: Background

We start with a brief review of the mathematics of linear operators on finite-dimensional Hilbert spaces and maps between them, particularly completely-positive maps and channels. We then proceed to a brief review of quantum states. The end of the chapter is devoted to a general review of QKD, with particular emphasis on protocols using the six-state and BB84 signal states. For these two types of protocols, we use symmetric extendability to prove that one-way classical post-processing protocols cannot be used to distill a secret key for QBER beyond $\frac{1}{6}$ with the six-state signal states and beyond $\frac{2-\sqrt{2}}{4}$ with the BB84 signal states.

Chapter 3: Symmetrically Extendable States

In this chapter, we define the notion of symmetric extendability of a bipartite quantum state and formulate the existence of symmetrically extendable states as a semi-definite programming (SDP) problem. We also consider the problem of explicitly constructing symmetric extensions of symmetrically extendable states, providing one simple possible method of constructing a symmetric extension.

[1] Bound entangled states are entangled states that have zero distillable entanglement. See [Hor97; HHH98], where they were first discussed.

[2] Those works considered only *individual* eavesdropping attacks, while the results in this thesis will hold for completely general eavesdropping attacks. See §2.4.1 for details.

Chapter 4: Two-Way Protocols and Breaking Symmetric Extendability

In this chapter, we begin our search for two-way post-processing protocols that can break the symmetric extendability of Alice and Bob's correlations for QBER within the gap. Since we are only concerned with whether or not key can be distilled within the gap and not with the rate of key distillation, we manage to restrict our search of protocols to those in which Alice and Bob merely perform an independent post-selection on blocks of their data according to some classical error-correcting codes. We define the effective quantum state after this post-selection, and use properties of these states to reduce the search of protocols even further by identifying codes that give rise to the same effective state. By doing a numerical search, we are able to determine all the inequivalent codes for small code sizes and block lengths.

At the end of the chapter, we look at some important ways of combining codes to obtain new ones and examine the effect such combining has on the effective quantum states.

Chapter 5: Repetition Codes

In this chapter, we examine the symmetric extendability of the effective quantum states arising after post-selection on repetition codes. The protocol defined by this post-selection is the advantage distillation protocol that currently provides the best bounds on key distillability with two-way post-processing for both the six-state and BB84 signal states. We use the result in [Che+14] to re-derive these bounds by analytically determining the symmetric extendability of the effective states. We also use the special method of Chapter 3 to provide an explicit construction of a symmetric extension of the states within the entire symmetric extendability region.

Chapter 6: Simplex Codes

The repetition codes generalize naturally to simplex codes, which are codes in which the Hamming distance between any two distinct codewords is a constant. In this chapter, we examine the symmetric extendability of the effective states arising after post-selection on these codes, using the result of [Ran09] to prove that they cannot do better than repetition codes, hence proving that they cannot be used to break the symmetric extendability of the original state within the gap. As in the previous chapter, we use the special method of Chapter 3 to provide an explicit construction of a symmetric extension of the effective state within the entire symmetric extendability region.

Chapter 7: Testing the Special Map

In this chapter, we show the results of applying the special method of constructing symmetric extensions defined in Chapter 3 to over 540,000 randomly-selected codes of varying sizes and block lengths. All of these tested codes are found to be symmetrically extendable within the gap. We indicate all those codes for which the corresponding states are symmetrically extendable but whose symmetric extension could not be constructed using the special method. In particular, we discover that there exist symmetrically extendable states arising from post-selection on (linear) Reed-Muller codes whose symmetric extension cannot be constructed using the special method.

The results of this chapter give very strong evidence that there does not exist a two-way classical post-processing protocol that can distill a secret key within the gap.

Chapter 8: Numerical Estimation of Thresholds

In this final chapter, we show the results of our numerical estimation of the threshold errors for the inequivalent codes determined in Chapter 4. These threshold errors have distinctive trends as functions of the code size and block length, all of which strengthen our belief that two-way post-processing protocols distilling a secret key within the gap do not exist.

Chapter 2

Background

We first review some background material needed for the main part of the thesis. The first section on linear operators will review the definitions needed and will establish notational conventions. After brief reviews of quantum channels and quantum states, we will review QKD with the six-state and BB84 signal states and will derive the QBER upper bounds for one-way classical post-processing and for intercept-resend attacks.

2.1 Linear Operators

The main reference for this section is [Wat16]. All details pertaining to definitions and theorems, and proofs of theorems, may be found there.

Throughout this thesis, we consider linear operators on finite-dimensional complex vector spaces endowed with the Euclidean inner product, called *complex Euclidean spaces* for short. We will use $\mathfrak{H}, \mathfrak{K}$, etc. to refer to such spaces and $d_{\mathfrak{H}}$, $d_{\mathfrak{K}}$, etc. to refer to their dimension. All such spaces are isomorphic to the Hilbert space $\mathbb{C}^d$, where d is the dimension, so that the Euclidean inner product can be written as

$$\langle \psi | \phi \rangle = \sum_{i=1}^{d} \overline{\psi_i} \phi_i \quad \forall\, \psi, \phi \in \mathbb{C}^d, \tag{2.1}$$

where $\overline{\psi_i}$ refers to the complex conjugate of the components $\psi_i \in \mathbb{C}$ of ψ. When dealing with tensor-product spaces, we will sometimes use subscripts to distinguish the tensor factors, for example, $\mathfrak{H}_A \otimes \mathfrak{H}_B$, which will sometimes be abbreviated as $\mathfrak{H}_{AB}$. In such cases, we will quite often refer to the constituent spaces simply by their subscripts and write, for example, $|\psi\rangle^{AB}$ or $|\psi\rangle_{AB}$, to indicate that $|\psi\rangle \in \mathfrak{H}_A \otimes \mathfrak{H}_B$. The set $\{|i\rangle^A\}_{i=0}^{d_A-1} \subset \mathfrak{H}_A$ satisfying $\langle i|j\rangle = \delta_{i,j}$ for all $0 \leq i, j \leq d_A - 1$ will be called the *standard (orthonormal) basis* of $\mathfrak{H}_A$. For tensor product spaces, we will use the abbreviation $|i,j\rangle^{AB} \equiv |i\rangle^A \otimes |j\rangle^B$ for the elements of the standard basis.

The set of all *linear operators* between $\mathfrak{H}$ and $\mathfrak{K}$ is denoted $\mathrm{L}(\mathfrak{H}, \mathfrak{K})$. We will use the abbreviation $\mathrm{L}(\mathfrak{H}) \equiv \mathrm{L}(\mathfrak{H}, \mathfrak{H})$. For linear operators $X \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$, we will sometimes write X^{AB} or X_{AB}, that is, with the tensor factor labels as a superscript or a subscript, if the space on which the operator acts is important. Every operator $X \in \mathrm{L}(\mathfrak{H}, \mathfrak{K})$ can be associated with a matrix whose entry in row i and column j, denoted $X_{\substack{i \\ j}}$, is defined as

$$X_{\substack{i \\ j}} = \langle i | X | j \rangle \quad \forall\, 0 \leq i \leq d_{\mathfrak{K}} - 1,\ \ 0 \leq j \leq d_{\mathfrak{H}} - 1.$$

$\mathrm{L}(\mathfrak{H}, \mathfrak{K})$ is spanned by $\{|i\rangle\langle j| : 0 \leq i \leq d_{\mathfrak{K}} - 1,\ 0 \leq j \leq d_{\mathfrak{H}} - 1\}$, so for any $A \in \mathrm{L}(\mathfrak{H}, \mathfrak{K})$ we will very often write

$$X = \sum_{i=0}^{d_{\mathfrak{K}}-1} \sum_{j=0}^{d_{\mathfrak{H}}-1} X_{\substack{i \\ j}} |i\rangle\langle j| .$$

For every $X \in \mathrm{L}(\mathfrak{H}, \mathfrak{K})$:

1. $\overline{X} \in \mathrm{L}(\mathfrak{H}, \mathfrak{K})$ is called the *entry-wise complex conjugate* of A and is defined as

$$(\overline{X})_{\substack{i \\ j}} = \overline{X_{\substack{i \\ j}}} \quad \forall\, 0 \leq i \leq d_{\mathfrak{K}} - 1,\ \ 0 \leq j \leq d_{\mathfrak{H}} - 1;$$

2. $X^{\mathsf{T}} \in \mathrm{L}(\mathfrak{K}, \mathfrak{H})$ is called the *transpose* of X and is defined as

$$(X^{\mathsf{T}})_{\substack{i \\ j}} = X_{\substack{j \\ i}} \quad \forall\, 0 \leq i \leq d_{\mathfrak{H}} - 1,\ \ 0 \leq j \leq d_{\mathfrak{K}} - 1;$$

3. $X^{\dagger} \in \mathrm{L}(\mathfrak{K}, \mathfrak{H})$ is called the *adjoint*, *Hermitian conjugate*, or *conjugate transpose* of A and is defined as

$$X^{\dagger} = \overline{X^{\mathsf{T}}} = \overline{X}^{\mathsf{T}}.$$

Definition 2.1 Classes of Linear Operators

For any complex Euclidean space $\mathfrak{H}$, we define the following subsets of $\mathrm{L}(\mathfrak{H})$:

1. *Normal Operators*: $\{X \in \mathrm{L}(\mathfrak{H}) : XX^{\dagger} = X^{\dagger}X\}$.
2. *Hermitian Operators*: $\mathrm{Herm}(\mathfrak{H}) = \{X \in \mathrm{L}(\mathfrak{H}) : X^{\dagger} = X\}$.
3. *Positive Semi-Definite Operators*: $\mathrm{Pos}(\mathfrak{H}) = \{X \in \mathrm{L}(\mathfrak{H}) : X = Y^{\dagger}Y,\ Y \in \mathrm{L}(\mathfrak{H})\}$.
4. *Density Operators*: $\mathrm{D}(\mathfrak{H}) = \{P \in \mathrm{Pos}(\mathfrak{H}) : \mathrm{Tr}(P) = 1\}$.
5. *Isometric Operators*: $\mathrm{U}(\mathfrak{H}, \mathfrak{K}) = \{V \in \mathrm{L}(\mathfrak{H}, \mathfrak{K}) : V^{\dagger}V = \mathbb{1}_{\mathfrak{H}}\}$. This includes the set $\mathrm{U}(\mathfrak{H}) := \mathrm{U}(\mathfrak{H}, \mathfrak{H})$ of all unitary operators on $\mathfrak{H}$, which are invertible and satisfy $UU^{\dagger} = \mathbb{1}_{\mathfrak{H}}$ in addition to $U^{\dagger}U = \mathbb{1}_{\mathfrak{H}}$.

Definition 2.2 The vec Map

For any $\mathfrak{H}, \mathfrak{K}$, the map $\mathrm{vec} : \mathrm{L}(\mathfrak{K}, \mathfrak{H}) \to \mathfrak{H} \otimes \mathfrak{K}$ is defined by

$$\mathrm{vec}\left(|i\rangle\langle j|\right) = |i\rangle \otimes |j\rangle \quad \forall\, 0 \leq i \leq d_{\mathfrak{H}} - 1,\ \ 0 \leq j \leq d_{\mathfrak{K}} - 1. \tag{2.2}$$

The map vec is an isomorphism between the vector spaces $\mathrm{L}(\mathfrak{K}, \mathfrak{H})$ and $\mathfrak{H} \otimes \mathfrak{K}$ and it will be used repeatedly throughout the thesis. The following identity will be particularly useful:

$$\mathrm{Tr}_{\mathfrak{K}}(\mathrm{vec}(X)\mathrm{vec}(Y)^{\dagger}) = XY^{\dagger} \quad \forall\, X, Y \in \mathrm{L}(\mathfrak{K}, \mathfrak{H}). \tag{2.3}$$

Theorem 2.3 Spectral Theorem

For any normal operator $X \in \mathrm{L}(\mathfrak{H})$ there exists a unique collection of complex numbers $\lambda_0, \ldots, \lambda_{d_{\mathfrak{H}}-1} \in \mathbb{C}$ and an orthonormal basis $\{|v_0\rangle, |v_2\rangle, \ldots, |v_{d_{\mathfrak{H}}-1}\rangle\}$ of $\mathfrak{H}$ such that

$$X = \sum_{k=0}^{d_{\mathfrak{H}}-1} \lambda_k |v_k\rangle \langle v_k| . \tag{2.4}$$

The numbers $\lambda_0, \ldots, \lambda_{d_{\mathfrak{H}}-1}$ are called the *eigenvalues* of X. They are defined by the condition $X|v_k\rangle = \lambda_k |v_k\rangle$ for all $0 \leq k \leq d_{\mathfrak{H}} - 1$, where $\{|v_k\rangle\}_{k=0}^{d_{\mathfrak{H}}-1}$ are the associated *eigenvectors* of X. The set of all eigenvalues (in which each eigenvalue may appear more than once according to its multiplicity) is called the *spectrum* of X, denoted $\mathrm{spec}(X)$. The number of non-zero elements in $\mathrm{spec}(X)$ is called the *rank* of X.

The *trace* of X, defined as the sum $\mathrm{Tr}(X) = \sum_{i=0}^{d_{\mathfrak{H}}-1} X_{\substack{i \\ i}}$, can be written as $\mathrm{Tr}(X) = \sum_{\lambda \in \mathrm{spec}(X)} \lambda$. The *determinant* of X can be written as $\det(X) = \prod_{\lambda \in \mathrm{spec}(X)} \lambda$.

The spectral theorem can be used to prove the following important fact that will be used repeatedly throughout the thesis.

Theorem 2.4

An operator $P \in \mathrm{L}(\mathfrak{H})$ is positive semi-definite if and only if every eigenvalue of P is non-negative.

For $P \in \mathrm{Herm}(\mathfrak{H})$, we will write $P \geq 0$ or $0 \leq P$ to indicate that P is positive semi-definite. More generally, for $X, Y \in \mathrm{Herm}(\mathfrak{H})$, we will write $X \geq Y$ or $Y \leq X$ to indicate that $X - Y \in \mathrm{Pos}(\mathfrak{H})$.

By definition, $P \in \mathrm{Pos}(\mathfrak{H})$ if and only if $P = B^\dagger B$ for some $B \in \mathrm{L}(\mathfrak{H})$. In fact, for every $P \in \mathrm{Pos}(\mathfrak{H})$ there exists a unique $R \in \mathrm{Pos}(\mathfrak{H})$ such that $P = R^2$ [Bha07]. Such an operator R is called the *square root* of P and we will write it as $R = \sqrt{P}$. Given the spectral decomposition

$$P = \sum_{k=0}^{d_{\mathfrak{H}}-1} \lambda_k |v_k\rangle \langle v_k|$$

of P, it holds that

$$\sqrt{P} = \sum_{k=0}^{d_{\mathfrak{H}}-1} \sqrt{\lambda_k} |v_k\rangle \langle v_k| . \tag{2.5}$$

The set of linear maps $\Lambda : \mathrm{L}(\mathfrak{H}) \to \mathrm{L}(\mathfrak{K})$ will be denoted $\mathrm{T}(\mathfrak{H}, \mathfrak{K})$ and is sometimes called the set of *superoperators*. We will use the abbreviation $\mathrm{T}(\mathfrak{H}) \equiv \mathrm{T}(\mathfrak{H}, \mathfrak{H})$.

Definition 2.5 Important Subsets of $\mathrm{T}(\mathfrak{H}, \mathfrak{K})$

For any two complex Euclidean spaces $\mathfrak{H}, \mathfrak{K}$, we define the following subsets of $\mathrm{T}(\mathfrak{H}, \mathfrak{K})$.

1. *Positive maps*: Maps for which $\Lambda(P) \in \mathrm{Pos}(\mathfrak{K})$ for all $P \in \mathrm{Pos}(\mathfrak{H})$.
2. *Completely-positive maps*: Maps for which $\mathbb{1}_{\mathrm{L}(\mathbb{C}^d)} \otimes \Lambda$ is positive for all $d \geq 1$. The set of all completely-positive maps is denoted $\mathrm{CP}(\mathfrak{H}, \mathfrak{K})$.
3. *Trace-preserving maps*: Maps for which $\mathrm{Tr}(\Lambda(X)) = \mathrm{Tr}(X)$ for all $X \in \mathrm{L}(\mathfrak{H})$.

An important example of a map in $\mathrm{T}(\mathfrak{H}_A \otimes \mathfrak{H}_B, \mathfrak{H}_B)$ is Tr_A, called the *partial trace (over A)*. It is defined as

$$\mathrm{Tr}_A = \mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathfrak{H}_B)}, \tag{2.6}$$

and it is the unique map satisfying the equation

$$\mathrm{Tr}_A[X \otimes Y] = \mathrm{Tr}(X)Y \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A),\ \ Y \in \mathrm{L}(\mathfrak{H}_B).$$

The partial trace over B, denoted Tr_B, is defined analogously to Tr_A. The partial trace is trace-preserving, which can be easily checked. It also happens to be completely-positive, though this is not obvious. For any operator $X^{AB} \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$, we will often write X^A to mean $\mathrm{Tr}_B(X^{AB})$. Similarly, X^B will refer to $\mathrm{Tr}_A(X^{AB})$.

Another important example, this time in $\mathrm{T}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$, is T_A, called the *partial transpose (on A)*, and it is defined as

$$\mathrm{T}_A(X) = X^{\mathsf{T}_A} \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B), \tag{2.7}$$

where by definition

$$\left(X^{\mathsf{T}_A}\right)_{\substack{i,j\\k,\ell}} = X_{\substack{k,j\\i,\ell}} \quad \forall\, 0 \leq i,k \leq d_A - 1,\ \ 0 \leq j,\ell \leq d_B - 1. \tag{2.8}$$

A similar definition holds for the partial transpose T_B on B. The partial transpose is trace-preserving but *not* completely-positive.

Definition 2.6 Choi Representation

The *Choi representation* of $\Lambda \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ is the operator $J(\Lambda) \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ defined by

$$J(\Lambda) := (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \Lambda)\left(\sum_{k,k'=0}^{d_A-1} |k,k\rangle\langle k',k'|\right) = \sum_{k,k'=0}^{d_A-1} |k\rangle\langle k'| \otimes \Lambda(|k\rangle\langle k'|). \tag{2.9}$$

The Choi representation uniquely specifies the map, which means that any two maps $\Lambda_1 \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ and $\Lambda_2 \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ are equal if and only if $J(\Lambda_1) = J(\Lambda_2)$. As well, for $\Phi_1 \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ and $\Phi_2 \in \mathrm{T}(\mathfrak{H}_B, \mathfrak{H}_C)$, it holds that

$$J(\Phi_2 \circ \Phi_1) = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \Phi_2)J(\Phi_1). \tag{2.10}$$

An important fact that will be used throughout this thesis is the following.

Theorem 2.7 Completely-Positive Maps and the Choi Representation

A map $\Lambda \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ is completely-positive if and only if $J(\Lambda) \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$.

This theorem can be used to establish that the partial trace is completely-positive while the partial transpose is not completely-positive.

Now, $J : \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B) \to \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ is an isomorphism between $\mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ and $\mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ since the action of $\Lambda \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ can be recovered from $J(\Lambda)$ using

$$\Lambda(X) = \mathrm{Tr}_A[(X^{\mathsf{T}} \otimes \mathbb{1}_B)J(\Lambda)] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A). \tag{2.11}$$

This means that, given any $W \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$, we can define a map $\Lambda_W \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$, whose Choi representation is W, by

$$\Lambda_W(X) = \mathrm{Tr}_A[(X^{\mathsf{T}} \otimes \mathbb{1}_B)W] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A). \tag{2.12}$$

This equation, along with Theorem 2.7, puts the set of positive semi-definite operators and the set of completely-positive maps in one-to-one correspondence, meaning that each positive semi-definite operator has an associated completely-positive map defined by (2.12). This fact will be used repeatedly throughout the thesis.

Definition 2.8 Natural Representation

The *natural representation* of $\Lambda \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ is the operator $K(\Lambda) \in \mathrm{L}(\mathfrak{H}_A \otimes \mathfrak{H}_A, \mathfrak{H}_B \otimes \mathfrak{H}_B)$ defined by

$$\mathrm{vec}\,(\Lambda(X)) = K(\Lambda)\mathrm{vec}(X) \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A). \tag{2.13}$$

Like the Choi representation, the natural representation uniquely specifies the map. As well, for $\Phi_1 \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ and $\Phi_2 \in \mathrm{T}(\mathfrak{H}_B, \mathfrak{H}_C)$, it holds that

$$K(\Phi_1 \circ \Phi_2) = K(\Phi_1)K(\Phi_2). \tag{2.14}$$

Definition 2.9 Shuffling Map

For any two complex Euclidean spaces $\mathfrak{H}$ and $\mathfrak{K}$, define the map $S : \mathrm{L}(\mathfrak{H} \otimes \mathfrak{K}) \to \mathrm{L}(\mathfrak{H} \otimes \mathfrak{H}, \mathfrak{K} \otimes \mathfrak{K})$, called the *shuffling map*, as follows:

$$S(|k, \ell\rangle \langle k', \ell'|) = |\ell, \ell'\rangle \langle k, k'| \tag{2.15}$$

for all $0 \leq k, k' \leq d_{\mathfrak{H}} - 1$ and all $0 \leq \ell, \ell' \leq d_{\mathfrak{K}} - 1$.

It follows from the definition of the shuffling map that for all $X \in \mathrm{L}(\mathfrak{H} \otimes \mathfrak{K})$

$$(S(X))_{\substack{\ell,\ell' \\ k,k'}} = X_{\substack{k,\ell \\ k',\ell'}} \quad \forall\, 0 \leq k, k' \leq d_{\mathfrak{H}} - 1,\ \ 0 \leq \ell, \ell' \leq d_{\mathfrak{K}} - 1. \tag{2.16}$$

The shuffling map is important because is allows us to convert between the Choi and natural representations of maps in $\mathrm{T}(\mathfrak{H}, \mathfrak{K})$, as the following proposition proves.

Proposition 2.10

For any $\Lambda \in \mathrm{T}(\mathfrak{H}, \mathfrak{K})$, it holds that

$$K(\Lambda) = S(J(\Lambda)).$$

PROOF: By writing

$$J(\Lambda) = \sum_{k,k'=0}^{d_{\mathfrak{H}}-1} \sum_{\ell,\ell'=0}^{d_{\mathfrak{K}}-1} (J(\Lambda))_{\substack{k,\ell \\ k',\ell'}} |k,\ell\rangle \langle k',\ell'|,$$

so that

$$\Lambda(|k\rangle \langle k'|) = \sum_{\ell,\ell'=0}^{d_{\mathfrak{K}}-1} (J(\Lambda))_{\substack{k,\ell \\ k',\ell'}} |\ell\rangle \langle \ell'| \quad \forall\, 0 \leq k,k' \leq d_{\mathfrak{H}} - 1,$$

we have

$$S(J(\Lambda)) = \sum_{k,k'=0}^{d_{\mathfrak{H}}-1} \sum_{\ell,\ell'=0}^{d_{\mathfrak{K}}-1} (J(\Lambda))_{\substack{k,\ell \\ k',\ell'}} |\ell,\ell'\rangle \langle k,k'|.$$

Therefore, for all $0 \leq i,i' \leq d_{\mathfrak{H}} - 1$,

$$S(J(\Lambda))\mathrm{vec}(|i\rangle \langle i'|) = S(J(\Lambda))\,|i,i'\rangle = \sum_{\ell,\ell'=0}^{d_{\mathfrak{K}}-1} (J(\Lambda))_{\substack{i,\ell \\ i',\ell'}} |\ell,\ell'\rangle = \mathrm{vec}\left(\Lambda(|i\rangle \langle i'|)\right).$$

So $S(J(\Lambda))$ acts by definition as a natural representation of Λ. By uniqueness of natural representations, it is the natural representation of Λ, that is, $S(J(\Lambda)) = K(\Lambda)$. ■

2.2 Quantum Channels

Definition 2.11 Quantum Channel

A quantum channel is a completely-positive and trace-preserving map in $\mathrm{T}(\mathfrak{H},\mathfrak{K})$ for some $\mathfrak{H},\mathfrak{K}$. The set of all quantum channels $\Phi \in \mathrm{T}(\mathfrak{H},\mathfrak{K})$ is denoted $\mathrm{C}(\mathfrak{H},\mathfrak{K})$.

Quantum channels are viewed as representing the most general kind of evolution of a quantum system. Evolution given by the Schrödinger equation, for example, corresponds to a *unitary* channel. The unitary channels is a simple class of quantum channels defined as $\Phi(X) = UXU^\dagger$ for some unitary $U \in \mathrm{U}(\mathfrak{H})$.

The following theorem provides three important facts about quantum channels.

Theorem 2.12 Characterization of Quantum Channels

For a quantum channel $\Phi \in \mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$, the following hold:

1. $J(\Phi)$ is positive semi-definite and $\mathrm{Tr}_B[J(\Phi)] = \mathbb{1}_A$.
2. Φ has the operator-sum decomposition, called a *Kraus decomposition* or a *Kraus representation* of Φ,
$$\Phi(X) = \sum_{i=1}^{r} A_i X A_i^\dagger, \quad \sum_{i=1}^{r} A_i^\dagger A_i = \mathbb{1}_A, \tag{2.17}$$
where $r \geq \mathrm{rank}(J(\Phi))$. The set $\{A_i\}_{i=1}^r$ is called the *Kraus operators* of Φ.
3. Φ can be written in *Stinespring form*,
$$\Phi(X) = \mathrm{Tr}_E[VXV^\dagger],$$
where $V : \mathfrak{H}_A \to \mathfrak{H}_B \otimes \mathfrak{H}_E$ is an isometry and $d_E \geq \mathrm{rank}(J(\Phi))$. V is sometimes called an *isometric extension*, or *purification*, of Φ.

One possible set of Kraus operators for a channel $\Phi \in \mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$ is the the set $\{A_i\}_{i=1}^{\mathrm{rank}(J(\Phi))}$ defined by
$$A_i |k\rangle^A = \sqrt{\lambda_i}(\langle k| \otimes \mathbb{1}_B) |\phi_i\rangle^{AB} \quad \forall\, 0 \leq k \leq d_A - 1,$$
where $\{\lambda_i\}_{i=1}^{\mathrm{rank}(J(\Phi))}$ are the non-zero eigenvalues of $J(\Phi)$ and $\{|\phi_i\rangle^{AB}\}_{i=1}^{\mathrm{rank}(J(\Phi))}$ are the corresponding (orthonormal) eigenvectors. With this set of Kraus operators, one possible isometric extension V of Φ is one in which $d_E = \mathrm{rank}(J(\Phi))$ and
$$V = \sum_{i=1}^{\mathrm{rank}(J(\Phi))} A_i \otimes |e_i\rangle^E,$$
where $\{|e_i\rangle^E\}_{i=1}^{\mathrm{rank}(J(\Phi))}$ is any orthonormal basis for $\mathfrak{H}_E$.

In the characterization theorem above, the condition that $J(\Phi)$ is positive semi-definite follows from the complete-positivity of Φ, while the condition $\mathrm{Tr}_B[J(\Phi)] = \mathbb{1}_A$ is the result of Φ being trace-preserving. Similarly, for the Kraus representation of Φ given in (2.17), the fact that $\Phi(X) = \sum_{i=1}^r A_i X A_i^\dagger$ follows from the complete-positivity of Φ, while the condition $\sum_{i=1}^r A_i^\dagger A_i = \mathbb{1}_A$ is the result of Φ being trace-preserving. This means that any completely-positive map can be represented in the form (2.17), except that possibly $\sum_{i=1}^r A_i^\dagger A_i \leq \mathbb{1}_A$ since completely-positive maps are not generally trace-preserving. Finally, the fact that $\Phi(X) = \mathrm{Tr}_E[VXV^\dagger]$ follows from the complete-positivity of Φ, while the condition that V is an isometry is the result of Φ being trace-preserving.

By observing that when $\Phi \in \mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$ the operator $\rho_\Phi := \frac{1}{d_A} J(\Phi)$ is positive semi-definite and has unit trace, that is, $\rho_\Phi \in \mathrm{D}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$, we obtain a one-to-one correspondence between the set $\mathcal{D} := \left\{\rho \in \mathrm{D}(\mathfrak{H}_A \otimes \mathfrak{H}_B) : \mathrm{Tr}_B(\rho) = \frac{\mathbb{1}_A}{d_A}\right\}$ of density operators and the set of all channels $\mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$, a correspondence that is sometimes called *state-channel duality* or the *Choi-Jamiolkowski isomorphism*. Specifically, by (2.12), every density operator $\rho \in \mathcal{D}$ defines a channel $\Phi_\rho \in \mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$ according to
$$\Phi_\rho(X) = d_A \mathrm{Tr}_A[(X^\intercal \otimes \mathbb{1}_B)\rho] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A),$$
and every channel $\Phi \in \mathrm{C}(\mathfrak{H}_A, \mathfrak{H}_B)$ defines the density operator $\rho_\Phi = \frac{1}{d_A} J(\Phi) \in \mathrm{D}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$. Density operators not in $\mathcal{D}$ will, by Theorem 2.7, correspond to completely positive maps according to (2.12).

The Stinespring form $\Phi(\rho) = \mathrm{Tr}_E[V\rho V^\dagger]$ of a CP map or channel $\Phi \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ has the following physical interpretation: the input state $\rho \in \mathrm{D}(\mathfrak{H}_A)$ interacts with its *environment*, modelled by the space $\mathfrak{H}_E$, via the isometry V, leaving the system and environment in the joint state $V\rho V^\dagger$. The state of the system resulting from this interaction is then given by tracing over, or "ignoring", the environment. If we instead ask what happsn to the *environment* after the interaction, then we obtain the following.

Definition 2.13 Complementary Map

For $\Phi \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$ in Stinespring form,

$$\Phi(X) = \mathrm{Tr}_E[VXV^\dagger] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A),$$

the map $\Phi^c \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_E)$ *complementary* to Φ is defined by

$$\Phi^c(X) = \mathrm{Tr}_B[VXV^\dagger] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A).$$

Φ^c is unique up to isometries on $\mathfrak{H}_E$.

Definition 2.14 Degradable and Anti-degradable CP Maps

A completely-positive map $\Phi \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$ is called *degradable* if there exists a quantum channel $\mathcal{E} \in \mathrm{C}(\mathfrak{H}_B, \mathfrak{H}_E)$, called the *degrading map*, such that

$$\mathcal{E} \circ \Phi = \Phi^c.$$

Φ is called *anti-degradable* if its complement Φ^c is degradable, that is, if there exists a quantum channel $\mathcal{E} \in \mathrm{C}(\mathfrak{H}_E, \mathfrak{H}_B)$ such that

$$\mathcal{E} \circ \Phi^c = \Phi.$$

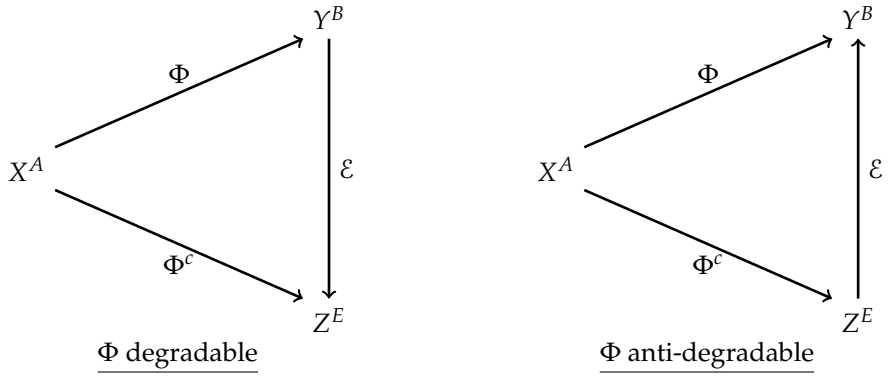


Figure 2.1: Degradable and anti-degradable CP maps $\Phi \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$.

As indicated in Figure 2.1 above, degradable CP maps Φ are those whose complements may be simulated by processing, or "degrading", the output of Φ using $\mathcal{E}$, while anti-degradable maps are those than can be

simulated by degrading the output of the *complementary* map Φ^c using $\mathcal{E}$.

2.2.1 Pauli Channels

An important class of channels in $\mathrm{C}(\mathbb{C}^2, \mathbb{C}^2)$ is the *Pauli channels* $\{\Psi_{\vec{p}} : \vec{p} = (p_x, p_y, p_z) \in \mathbb{R}^3,\ p_x, p_y, p_z \geq 0,\ p_x + p_y + p_z \leq 1\}$, where

$$\Psi_{\vec{p}}(X) = p_I X + p_x \sigma_x X \sigma_x^\dagger + p_y \sigma_y X \sigma_y^\dagger + p_z \sigma_z X \sigma_z^\dagger \quad \forall\, X \in \mathrm{L}(\mathbb{C}^2), \tag{2.18}$$

$p_I = 1 - p_x - p_y - p_z$, and $\sigma_x, \sigma_y, \sigma_z$ are the *Pauli operators* and are defined in the standard basis of $\mathbb{C}^2$ as

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.19}$$

We will sometimes use the alternative notation $\sigma_1 \equiv \sigma_x$, $\sigma_2 \equiv \sigma_y$, and $\sigma_3 \equiv \sigma_z$ to refer to them. They are traceless Hermitian operators satisfying $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}_{\mathbb{C}^2}$. Together with $\sigma_0 \equiv \mathbb{1}_{\mathbb{C}^2}$, $\{\mathbb{1}_{\mathbb{C}^2}, \sigma_x, \sigma_y, \sigma_z\}$ forms an orthogonal basis for $\mathrm{L}(\mathbb{C}^2)$. As such, any operator $X \in \mathrm{L}(\mathbb{C}^2)$ can be written as

$$X = \frac{1}{2} \sum_{i=0}^{3} \alpha_i(X) \sigma_i, \quad \alpha_i(X) \coloneqq \mathrm{Tr}(X^\dagger \sigma_i). \tag{2.20}$$

$\Psi_{\vec{p}}$ has Kraus operators

$$A_I = \sqrt{p_I}\mathbb{1}_{\mathbb{C}^2}, \quad A_x = \sqrt{p_x}\sigma_x, \quad A_y = \sqrt{p_y}\sigma_y, \quad A_z = \sqrt{p_z}\sigma_z,$$

so that an isometric extension of $\Psi_{\vec{p}}$ is

$$V_{\Psi_{\vec{p}}} = A_I \otimes |0\rangle^E + A_x \otimes |1\rangle^E + A_y \otimes |2\rangle^E + A_z \otimes |3\rangle^E.$$

The Choi representation of $\Psi_{\vec{p}}$ is

$$J(\Psi_{\vec{p}}) = 2\rho_{\mathrm{Bell}}(\vec{p}),$$

where

$$\rho_{\mathrm{Bell}}(\vec{p}) = p_I \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + p_x \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + p_y \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + p_z \left|\Phi^-\right\rangle\left\langle\Phi^-\right| \tag{2.21}$$

and

$$\begin{aligned} \left|\Phi^+\right\rangle &\coloneqq \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle), \quad \left|\Phi^-\right\rangle \coloneqq \frac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle), \\ \left|\Psi^+\right\rangle &\coloneqq \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle), \quad \left|\Psi^-\right\rangle \coloneqq \frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle) \end{aligned} \tag{2.22}$$

are the *Bell states*. They form an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ and feature prominently throughout the thesis. Density operators that are diagonal in this basis are called *Bell-diagonal states* and will be explored further in §2.3.1.

An important subset of the Pauli channels comes from setting $p_x = p_y = p_z = \frac{Q}{2}$ for some $0 \leq Q \leq \frac{2}{3}$:

$$\begin{aligned} \Psi_{\left(\frac{Q}{2}, \frac{Q}{2}, \frac{Q}{2}\right)}(X) &= \left(1 - \frac{3Q}{2}\right) X + \frac{Q}{2}\sigma_x X \sigma_x^\dagger + \frac{Q}{2}\sigma_y X \sigma_y^\dagger + \frac{Q}{2}\sigma_z X \sigma_z^\dagger \\ &= (1 - 2Q)X + \frac{Q}{2}(X + \sigma_x X \sigma_x^\dagger + \sigma_y X \sigma_y^\dagger + \sigma_z X \sigma_z^\dagger) \\ &= (1 - 2Q)X + \mathrm{Tr}(X) Q \mathbb{1}_{\mathbb{C}^2}, \end{aligned}$$

where in the last step we used the fact that

$$\frac{1}{2}(X + \sigma_x X \sigma_x^\dagger + \sigma_y X \sigma_y^\dagger + \sigma_z X \sigma_z^\dagger) = \mathrm{Tr}(X)\mathbb{1}_{\mathbb{C}^2} \quad \forall\, X \in \mathrm{L}(\mathbb{C}^2).$$

The channels $\{\Delta_Q : 0 \leq Q \leq \frac{2}{3}\}$ defined by

$$\Delta_Q(X) = (1 - 2Q)X + \mathrm{Tr}(X)Q\mathbb{1}_{\mathbb{C}^2} \quad \forall\, X \in \mathrm{L}(\mathbb{C}^2) \tag{2.23}$$

are called *depolarizing channels*. $\Delta_{\frac{1}{2}} \equiv \Delta$ is called the *completely-depolarizing channel*.

The Pauli operators and Pauli channels can be generalized to spaces of dimension higher than two, as we will see in Chapter 6.

2.3 Quantum States

The set of possible physical states of a quantum system is modelled by the set $\mathrm{D}(\mathfrak{H})$ of density operators on a complex Euclidean space $\mathfrak{H}$. If a system consists of a set of n subsystems labelled $1, 2, \ldots, n$, then the set of states is $\mathrm{D}(\mathfrak{H}_1 \otimes \mathfrak{H}_2 \otimes \cdots \otimes \mathfrak{H}_n)$, where $\mathfrak{H}_i$ is the underlying space of subsystem i. The subsystems are also sometimes called *registers*.

The set of density operators is a convex set, which by definition means that for any $\rho_1, \rho_2 \in \mathrm{D}(\mathfrak{H})$, $p\rho_1 + (1-p)\rho_2 \in \mathrm{D}(\mathfrak{H})$ for all $p \in [0, 1]$. The sum $p\rho_1 + (1-p)\rho_2$ is called a *convex combination* of ρ_1 and ρ_2 and can be generalized to arbitrary probability distributions $\{p_i\}_{i=1}^n$, so that $p_1\rho_1 + p_2\rho_2 + \cdots p_n\rho_n$ is called a convex combination of $\rho_1, \rho_2, \ldots \rho_n \in \mathrm{D}(\mathfrak{H})$[1]. The *convex hull* of a subset $\mathcal{D}$ of density operators is the set of all density operators that may be written as a convex combination of the density operators in $\mathcal{D}$. The *extremal points* of a convex set are those elements of the set that cannot be written as a non-trivial convex combination of other elements in the set. An important consequence of the definition of extremal points is that any convex set is the convex hull of the set of its extremal points.

The set of extremal points of the set $\mathrm{D}(\mathfrak{H})$ is called the set of *pure states*. Pure states have unit rank and are of the form $|\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathfrak{H}$. We commonly refer to the pure state $|\psi\rangle\langle\psi|$ as $|\psi\rangle$, although this identification is unique only up to a complex phase factor since for any $\alpha \in \mathbb{C}$ with $|\alpha|^2 = 1$ the vector $|\phi\rangle := \alpha|\psi\rangle$ has the same corresponding pure state as $|\psi\rangle$: $|\phi\rangle\langle\phi| = |\alpha|^2|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$. Since pure states are extremal points in $\mathfrak{H}$, any density operator can be written as a convex combination of pure states.

Theorem 2.15 Schmidt Decomposition

Any non-zero vector $|\psi\rangle \in \mathfrak{H} \otimes \mathfrak{K}$ can be written in the form

$$|\psi\rangle = \sum_{k=1}^{n} \sqrt{s_k}\,|e_k\rangle \otimes |f_k\rangle\,,$$

where $n = \min\{d_{\mathfrak{H}}, d_{\mathfrak{K}}\}$, $\{s_k\}_{k=1}^n$ is a set of positive real numbers, and $\{|e_1\rangle, \ldots, |e_n\rangle\} \subset \mathfrak{H}$, $\{|f_1\rangle, \ldots, |f_n\rangle\} \subset \mathfrak{K}$ are orthonormal sets.

[1] The notion of convex sets and convex combination, as well as the notions of convex hull and extremal points to be described below, are defined for any subsets of elements of a vector space, not just for the space of density operators.

Definition 2.16 Purification

A pure state $|\psi\rangle \in \mathfrak{H} \otimes \mathfrak{K}$ is called a *purification* in $\mathfrak{K}$ of $\rho \in \mathrm{D}(\mathfrak{H})$ if $\mathrm{Tr}_{\mathfrak{K}}(|\psi\rangle\langle\psi|) = \rho$.

Given two purifications $|\psi\rangle, |\phi\rangle \in \mathfrak{H} \otimes \mathfrak{K}$ in $\mathfrak{K}$ of a density operator $\rho \in \mathrm{D}(\mathfrak{H})$, there exists a unitary $U \in \mathrm{U}(\mathfrak{K})$ such that

$$|\phi\rangle = (\mathbb{1}_{\mathfrak{H}} \otimes U)|\psi\rangle .$$

This fact is often called the *unitary equivalence of purifications*.

Theorem 2.17 State Purification

For any $\rho \in \mathrm{D}(\mathfrak{H})$ there exists a purification $|\psi\rangle \in \mathfrak{H} \otimes \mathfrak{K}$ in $\mathfrak{K}$ of ρ with $d_{\mathfrak{K}} \geq d_{\mathfrak{H}}$.

An important fact that we use in this thesis, which can be verified using (2.3), is that for any $\rho \in \mathrm{D}(\mathfrak{H})$ $\mathrm{vec}(\sqrt{\rho}) \in \mathfrak{H} \otimes \mathfrak{K}$ is a purification of ρ in $\mathfrak{K}$, where $d_{\mathfrak{K}} = \mathrm{rank}(\rho)$.

Definition 2.16 and Theorem 2.17 can be generalized to apply to arbitrary positive semi-definite operators, not just to density operators. This allows us to prove the following fact about the complements of completely-positive maps.

Proposition 2.18

Given a $\Phi \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$, the Choi representation of the complementary map $\Phi^c \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_E)$ is given by (up to isometries on $\mathfrak{H}_E$)

$$J(\Phi^c) = \mathrm{Tr}_B[|\psi\rangle\langle\psi|_\Phi],$$

where $|\psi\rangle_\Phi \in \mathfrak{H}_A \otimes \mathfrak{H}_B \otimes \mathfrak{H}_E$ is a purification of $J(\Phi)$ in $\mathfrak{H}_E$.

PROOF: Let $V_\Phi \in \mathrm{U}(\mathfrak{H}_A, \mathfrak{H}_B \otimes \mathfrak{H}_E)$ be an isometric extension of Φ for some space $\mathfrak{H}_E$ with $d_E \geq \mathrm{rank}(J(\Phi))$. Then,

$$(\mathbb{1}_A \otimes V_\Phi)\left(\sum_{k=0}^{d_A-1} |k,k\rangle^{AA}\right) =: |\psi\rangle_\Phi$$

is a purification in $\mathfrak{H}_E$ of $J(\Phi)$ by definition of the action of Φ in Stinespring form. Therefore, by definition of the action of Φ^c in Stinespring form, we have

$$\mathrm{Tr}_B[|\psi\rangle\langle\psi|_\Phi] = \mathrm{Tr}_B[(\mathbb{1}_A \otimes V_\Phi)\left(\sum_{k,k'=0}^{d_A-1} |k,k\rangle\langle k',k'|\right)(\mathbb{1}_A \otimes V_\Phi)^\dagger] = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \Phi^c)\left(\sum_{k,k'=0}^{d_A-1} |k,k\rangle\langle k',k'|\right) = J(\Phi^c),$$

as required. ■

Definition 2.19 Separable and Entangled States

A density operator $\rho \in \mathrm{D}(\mathfrak{H} \otimes \mathfrak{K})$ is called *separable* if there exists $n \in \mathbb{N}$, collections $\{\tau_i : 1 \leq a \leq n\} \subseteq \mathrm{D}(\mathfrak{H})$ and $\{\xi_i : 1 \leq a \leq n\} \subseteq \mathrm{D}(\mathfrak{K})$, and a probability distribution $\{p_i : 1 \leq i \leq n\}$ such that

$$\rho = \sum_{i=1}^{n} p_i \tau_i \otimes \xi_i.$$

A density operator that is not separable is called *entangled*.

An important theorem due to Peres and Horodecki [Per96; HHH96], sometimes called the *Postive-Partial-Transpose (PPT) criterion*, gives a necessary and sufficient condition for density operators on $\mathbb{C}^2 \otimes \mathbb{C}^2$ to be separable.

Theorem 2.20 PPT Criterion

A density operator $\rho \in \mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is separable if and only if ρ^{T_2}, the partial transpose of ρ on the second tensor factor, is positive semi-definite.

For density operators $\rho \in \mathrm{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ on higher-dimensional spaces, the PPT criterion is merely necessary and not sufficient for separability. It can still be useful, however, since if ρ^{T_B} has a negative eigenvalue, then ρ is entangled.

A purification is an example of what is called an *extension* of an operator, a concept that is particularly important in this thesis.

Definition 2.21 Extension of an Operator

For any $X \in \mathrm{L}(\mathfrak{H})$, an operator $Y \in \mathrm{L}(\mathfrak{H} \otimes \mathfrak{K})$ is called an *extension* of X to $\mathfrak{K}$ if

$$\mathrm{Tr}_{\mathfrak{K}}(Y) = X.$$

For any $X^A \in \mathrm{L}(\mathfrak{H}_A)$, X^{AB} will be used to denote an extension of X^A to $\mathfrak{H}_B$.

The following important fact tells us that an arbitrary extension of a positive semi-definite operator can be "reached" from its purification by some quantum channel.

Theorem 2.22

For any extension $Y \in \mathrm{Pos}(\mathfrak{H} \otimes \mathfrak{L})$ of $X \in \mathrm{Pos}(\mathfrak{H})$ to $\mathfrak{L}$ there exists $\Lambda \in \mathrm{C}(\mathfrak{K}, \mathfrak{L})$ such that

$$(\mathbb{1}_{\mathrm{L}(\mathfrak{H})} \otimes \Lambda)(|\psi\rangle \langle\psi|) = Y,$$

where $|\psi\rangle \in \mathfrak{H} \otimes \mathfrak{K}$ is a purification of X in $\mathfrak{K}$.

2.3.1 Two-Qubit Bell-Diagonal States

Two-qubit Bell-diagonal states comprise density operators that are diagonal in the Bell basis introduced in (2.22). Recall from (2.21) that they have the general form

$$\rho_{\text{Bell}}(\vec{p}) = p_I \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + p_x \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + p_y \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + p_z \left|\Phi^-\right\rangle\left\langle\Phi^-\right|, \tag{2.24}$$

where $\vec{p} = (p_x, p_y, p_z)$ satisfies $p_x + p_y + p_z \leq 1$, and $p_I = 1 - p_x - p_y - p_z$. An important class of Bell-diagonal states that will be considered in this thesis is the *isotropic states*[2], which for $0 \leq Q \leq \frac{2}{3}$ are defined as

$$\rho_{\text{iso}}(Q) = (1 - 2Q)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2}\mathbb{1}_{\mathbb{C}^2\otimes\mathbb{C}^2}. \tag{2.25}$$

We can observe using (2.23) that $\rho_{\text{iso}}(Q)$ is proportional to the Choi representation of the depolarizing channel Δ_Q.

Now, just as (2.20) gives us a decomposition of any $X \in \mathrm{L}(\mathbb{C}^2)$ in terms of the Pauli operators, any $X \in \mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ can be written as[3]

$$X = \frac{1}{4}\sum_{i,j=0}^{3} \alpha_{i,j}(X)\sigma_i \otimes \sigma_j, \quad \alpha_{i,j}(X) \coloneqq \mathrm{Tr}[X^\dagger(\sigma_i \otimes \sigma_j)]. \tag{2.26}$$

Under this decomposition, $\rho_{\text{Bell}}(\vec{p})$ has the form

$$\rho_{\text{Bell}}(\vec{p}) = \frac{1}{4}(\mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2} + \alpha_x\sigma_x \otimes \sigma_x + \alpha_y\sigma_y \otimes \sigma_y + \alpha_z\sigma_z \otimes \sigma_z), \tag{2.27}$$

where $\alpha_x = \alpha_{1,1}(\rho_{\text{Bell}}(\vec{p}))$, $\alpha_y = \alpha_{2,2}(\rho_{\text{Bell}}(\vec{p}))$ and $\alpha_z = \alpha_{3,3}(\rho_{\text{Bell}}(\vec{p}))$ are given by

$$\alpha_x = p_I + p_x - p_y - p_z, \quad \alpha_y = -p_I + p_x - p_y + p_z, \quad \alpha_z = p_I - p_x - p_y + p_z. \tag{2.28}$$

Using this decomposition, we observe that $\rho_{\text{Bell}}(\vec{p})$ is invariant under $\sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z$: for all $\vec{p}$,

$$\begin{aligned}(\sigma_x \otimes \sigma_x)\rho_{\text{Bell}}(\vec{p})(\sigma_x \otimes \sigma_x) &= \rho_{\text{Bell}}(\vec{p}),\\ (\sigma_z \otimes \sigma_z)\rho_{\text{Bell}}(\vec{p})(\sigma_z \otimes \sigma_z) &= \rho_{\text{Bell}}(\vec{p}).\end{aligned} \tag{2.29}$$

We also see from this decomposition that $\rho_{\text{Bell}}(\vec{p})$ is invariant under transposition: for all $\vec{p}$,

$$(\rho_{\text{Bell}}(\vec{p}))^\mathsf{T} = \rho_{\text{Bell}}(\vec{p}), \tag{2.30}$$

since $\sigma_x^\mathsf{T} = \sigma_x$, $\sigma_z^\mathsf{T} = \sigma_z$, and $\sigma_y^\mathsf{T} = -\sigma_y \Rightarrow (\sigma_y^\mathsf{T} \otimes \sigma_y^\mathsf{T}) = \sigma_y \otimes \sigma_y$.

We can assume without loss of generality that the coefficients $\{p_I, p_x, p_y, p_z\}$ satisfy the following [BA07],

$$p_I = \max\{p_I, p_x, p_y, p_z\}, \quad p_z = \min\{p_I, p_x, p_y, p_z\}, \tag{2.31}$$

[2]Isotropic states $\rho \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ are defined by the condition [HH99] $(U \otimes \overline{U})\rho(U \otimes \overline{U})^\dagger = \rho$ for all $U \in \mathrm{U}(\mathbb{C}^d)$. These states are often erroneously called *Werner states*, which are strictly-speaking a completely different class of states [Wer89] defined by the condition $(U \otimes U)\rho(U \otimes U)^\dagger = \rho$ for all $U \in \mathrm{U}(\mathbb{C}^d)$. While for the two-qubit case the isotropic and Werner states are unitarily equivalent, which is why the names are often used interchangeably, this is not so in higher dimensions.

[3]An analogous decomposition holds for any operator in $\mathrm{L}((\mathbb{C}^2)^{\otimes n})$ for any n.

since any Bell-diagonal state not of this form can be put into this form by means of the following local operators that transform the Bell basis elements:

$$\begin{aligned}
\left|\Phi^+\right\rangle\left\langle\Phi^+\right| &\leftrightarrow \left|\Phi^-\right\rangle\left\langle\Phi^-\right| : \quad \frac{\mathrm{i}}{2}(\mathbb{1} - \mathrm{i}\sigma_z) \otimes (\mathbb{1} - \mathrm{i}\sigma_z), \\
\left|\Phi^-\right\rangle\left\langle\Phi^-\right| &\leftrightarrow \left|\Psi^+\right\rangle\left\langle\Psi^+\right| : \quad \frac{1}{2}(\sigma_x + \sigma_z) \otimes (\sigma_x + \sigma_z), \\
\left|\Psi^+\right\rangle\left\langle\Psi^+\right| &\leftrightarrow \left|\Psi^-\right\rangle\left\langle\Psi^-\right| : \quad \frac{1}{2}(\mathbb{1} + \mathrm{i}\sigma_z) \otimes (\mathbb{1} - \mathrm{i}\sigma_z).
\end{aligned}$$

Proposition 2.23

Every state $\rho_{\text{Bell}}(\vec{p}) = p_I \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + p_x \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + p_y \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + p_z \left|\Phi^-\right\rangle\left\langle\Phi^-\right|$ of the form (2.31) is separable if and only if

$$p_I \leq p_x + p_y + p_z.$$

PROOF: We will use the PPT criterion of Theorem 2.20 to prove this. In the standard basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$, we have

$$\rho_{\text{Bell}}(\vec{p}) = \begin{bmatrix} \frac{p_I+p_z}{2} & 0 & 0 & \frac{p_I-p_z}{2} \\ 0 & \frac{p_x+p_y}{2} & \frac{p_x-p_y}{2} & 0 \\ 0 & \frac{p_x-p_y}{2} & \frac{p_x+p_y}{2} & 0 \\ \frac{p_I-p_z}{2} & 0 & 0 & \frac{p_I+p_z}{2} \end{bmatrix}$$

Then, the partial transpose $(\rho_{\text{Bell}}(\vec{p}))^{\mathsf{T}_2}$ is

$$(\rho_{\text{Bell}}(\vec{p}))^{\mathsf{T}_2} = \begin{bmatrix} \frac{p_I+p_z}{2} & 0 & 0 & \frac{p_x-p_y}{2} \\ 0 & \frac{p_x+p_y}{2} & \frac{p_I-p_z}{2} & 0 \\ 0 & \frac{p_I-p_z}{2} & \frac{p_x+p_y}{2} & 0 \\ \frac{p_x-p_y}{2} & 0 & 0 & \frac{p_I+p_z}{2} \end{bmatrix},$$

which has eigenvalues

$$p_I + p_x + p_y - p_z, \quad p_I + p_x - p_y + p_z, \quad p_y + p_z + p_I - p_x, \quad p_y + p_z - p_I + p_x.$$

Non-negativity of these eigenvalues leads to the conditions

$$p_I \geq p_z - p_y - p_x, \quad p_I \geq p_y - p_z - p_x, \quad p_I \geq p_x - p_y - p_z, \quad p_I \leq p_y + p_z + p_x. \tag{2.32}$$

The last of these, which is the claimed inequality, is clearly necessary for the positive semi-definiteness of $(\rho_{\text{Bell}}(\vec{p}))^{\mathsf{T}_2}$ and hence for the separability of $\rho_{\text{Bell}}(\vec{p})$ by the PPT criterion. We now prove that it is also sufficient.

Assuming $p_I \leq p_x + p_y + p_z$, because $p_I = \max\{p_I, p_x, p_y, p_z\}$, we can write this inequality as

$$p_z + p_x \geq p_I - p_y \geq -(p_I - p_y) = -p_I + p_y \Rightarrow p_I \geq p_y - p_z - p_x,$$

which is the second inequality in (2.32) above. Next,

$$p_I \leq p_x + p_y + p_z \Rightarrow p_y + p_z \geq p_I - p_x \geq -(p_I - p_x) = -p_I + p_x \Rightarrow p_I \geq p_x - p_y - p_z,$$

which is the third inequality in (2.32) above. Finally,

$$p_I \leq p_x + p_y + p_z \Rightarrow p_y + p_x \geq p_I - p_z \geq -(p_I - p_z) = -p_I + p_z \Rightarrow p_I \geq p_z - p_y - p_x,$$

which is the first inequality in (2.32) above. So the inequality $p_I \leq p_y + p_z + p_x$ is also sufficient for the positive semi-definiteness of $(\rho_{\text{Bell}}(\vec{p}))^{\mathsf{T}_2}$ and hence for the separability of $\rho_{\text{Bell}}(\vec{p})$. ■

2.3.2 Measurements

Physical measurements of a quantum system are modelled by *positive operator-valued measures (POVMs)*, which are sets $\mathcal{M} = \{\Pi_a\}_{a\in I} \subset \mathrm{Pos}(\mathfrak{H})$ satisfying $\sum_{a\in I}\Pi_a = \mathbb{1}_{\mathfrak{H}}$. The elements of the index set I are used to label the outcomes of the measurement. Given a quantum state $\rho \in \mathrm{D}(\mathfrak{H})$, the random variable $O_{\mathcal{M},\rho}$ describing the *outcomes* of the measurement has by definition probability distribution

$$\Pr[O_{\mathcal{M},\rho} = a] = \mathrm{Tr}[\Pi_a\rho]. \tag{2.33}$$

Quite often, measurements are described using *observables*, which by definition are Hermitian operators in $\mathrm{L}(\mathfrak{H})$. The POVM corresponding to a measurement of an observable is the set of projection operators appearing in its spectral decomposition and the outcome set I is the set of its eigenvalues.

For every state ρ, the POVM $\mathcal{M}$ defines the ensemble $\{(p_{\mathcal{M},\rho}(a), \rho_{\mathcal{M},a})\}_{a\in I}$, where

$$p_{\mathcal{M},\rho}(a) \coloneqq \Pr[O_{\mathcal{M},\rho} = a], \quad \rho_{\mathcal{M},a} \coloneqq \frac{\sqrt{\Pi_a}\rho\sqrt{\Pi_a}}{p_{\mathcal{M},a}}.$$

This is not the only ensemble one can define. Quite often, one writes $\Pi_a = M_a^\dagger M_a$ for all $a \in I$ for some collection $\{M_a\}_{a\in I} \subset \mathrm{L}(\mathfrak{H})$ and sets

$$\rho_{\mathcal{M},a} = \frac{M_a\rho M_a^\dagger}{p_{\mathcal{M},\rho}(a)},$$

In both cases, the collections $\{M_a\}_{a\in I}$ and $\{\sqrt{\Pi_a}\}_{a\in I}$ are the Kraus operators of a channel giving rise to the state $\rho_{\mathcal{M}}$ after measurement defined as

$$\rho_{\mathcal{M}} \coloneqq \sum_{a\in I} p_{\mathcal{M},\rho}(a)\rho_{\mathcal{M},a} = \sum_{a\in I} M_a\rho M_a^\dagger \quad \left(\text{or } \sum_{a\in I}\sqrt{\Pi_a}\rho\sqrt{\Pi_a}\right). \tag{2.34}$$

Physically, the ensemble corresponding to a measurement represents the probabilistic knowledge of the experimenter performing the measurement about the outcome that occurred. Sometimes, the experimenter will want to *post-select* certain outcomes of the experiment that are desired. Suppose some subset $I_s \subseteq I$ represents these desired, or "successful" outcomes of the experiment. The state (2.34) after measurement can be written as

$$\rho_{\mathcal{M}} = \sum_{a\in I_s} M_a\rho M_a^\dagger + \sum_{a\in I\setminus I_s} M_a\rho M_a^\dagger.$$

The state after post-selection on I_s is then taken to be

$$\rho_{\mathcal{M}}^{\mathrm{succ}} \coloneqq \frac{\sum_{a\in I_s} M_a\rho M_a^\dagger}{p_{\mathcal{M},\rho}^{\mathrm{succ}}}, \quad \text{where} \quad p_{\mathcal{M},\rho}^{\mathrm{succ}} \coloneqq \sum_{a\in I_s} p_{\mathcal{M},\rho}(a) = \mathrm{Tr}\left(\sum_{a\in I_s} M_a\rho M_a^\dagger\right).$$

2.4 Quantum Key Distribution

The goal of quantum key distribution (QKD) is to use the laws of quantum physics to establish a secret key between two parties, conventionally called Alice and Bob, in the presence of an eavesdropper, conventionally called Eve. The key is then used to communicate securely between Alice and Bob using for example the one-time pad encryption scheme (see [Lüt14] for details and further motivation).

To achieve their goal, Alice and Bob have access to a classical communication channel that is authenticated, which means that Eve can only listen to Alice and Bob, not alter the messages being sent. They also have access to a quantum channel that is not authenticated, meaning that Eve can tamper with the channel in any way that is allowed by quantum physics. For the purpose of security analysis, the channel and Eve are not distinguished: any alteration of the signals through the channel is assumed to be due to Eve.

A QKD protocol is typically split into a *quantum phase* and a *classical phase*, which proceed as follows.

Quantum Phase

1. *Distribution*: Alice prepares an ensemble $\{(p_i, |\psi_i\rangle)\}_i$ of states according to a probability distribution $\{p_i\}_i$ and sends signals with these states to Bob through the quantum channel several times.
2. *Measurement*: Bob measures each of the signals sent by Alice using a POVM $\mathcal{M}_B = \{B_i\}_i$.

Classical Phase

1. *Parameter Estimation and Continuation Decision*: Alice and Bob use the information about the signals sent and the measurement results obtained to estimate the probabilities $p_{i|j}$ that Bob got measurement outcome i given that Alice sent signal j. These probabilities allow Alice and Bob to estimate Eve's information about the measurement results. If they determine that Eve has obtained too much information, then they abort the protocol; otherwise, they continue to error-correction and privacy amplification.
2. *Key Map*: Alice and Bob execute some local operation to transform their data[4] into strings called *raw keys*.
3. *Error-Correction*: Alice and Bob communicate over the classical channel to correct any discrepancies in their raw keys, which may have arisen from Eve tampering with the quantum channel during the quantum phase. This results in equal strings between Alice and Bob but gives Eve additional information about the key.
4. *Privacy Amplification*: This step takes the strings held by Alice and Bob and maps them to a shorter string that can be proved to be uncorrelated with Eve[5]. The result is a secret key.

Note that at least some of the states in the ensemble used by Alice should be non-orthogonal, otherwise Eve could simply intercept the signals sent by Alice, perform a measurement to perfectly distinguish them, and resend them to Bob without ever being detected. Also, the parameter estimation step involves communication between Alice and Bob over the classical authenticated channel in order to obtain an estimate of the probabilities $\{p_{i|j}\}_{i,j}$. This means that they will be sacrificing some amount of their data since all information announced could be accessed by Eve. We will assume throughout this thesis that Alice and Bob have enough data so that they can determine the probabilities $\{p_{i|j}\}_{i,j}$ exactly. This assumption holds in the so-called *infinite-key limit*, in which the number of signals distributed between Alice and Bob during the distribution step approaches infinity. All statements and analyses concerning secret key distillation will assume this limit throughout this thesis.

The error-correction and privacy amplification steps are collectively called *one-way (classical) post-processing protocols* as they require classical communication to establish a secret key using the raw key data from either

[4] Alice's data consists of the signals sent and Bob's data consists of the results of his measurement on the signals.

[5] See [BBR88; ILL89; Ben+95] for privacy amplification in the presence of an eavesdropper with classical information and [KMR05; RK05; Ren05] for privacy amplification in the presence of an eavesdropper with quantum information, which is most relevant to QKD.

Alice or Bob[6]. Throughout this thesis, we will assume without loss of generality that one-way post-processing protocols are used to establish a secret key using Alice's raw key. Also, as alluded to in the introduction, Alice and Bob might first execute the advantage distillation protocol (involving communication from Alice to Bob and from Bob to Alice) before performing the key map step and subsequently error-correction and privacy amplification. Any such additional protocol will be generally referred to as a *two-way (classical) post-processing protocol*.

QKD protocols with quantum phase as described above are typically called *prepare-and-measure (PM)* protocols. An alternative, but equivalent approach is to let an untrusted source distribute bipartite entangled particles to Alice and Bob, who then measure them using pre-specified POVMs $\mathcal{M}_A = \{A_i\}_i$ and $\mathcal{M}_B = \{B_j\}_j$. QKD protocols with such a quantum phase are called *entanglement-based (EB)* protocols. In EB protocols, both Alice and Bob perform measurements while in PM protocols only Bob measures. For the parameter estimation step in EB protocols, Alice and Bob use some of their measurement results to estimate the set of states ρ^{AB} that are consistent with their observations, that is, states ρ^{AB} satisfying

$$\Pr[O_{\mathcal{M}_A,\rho} = i, O_{\mathcal{M}_B,\rho} = j] = \mathrm{Tr}[(A_i \otimes B_j)\rho^{AB}] \quad \forall\, i, j,$$

where $\Pr[O_{\mathcal{M}_A,\rho} = i, O_{\mathcal{M}_B,\rho} = j]$ represents the observed statistics. The remaining error-correction and privacy amplification steps proceed as in PM protocols.

Source-Replacement Scheme

EB and PM protocols are equivalent since any PM protocol can be converted to an EB protocol by placing the entanglement source in Alice's lab. This conversion is done using the so-called *source-replacement scheme* and is described in [Lüt14]. The idea is to identify the ensemble $\{(p_i, |\psi_i\rangle)\}_i$ prepared by Alice with the state

$$|\psi\rangle^{AA'}_{\text{source}} := \sum_i \sqrt{p_i}\, |m_i\rangle^A \otimes |\psi_i\rangle^{A'},$$

where $\{|m_i\rangle\}_i$ is an orthonormal set, and let $\mathcal{M}_A = \{|m_i\rangle\langle m_i|\}_i$. Alice's measurement of the register A with this POVM effectively prepares the A' register in the required signal states with the correct probabilities, which is then sent to Bob. Any interaction by Eve while the signals are being sent to Bob will change the state from $|\psi\rangle^{AA'}_{\text{source}}$ to another state ρ^{AB}, which they must then estimate during parameter estimation as described above.

2.4.1 Attack Strategies

An attack strategy consists of a pair $(\mathcal{N}, \mathcal{M})$, where $\mathcal{N}$ represents Eve's interaction with the signals while they are travelling from Alice to Bob (in the PM scenario) or while the signals are being distributed amongst both of them (in the EB scenario), and $\mathcal{M}$ is a POVM describing the measurement Eve performs to gain information about the key bits. The interaction $\mathcal{N}$ is implemented by attaching a probe to the signal being sent and performing the interaction in the joint signal-and-probe system. The POVM $\mathcal{M}$ then measures the probe. Attack strategies are typically put into three classes[7].

[6] Typically, the communication in such protocols is also only in one direction, though this is not required. "One-way" simply refers to the fact that the raw key from only *one* of the parties is being used to establish the secret key.

[7] See also [BA07] for a concise summary of these attack strategies with some additional details not provided here.

Individual Attacks

Eve interacts with the signals individually and in the same way each time as they are being sent from Alice to Bob and measures her probes individually immediately after. For protocols that include a step called *sifting* to be described below, Eve might wait until the end of sifting before making her measurement.

Collective Attacks

Eve interacts with the signals individually and in the same way each time as they are being sent from Alice to Bob. Instead of measuring the probes individually, however, she measures them collectively. She might even wait until after the classical post-processing phase to do the measurement.

Coherent/Joint Attacks

Eve does not interact individually with the signals but uses a probe to interact with them coherently as one large entity. She then waits until a time of her choosing before measuring.

For the purpose of analyzing QKD protocols, it is common to use the entanglement-based picture. As mentioned above, Eve's interaction then results in a state $\rho^{AB} := (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{N})(|\psi\rangle\langle\psi|^{AA'}_{\text{source}})$ that Alice and Bob must estimate before proceeding to the one-way classical post-processing protocols. In individual and collective attacks, the state ρ^{AB} is of product form, $\rho^{AB} = (\sigma^{AB})^{\otimes n}$, where n is the number of signals distributed and σ^{AB} is the state describing the correlations between Alice and Bob for each signal. In coherent attacks, the state ρ^{AB} need not have product form and there could indeed be correlations between the different signals corresponding to Eve using her probe to interact with multiple signals at the same time.

Individual attacks are weaker than collective ones, so it is common nowadays to prove security against collective attacks. During parameter estimation, Alice and Bob can then simply estimate σ^{AB} corresponding to one signal. In fact, it was proved in [Ren05] (see also [Ren07; CKR09]) using the quantum de Finetti theorem that coherent attacks cannot be stronger than collective attacks for protocols that are symmetric in the different uses of the channel; in particular, for such protocols, security against collective attacks implies security against general coherent attacks. Therefore, for protocols that are symmetric in the use of the channel, the assumption of a collective attack, and hence of a product form for the state ρ^{AB}, does not give Eve an advantage.

Since in collective attacks Eve can arbitrarily delay her measurement, we assume that she has a quantum memory to store her quantum information. For the security analysis of QKD protocols, her quantum information, along with Alice and Bob's classical information, is described by an extension ρ^{ABE} to $\mathfrak{H}_E$ of ρ^{AB}, but since by Theorem 2.22 there exists a channel on the purification space that maps to ρ^{ABE} from a purification of ρ^{AB}, we make the worst-case assumption throughout this thesis that Eve's knowledge corresponds to a purification of ρ^{AB}.

Having estimated the state ρ^{AB} during parameter estimation, Alice and Bob must decide whether or not to continue to the one-way classical post-processing protocols to distill a secret key. The following important result in [MCL06] gives a condition under which a secret key definitely *cannot* be distilled by *any* one-way classical post-processing protocol.

Theorem 2.24 Symmetric Extendability and One-Way QKD [MCL06]

If Alice and Bob's measurement results are consistent with a state ρ^{AB} that has a symmetric extension to a copy of B, then there does not exist a one-way Alice-to-Bob classical post-processing protocol to distill a secret key.

PROOF: If ρ^{AB} is symmetrically extendable to $\rho^{ABB'}$, then by Theorem 2.22 there exists a channel on the purification space $\mathfrak{H}_E$ mapping a purification of ρ^{AB} to $\rho^{ABB'}$. Since the purification register E, and therefore B', is assumed to belong to Eve, it holds that Eve can perform a local quantum operation such that $\rho^{AB'} = \rho^{AB}$ by definition of symmetric extendability. Under one-way Alice-to-Bob communication, it therefore holds that Eve is just as knowledgeable about Alice's key information as Bob is, so that the resulting key is not secure. ■

As described in the introduction, it might be possible to break the symmetry between Bob and Eve resulting from a symmetrically extendable state ρ^{AB} by first performing a *two-way* post-processing protocol followed by the one-way Alice-to-Bob error-correction and privacy amplification protocols. The existence of such additional two-way post-processing protocols is the subject of this thesis.

It is worth mentioning that no classical post-processing protocol distilling secret key exists whenever ρ^{AB} is separable. One-way protocols do not exist by Theorem 2.24 above since all separable states are symmetrically extendable, as we will see in Chapter 3. Nor do two-way protocols exist that can break this symmetric extendability of separable states since separable states remain separable, and hence symmetrically extendable, after any two-way protocol. Separable states correspond to *intercept-resend attacks* in which Eve intercepts the signals being sent from Alice, measures them, and resends to Bob the signal corresponding to her measurement result.

2.4.2 Six-State Signal States

QKD protocols with the six-state signal states [Bru98; BG99] are defined by the following ensemble of six pure qubit states prepared by Alice:

$$|0\rangle, \quad |1\rangle, \quad |\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |\pm\mathrm{i}\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}\,|1\rangle). \tag{2.35}$$

Recalling the Pauli operators defined in equation (2.19), we have that the first two states $\{|0\rangle, |1\rangle\}$ are eigenvectors of σ_z, so we call them the *z-basis*; the second two states $\{|+\rangle, |-\rangle\}$ are eigenvectors of σ_x, so we call them the *x-basis*; the last two states $\{|+\mathrm{i}\rangle, |-\mathrm{i}\rangle\}$ are eigenvectors of σ_y, so we call them the *y-basis*. These three bases are pairwise *mutually-unbiased*, which is to say that all the outcomes of measurement in one basis of any state prepared in another basis have probability $\frac{1}{2}$.

The following analysis, as well as the analysis in §2.4.3 below, has been adapted from [Myh10]. Alice chooses with probabilities q_x^A, q_y^A, q_z^A a signal at random (with probability $\frac{1}{2}$) from the x-, y-, or z-basis, respectively, and sends it to Bob. Bob measures the signal using the POVM $\mathcal{M}_B = \{B_0^{(x)}, B_1^{(x)}, B_0^{(y)}, B_1^{(y)}, B_0^{(z)}, B_1^{(z)}\}$, where

$$\begin{aligned} B_0^{(x)} &:= q_x^B |+\rangle\langle+|, & B_1^{(x)} &:= q_x^B |-\rangle\langle-|, \\ B_0^{(y)} &:= q_y^B |+\mathrm{i}\rangle\langle+\mathrm{i}|, & B_1^{(y)} &:= q_y^B |-\mathrm{i}\rangle\langle-\mathrm{i}|, \\ B_0^{(z)} &:= q_z^B |0\rangle\langle0|, & B_1^{(z)} &:= q_z^B |1\rangle\langle1|. \end{aligned} \tag{2.36}$$

That is, Bob chooses with probabilities q_x^B, q_y^B, q_z^B to measure in either the x-, y-, or z-basis, respectively. The x, y, z superscripts on the POVM elements label the basis choice, and the $0, 1$ subscripts label the outcomes of the measurement in the chosen basis.

To get the equivalent EB protocol, we use the source-replacement scheme outlined above. The source state

on Alice is by definition

$$|\psi\rangle_{\text{source}}^{AA'} = \sqrt{\frac{q_x^A}{2}}\,|m_0\rangle \otimes |+\rangle + \sqrt{\frac{q_x^A}{2}}\,|m_1\rangle \otimes |-\rangle + \sqrt{\frac{q_y^A}{2}}\,|m_2\rangle \otimes |+\mathrm{i}\rangle + \sqrt{\frac{q_y^A}{2}}\,|m_3\rangle \otimes |-\mathrm{i}\rangle + \sqrt{\frac{q_z^A}{2}}\,|m_4\rangle \otimes |0\rangle + \sqrt{\frac{q_z^A}{2}}\,|m_5\rangle \otimes |1\rangle\,,$$

and measuring using the POVM $\{|m_i\rangle\langle m_i|\}_{i=0}^5$ prepares the A' register in the states to be sent to Bob through the channel. Due to the linear dependence of the signal states, however, we can write $|\psi\rangle_{\text{source}}^{AA'}$ as

$$|\psi\rangle_{\text{source}}^{AA'} = \frac{1}{\sqrt{2}}(|u_0\rangle \otimes |0\rangle + |u_1\rangle \otimes |1\rangle), \tag{2.37}$$

where

$$|u_0\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{q_x^A}\,|m_0\rangle + \sqrt{q_x^A}\,|m_1\rangle + \sqrt{q_y^A}\,|m_2\rangle + \sqrt{q_y^A}\,|m_3\rangle + \sqrt{2q_z^A}\,|m_4\rangle\right),$$
$$|u_1\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{q_x^A}\,|m_0\rangle - \sqrt{q_x^A}\,|m_1\rangle + \mathrm{i}\sqrt{q_y^A}\,|m_2\rangle - \mathrm{i}\sqrt{q_y^A}\,|m_3\rangle + \sqrt{2q_z^A}\,|m_5\rangle\right).$$

The state (2.37) is nothing but the Schmidt decomposition (recall Theorem 2.15) of $|\psi\rangle_{\text{source}}^{AA'}$. Since $|u_0\rangle$ and $|u_1\rangle$ are linearly independent and orthogonal, they span a two-dimensional subspace of $\mathfrak{H}_A$, so we can simply relabel them as $|0\rangle$ and $|1\rangle$, respectively, to get

$$|\psi\rangle_{\text{source}}^{AA'} = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \tag{2.38}$$

Therefore, instead of measuring using the POVM $\{|m_i\rangle\langle m_i|\}_{i=0}^5$, Alice can measure in the two-dimensional subspace using the POVM $\mathcal{M}_A := \{\Pi\,|m_i\rangle\langle m_i|\,\Pi^\dagger\}_{i=0}^5$, where $\Pi = |0\rangle\langle u_0| + |1\rangle\langle u_1|$ and

$$\Pi\,|m_0\rangle\langle m_0|\,\Pi^\dagger = q_x^A\,|+\rangle\langle +| =: A_0^{(x)}, \quad \Pi\,|m_1\rangle\langle m_1|\,\Pi^\dagger = q_x^A\,|-\rangle\langle -| =: A_1^{(x)},$$
$$\Pi\,|m_2\rangle\langle m_2|\,\Pi^\dagger = q_y^A\,|-\mathrm{i}\rangle\langle -\mathrm{i}| =: A_0^{(y)}, \quad \Pi\,|m_3\rangle\langle m_3|\,\Pi^\dagger = q_y^A\,|+\mathrm{i}\rangle\langle +\mathrm{i}| =: A_1^{(y)},$$
$$\Pi\,|m_4\rangle\langle m_4|\,\Pi^\dagger = q_z^A\,|0\rangle\langle 0| =: A_0^{(z)}, \quad \Pi\,|m_5\rangle\langle m_5|\,\Pi^\dagger = q_z^A\,|1\rangle\langle 1| =: A_1^{(z)},$$

where as before the x, y, z superscripts label the basis choice and the $0, 1$ subscripts label the outcomes of the measurement in the chosen basis. Therefore, measurements by Alice in either the x-, y-, or z-bases prepares a state in the same basis in the A' register. For the x- and z-bases, the prepared state is the same as the one left on the A register after the measurement, while for the y-basis the prepared state is opposite to the one left in the A register after measurement.

An additional step, which occurs either before or after parameter estimation, is called *sifting*. In sifting, Alice and Bob, through discussion over the classical channel, announce their basis choices and discard those signals for which their basis choices did not coincide.

Parameter Estimation

After Alice's measurement, the register A' is sent to Bob, giving an eavesdropper the opportunity to interact with it. This means that once Bob has received the signals and made his measurement the correlations between

Alice and Bob will be described by the state $\rho^{AB} = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{N})(|\psi\rangle\langle\psi|^{AA'}_{\text{source}})$, where $\mathcal{N}$ is the interaction and $|\psi\rangle^{AA'}_{\text{source}}$ is as written in (2.38)[8]. Using (2.26), we have that any quantum state ρ^{AB} can be written in the Pauli operator basis as

$$\rho^{AB} = \frac{1}{4}\sum_{i,j=0}^{3} \alpha_{i,j}(\rho^{AB})\sigma_i^A \otimes \sigma_j^B, \quad \alpha_{i,j}(\rho^{AB}) = \mathrm{Tr}[\rho^{AB}(\sigma_i^A \otimes \sigma_j^B)],$$

where by normalization $\alpha_{0,0}(\rho^{AB}) = 1$. This leaves Alice and Bob with 15 parameters to estimate, which they can do since $\alpha_{i,j}(\rho^{AB})$ is nothing but the expectation value of their measurements of the corresponding Pauli operator. In particular, by observing that

$$\sigma_i^A = \frac{1}{q_i^A}\left(A_0^{(i)} - A_1^{(i)}\right) \quad \forall\, i \neq 0,$$
$$\sigma_j^B = \frac{1}{q_j^B}\left(B_0^{(j)} - B_1^{(j)}\right) \quad \forall\, j \neq 0,$$

we have

$$\alpha_{i,j}(\rho^{AB}) = \frac{\mathrm{Tr}\left[\rho^{AB}(A_0^{(i)} - A_1^{(i)}) \otimes (B_0^{(j)} - B_1^{(j)})\right]}{q_i^A q_j^B} = \frac{p_{0,0}^{(i,j)} - p_{0,1}^{(i,j)} - p_{1,0}^{(i,j)} + p_{1,1}^{(i,j)}}{q_i^A q_j^B} \quad \forall\, i,j \neq 0, \tag{2.39}$$

where

$$p_{k,\ell}^{(i,j)} \equiv \mathrm{Tr}[\rho^{AB}(A_k^{(i)} \otimes B_\ell^{(j)})] = \Pr\left[(O_{\mathcal{M}_A,\rho} = k,\ O_{\mathcal{M}_B,\rho} = \ell) \bigcap \begin{pmatrix} \text{Alice chose basis } i, \\ \text{Bob chose basis } j \end{pmatrix}\right].$$

The remaining coefficients with either $i = 0$ or $j = 0$ can be determined using the fact that

$$A_0^{(i)} + A_1^{(i)} = q_i^A \mathbb{1}_A \quad \text{and} \quad B_0^{(i)} + B_1^{(i)} = q_i^B \mathbb{1}_B \quad \forall\, i \in \{x,y,z\}.$$

An important quantity is the *quantum bit-error rate (QBER)* Q_i, which is defined as the probability that Alice and Bob disagree on their measurement outcome given that they measured in the same basis i. It is equal to

$$\begin{aligned} Q_i &\coloneqq \Pr\left[\left(O_{\mathcal{M}_A,\rho} \neq O_{\mathcal{M}_B,\rho}\right) \middle| (\text{Alice, Bob chose basis } i)\right] \\ &= \frac{\Pr\left[(\text{Alice, Bob chose basis } i) \bigcap \left(O_{\mathcal{M}_A,\rho} \neq O_{\mathcal{M}_B,\rho}\right)\right]}{\Pr\left[\text{Alice, Bob chose basis } i\right]} \\ &= \frac{\Pr\left[(\text{Alice, Bob chose basis } i) \bigcap \left(O_{\mathcal{M}_A,\rho} = 0, O_{\mathcal{M}_B,\rho} = 1\right)\right]}{q_i^A q_i^B} \\ &\quad + \frac{\Pr\left[(\text{Alice, Bob chose basis } i) \bigcap \left(O_{\mathcal{M}_A,\rho} = 1, O_{\mathcal{M}_B,\rho} = 0\right)\right]}{q_i^A q_i^B} \end{aligned} \tag{2.40}$$

$$\Rightarrow \boxed{Q_i = \frac{p_{0,1}^{(i,i)} + p_{1,0}^{(i,i)}}{q_i^A q_i^B} \quad \forall\, i \in \{x,y,z\}.}$$

The states ρ^{AB} with which we are interested in this thesis are those that arise from Eve performing a Pauli channel interaction $\Psi_{\vec{p}}$ as defined in (2.18). We have then that the state ρ^{AB}, which is proportional to the

[8] Since (2.38) is nothing but the state $|\Phi^+\rangle$, ρ^{AB} is simply proportional to the Choi representation of $\mathcal{N}$.

Choi representation of $\Psi_{\vec{p}}$, is Bell-diagonal. Since Bell-diagonal states can be written in the form (2.27), the Bell-diagonal state consistent with the measurement outcomes of Alice and Bob is

$$\rho^{AB} = \frac{1}{4}\sum_{i=0}^{3} \alpha_{i,i}(\rho^{AB})\sigma_i^A \otimes \sigma_i^B,$$

where by using (2.39)

$$\begin{aligned}\alpha_{i,i}(\rho^{AB}) &= \frac{\mathrm{Tr}[\rho^{AB}(A_0^{(i)} - A_1^{(i)}) \otimes (B_0^{(i)} - B_1^{(i)})]}{q_i^A q_i^B} \\ &= \frac{p_{0,0}^{(i,i)} - p_{0,1}^{(i,i)} - p_{1,0}^{(i,i)} + p_{1,1}^{(i,i)}}{q_i^A q_i^B} = \frac{p_{0,0}^{(i,i)} + p_{1,1}^{(i,i)}}{q_i^A q_i^B} - Q_i \\ &= \frac{p_{0,0}^{(i,i)} + p_{0,1}^{(i,i)} + p_{1,0}^{(i,i)} + p_{1,1}^{(i,i)}}{q_i^A q_i^B} - 2Q_i.\end{aligned}$$

But

$$p_{0,0}^{(i,i)} + p_{0,1}^{(i,i)} + p_{1,0}^{(i,i)} + p_{1,1}^{(i,i)} = \mathrm{Tr}\Big[\rho^{AB} \underbrace{(A_0^{(i)} + A_1^{(i)})}_{q_i^A \mathbb{1}_A} \otimes \underbrace{(B_0^{(i)} + B_1^{(i)})}_{q_i^B \mathbb{1}_B}\Big] = q_i^A q_i^B.$$

Therefore,

$$\alpha_{i,i}(\rho^{AB}) = 1 - 2Q_i \quad \forall\, i \in \{1,2,3\}.$$

Therefore, in the case of a Pauli channel interaction[9], it is enough for Alice and Bob to estimate the three QBERs Q_i in order to estimate ρ^{AB} instead of the usual 15 parameters. This also means that they can perform sifting before parameter estimation. In the Bell basis, ρ^{AB} has the form

$$\begin{aligned}\rho_{\vec{Q}}^{AB} := &\left(1 - \frac{1}{2}(Q_x + Q_y + Q_z)\right)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1}{2}(Q_z - Q_x + Q_y)\left|\Psi^+\right\rangle\left\langle\Psi^+\right| \\ &+ \frac{1}{2}(Q_x - Q_y + Q_z)\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{1}{2}(Q_y - Q_z + Q_x)\left|\Phi^-\right\rangle\left\langle\Phi^-\right|.\end{aligned} \tag{2.41}$$

In other words, the noise parameters $\vec{p} = (p_x, p_y, p_z)$ characterizing the Pauli channel interaction are

$$p_x = \frac{1}{2}(Q_z - Q_x + Q_y), \quad p_y = \frac{1}{2}(Q_x - Q_y + Q_z), \quad p_z = \frac{1}{2}(Q_y - Q_z + Q_x).$$

If in addition to the assumption of a Pauli channel interaction we take $Q_x = Q_y = Q_z = Q$, that is, equal QBER in each basis, then we get

$$\begin{aligned}\rho_Q^{AB} &:= \left(1 - \frac{3}{2}Q\right)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2}\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2}\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{Q}{2}\left|\Phi^-\right\rangle\left\langle\Phi^-\right| \\ &= (1-2Q)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2}\mathbb{1}_A \otimes \mathbb{1}_B,\end{aligned} \tag{2.42}$$

which is the isotropic state (2.25). The Pauli channel giving rise to this state is the depolarizing channel Δ_Q. This noise model with equal QBER in each basis is the most commonly analyzed one for the six-state protocol,

[9]We do not have to assume, as implied here, that Eve performs a Pauli interaction. As described in [BA07; Myh10], before measuring their particles Alice and Bob can perform a symmetrization procedure called *twirling* that takes any state and makes it Bell-diagonal, effectively making Eve's interaction a Pauli channel.

and it will be the focus of this thesis[10]. As seen before, positive semi-definiteness of the state requires that $0 \leq Q \leq \frac{2}{3}$, although in this case it is enough to let $0 \leq Q \leq \frac{1}{2}$ since the classical *mutual information* between Alice and Bob's measurement results based on a single copy of the state ρ_Q^{AB} is equal to [Bru98] $1 + Q\log_2(Q) + (1-Q)\log_2(1-Q)$, which vanishes[11] at $Q = \frac{1}{2}$.

In the case of equal QBER in each basis, in order to distill a secret key after parameter estimation using one-way post-processing protocols, by Theorem 2.24 ρ_Q^{AB} must not have a symmetric extension. In Chapter 3, we will see that

$$\mathrm{Tr}[(\rho^B)^2] \geq \mathrm{Tr}[(\rho^{AB})^2] - 4\sqrt{\det(\rho^{AB})} \tag{2.43}$$

is necessary and sufficient for the symmetric extendabiliy of any two-qubit state $\rho^{AB} \in \mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. By applying this condition to ρ_Q^{AB}, we get

$$\frac{1}{2} \geq \left(1 - \frac{3Q}{2}\right)^2 + 3\left(\frac{Q}{2}\right)^2 - 4\sqrt{\left(1 - \frac{3Q}{2}\right)\left(\frac{Q}{2}\right)^3},$$

which can be simplified to

$$\frac{1}{4}(2Q-1)^3(6Q-1) \leq 0.$$

This holds for $Q \geq \frac{1}{6}$, which means that ρ_Q^{AB} is symmetrically extendable beyond $Q = \frac{1}{6}$. In other words, beyond $Q = \frac{1}{6}$, the one-way error-correction and privacy amplification protocols will not lead to a secret key.

As well, by the PPT criterion, we get that ρ_Q^{AB} is separable for all $Q \geq \frac{1}{3}$, which means that beyond $Q = \frac{1}{3}$ neither a one-way nor a two-way protocol can be used to distill a secret key.

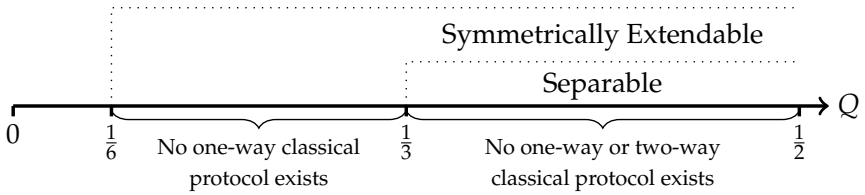


Figure 2.2: Properties of the isotropic state ρ_Q^{AB} characterizing the Alice-Bob correlations for QKD protocols using the six-state signal states with equal QBER in each basis.

2.4.3 BB84 Signal States

QKD protocols with the BB84 [BB84] signal states are defined by the following ensemble of four pure qubit states prepared by Alice:

$$|0\rangle, \quad |1\rangle, \quad |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle).$$

[10] For each signal, Alice and Bob hold two pieces of information: the basis choice and the measurement result in the chosen basis (for PM protocols, Alice holds for each signal the basis choice and the signal sent from that basis). The case of equal QBER in each basis that we consider here is equivalent to Alice and Bob *forgetting their basis choice* and considering only the *average QBER* $Q = \frac{Q_x+Q_y+Q_z}{3}$ since this gives rise to the same state ρ_Q^{AB} characterizing Alice and Bob's correlations. See §2.2.7 of [Myh10] for details.

[11] The mutual information between Alice and Bob is needed to calculate the rate of secret key distillation; if it vanishes, then no secret key is possible.

They are the first four of the six-state signal states corresponding to the mutually-unbiased x- and z-bases. Alice sends with probabilities q_x^A, q_z^A a signal at random (with probability $\frac{1}{2}$) from one of the two bases. The POVM $\mathcal{M}_B$ used by Bob to measure the signal sent to him from Alice is

$$B_0^{(x)} = q_x^B \left|+\right\rangle \left\langle+\right|, \quad B_1^{(x)} = q_x^B \left|-\right\rangle \left\langle-\right|,$$
$$B_0^{(z)} = q_z^B \left|0\right\rangle \left\langle 0\right|, \quad B_1^{(z)} = q_z^B \left|1\right\rangle \left\langle 1\right|.$$

Passing to the equivalent EB protocol using the source-replacement scheme is done similarly to the six-state signal states. The source state is

$$\begin{aligned}\left|\psi\right\rangle_{\text{source}}^{AA'} &= \sqrt{\frac{q_x^A}{2}} \left|m_0\right\rangle^A \otimes \left|+\right\rangle^{A'} + \sqrt{\frac{q_x^A}{2}} \left|m_1\right\rangle^A \otimes \left|-\right\rangle^{A'} + \sqrt{\frac{q_z^A}{2}} \left|m_2\right\rangle^A \otimes \left|0\right\rangle^{A'} + \sqrt{\frac{q_z^A}{2}} \left|m_3\right\rangle^A \otimes \left|1\right\rangle^{A'} \\ &= \frac{1}{\sqrt{2}}(\left|u_0\right\rangle \otimes \left|0\right\rangle + \left|u_1\right\rangle \otimes \left|1\right\rangle),\end{aligned}$$

where

$$\begin{aligned}\left|u_0\right\rangle &= \frac{1}{\sqrt{2}} \left(\sqrt{q_x^A} \left|m_0\right\rangle + \sqrt{q_x^A} \left|m_1\right\rangle + \sqrt{2q_z^A} \left|m_2\right\rangle \right), \\ \left|u_1\right\rangle &= \frac{1}{\sqrt{2}} \left(\sqrt{q_x^A} \left|m_0\right\rangle - \sqrt{q_x^A} \left|m_1\right\rangle + \sqrt{2q_z^A} \left|m_3\right\rangle \right).\end{aligned}$$

As with the six-state signal states, $\left|u_0\right\rangle$ and $\left|u_1\right\rangle$ are linearly independent and orthogonal, so we can write $\left|\psi\right\rangle_{\text{source}}^{AA'} = \frac{1}{\sqrt{2}}(\left|0\right\rangle \otimes \left|0\right\rangle + \left|1\right\rangle \otimes \left|1\right\rangle)$, so that the POVM $\{\left|m_i\right\rangle \left\langle m_i\right|\}_{i=0}^3$ projected onto the two-dimensional subspace of A spanned by $\left|u_0\right\rangle, \left|u_1\right\rangle$ is

$$A_0^{(x)} = q_x^A \left|+\right\rangle \left\langle+\right|, \quad A_1^{(x)} = q_x^A \left|-\right\rangle \left\langle-\right|,$$
$$A_0^{(z)} = q_z^A \left|0\right\rangle \left\langle 0\right|, \quad A_1^{(z)} = q_z^A \left|1\right\rangle \left\langle 1\right|.$$

The sifting step is done in exactly the same way as with the six-state signal states.

In the parameter estimation step, since Alice does not send signals from the y-basis nor does Bob measure in the y-basis, the POVMs $\mathcal{M}_A, \mathcal{M}_B$ do not allow Alice and Bob to uniquely estimate the state ρ^{AB} since determining the parameters $\alpha_{2,i}(\rho^{AB})$ and $\alpha_{i,2}(\rho^{AB})$ for all $0 \leq i \leq 3$ requires a y-basis measurement. In particular, the y-basis QBER Q_y cannot be estimated. Assuming as before a Pauli channel interaction with $Q_x = Q_z = Q$, and letting $x := Q - \frac{Q_y}{2}$, we get from (2.41)[12]

$$\rho_{Q,x}^{AB} := (1 - 2Q + x) \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + (Q - x) \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + x \left|\Psi^-\right\rangle \left\langle\Psi^-\right| + (Q - x) \left|\Phi^-\right\rangle \left\langle\Phi^-\right|. \tag{2.44}$$

The classical mutual information between Alice and Bob's measurement results is the same for $\rho_{Q,x}^{AB}$ as for ρ_Q^{AB}, which means that we again only consider Q in the interval $\left[0, \frac{1}{2}\right]$. For $\rho_{Q,x}^{AB}$ to be positive semi-definite, we therefore require $x \in [0, Q]$ for all $0 \leq Q \leq \frac{1}{2}$.

Unlike protocols using the six-state signal states, in which for each Q there exists only one state ρ_Q^{AB} consistent with Alice and Bob's measurement results, we see that in protocols using the BB84 signal states there exists for each Q a set $\{\rho_{Q,x}^{AB}\}_{x \in [0,Q]}$ of states consistent with Alice and Bob's measurement results. This means

[12] As with the six-state signal states, forgetting the basis choice and considering the average QBER will lead to the same state $\rho_{Q,x}^{AB}$ characterizing Alice and Bob's correlations.

that to use Theorem 2.24 to determine, as with the six-state signal states, the threshold QBER beyond which one-way classical post-processing protocols will not distill a secret key, we must find the highest QBER Q for which the set $\{\rho^{AB}_{Q,x}\}_{x\in[0,Q]}$ does not contain a symmetrically extendable state. Applying the condition (2.43) to $\rho^{AB}_{Q,x}$ tells us that $\rho^{AB}_{Q,x}$ is symmetrically extendable if and only if

$$\frac{1}{2} \geq (1-2Q+x)^2 + 2(Q-x)^2 + x^2 - 4\sqrt{(1-2Q+x)(Q-x)^2 x},$$

which can be simplified to

$$\frac{1}{4}(1-2Q)^2(36Q^2 - 64Qx - 12Q + 32x^2 + 8x + 1) \leq 0.$$

Since $(1-2Q)^2$ is always non-negative, we seek the largest Q such that $F_Q(x) := 36Q^2 - 64Qx - 12Q + 32x^2 + 8x + 1 > 0$ for all $0 \leq x \leq Q$. F_Q is a quadratic function of x for all Q and is in fact convex (or "concave up", which is due to the fact that $F''_Q(x) = 64$ for all x), which means that the positivity of F_Q can be determined by the number of its roots, which in turn can be determined by its discriminant, which is

$$(8-64Q)^2 - 4(32)(36Q^2 - 12Q + 1).$$

F_Q will be positive if it has no real roots, which is when the discriminant is negative, that is, when

$$(8-64Q)^2 - 4(32)(36Q^2 - 12Q + 1) < 0 \Rightarrow -8Q^2 + 8Q - 1 < 0 \Rightarrow Q < \frac{2-\sqrt{2}}{4} \approx 14.64\%.$$

This means that for all $Q \geq \frac{2-\sqrt{2}}{4}$ there exists x such that $\rho^{AB}_{Q,x}$ has a symmetric extension, so that for this range a secret key cannot be distilled by one-way classical post-processing protocols.

We must also find the highest QBER Q for which the set $\{\rho^{AB}_{Q,x}\}_{x\in[0,Q]}$ does not contain a separable state as this will give us an interval of the QBER in which there exists an intercept-resend attack that excludes secret key distillation by any post-processing protocol. Using the PPT criterion, we find that $\rho^{AB}_{Q,x}$ is *entangled* whenever $\left(\rho^{AB}_{Q,x}\right)^{\mathsf{T}_B}$ is *negative*, which is when at least one of the eigenvalues of $\left(\rho^{AB}_{Q,x}\right)^{\mathsf{T}_B}$, which are

$$\frac{1}{2} - x, \quad 2Q - x - \frac{1}{2}, \quad x - Q + \frac{1}{2},$$

is negative. $\frac{1}{2} - x < 0$ is never satisfied since x can only be in the interval $[0, Q]$ and we don't consider any Q beyond $\frac{1}{2}$. Similarly, $Q \leq \frac{1}{2}$ means that $x - Q + \frac{1}{2} < 0$ will also never be satisfied. Negativity of the second eigenvalue gives $x > 2Q - \frac{1}{2}$, which means that the second eigenvalue will be negative for all $x \in [0, Q]$ if and only if $2Q - \frac{1}{2} < 0 \Rightarrow Q < \frac{1}{4}$. Therefore, for all Q less than $\frac{1}{4}$ the second eigenvalue will be negative for all $x \in [0, Q]$, which means that $\rho^{AB}_{Q,x}$ will be entangled for all $x \in [0, Q]$. For $Q \geq \frac{1}{4}$, there exists x such that $\rho^{AB}_{Q,x}$ is separable, hence no post-processing protocol can be used to distill a secret key in this range.

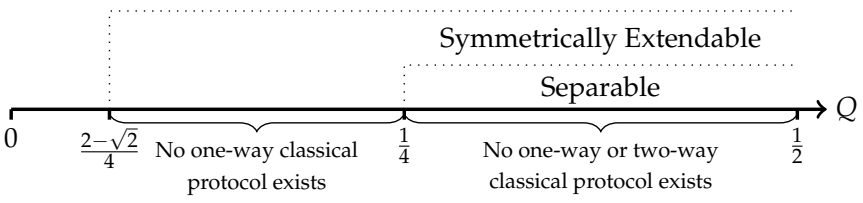


Figure 2.3: Properties of the state $\rho^{AB}_{Q,x}$ characterizing the Alice-Bob correlations for QKD protocols using the BB84 signal states with equal QBER in each basis.

2.4.4 Classical and Quantum Post-Processing Protocols

So far, QKD protocols have been described as having a quantum phase and a classical phase. The quantum phase, which can be either prepare-and-measure-based or entanglement-based, involves distribution and measurement of quantum signals. The classical phase consists of some classical post-processing protocol, typically error-correction and privacy amplification, which leads to a secret key as long as Eve's initial information from the quantum phase is not too high.

It is worth mentioning, as done in [BA07], that QKD protocols with entanglement-based quantum phase can be modified in the following way. Instead of having Alice and Bob measure their particle-pairs immediately after receiving them and then performing a classical post-processing protocol, they can retain them and sacrifice some of them to test whether or not they are entangled. If they are, then they can continue with *entanglement distillation/quantum privacy amplification* [Ben+96b; Ben+96a; BB85; Deu+96] to transform the states of the remaining particle-pairs to several (potentially fewer) copies of the maximally entangled state $|\Phi^+\rangle$. They can then measure each of these particles in the z-basis and obtain the same completely random and secure key.

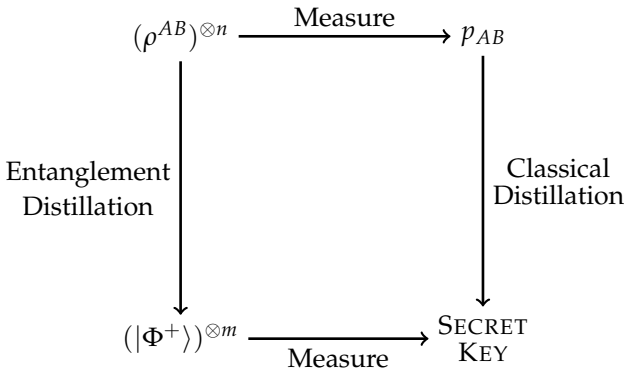


Figure 2.4: Quantum and classical post-processing protocols for distilling secret key from entangled states. Starting with n copies of the entangled state ρ^{AB}, Alice and Bob can perform the quantum entanglement distillation protocol, which takes the n copies of ρ^{AB} and produces some $m < n$ copies of $|\Phi^+\rangle$ states, which can then be measured to yield a secret key. Alternatively, Alice and Bob can first measure their states, leading to a joint probability distribution p_{AB} from which classical distillation methods (like error-correction and privacy amplification) can lead to a secret key. (Adapted from [BA07].)

Entanglement distillation protocols are examples of protocols involving local (quantum) operations and classical communication (LOCC). The classical communication can be either one-way or two-way. The symmetric extendability of the initial state ρ^{AB} is not relevant when Alice and Bob perform entanglement distillation since the protocol is defined by the condition that at the end of the protocol they end with copies of the pure maximally entangled state $|\Phi^+\rangle$. On the other hand, classical distillation protocols fall under the class of protocols involving local operations and public communication (LOPC). A general analysis and comparison of the LOCC and LOPC classes of protocols is done in [Chr+07; Hor+09] (see also [CP02]).

Entanglement distillation is an alternative route to secret key distillation from classical distillation. Remarkably, however, by adapting the ideas of entanglement distillation protocols for use in a classical setting [LC99] and by using the equivalence of one-way entanglement distillation protocols and quantum error correction [Ben+96a], Shor and Preskill obtained their well-known proof of the security of QKD with the BB84 signal states and one-way classical post-processing [SP00]. The analogous proof of security with the six-state

signal states was provided by Lo [Lo01]. In fact, the work by Gottesman and Lo [GL03] and Chau [Cha02] leading to the current best bounds for QKD with the BB84 and six-state signal states with two-way classical post-processing was done using this entanglement distillation proof technique modified to hold in the two-way scenario.

Of course, classical post-processing protocols can be analyzed by using classical information-theoretic tools directly. One of the earliest proofs of this type for QKD with the BB84 signal states and one-way communication was in [Ben02], with subsequent proofs for more general protocols under one-way communication in [Mat04; RGK05; KGR05] (see also [Ren05]). Each of these security proofs reproduced the BB84 threshold QBER determined by Shor-Preskill. In the two-way communication scenario, [Ren05; Ací+06; BA07; KBR07] used information-theoretic tools to prove security of QKD with the BB84 and six-state signal states with the additional advantage distillation protocol [Mau93] before error-correction and privacy amplification, and they obtained the same current best upper bounds as Chau.

As outlined in Chapter 4, though we are interested in two-way classical post-processing protocols, our approach to finding two-way protocols that are better than advantage distillation is based only on breaking the symmetric extendability of the initial state ρ_{Q}^{AB}. As a result, we are not concerned with efficiencies nor with key rates achieved by the protocols, as was the case with the aforementioned security proofs. As we will see, this allows us to greatly simplify the problem of finding two-way protocols in the gap, reducing it to simply checking the symmetric extendability of a broad class of quantum states corresponding to Alice and Bob's updated correlations after an effective post-selection protocol.

Chapter 3

Symmetrically Extendable States

In this chapter, we formally define the notion of symmetric extendability of a positive semi-definite operator and go through some of the relevant properties of symmetrically extendable states. We will write down a semi-definite program (SDP) that can be used to determine the symmetric extendability of an arbitrary positive semi-definite operator and will draw the connection between symmetrically extendable operators and anti-degradable CP maps that is crucial to many of the results of this thesis. Finally, we will look at a special way of constructing symmetric extensions.

3.1 Definition and Properties

Definition 3.1 Symmetrically Extendable Operator

An operator $P^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ is called *symmetrically extendable to a copy of B* if there exists an extension $P^{ABB'} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B \otimes \mathfrak{H}_{B'})$ of P^{AB} to $\mathfrak{H}_{B'}$, with $d_{B'} = d_B$, such that

$$\mathrm{Tr}_B[P^{ABB'}] = P^{AB}.$$

An equivalent definition is the following: $X^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ is called symmetrically extendable to a copy of B if there exists an extension $X^{ABB'} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B \otimes \mathfrak{H}_{B'})$ of X^{AB} to $\mathfrak{H}_{B'}$, with $d_{B'} = d_B$, such that

$$(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathrm{SWAP}_{BB'}) X^{ABB'} (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathrm{SWAP}_{BB'})^\dagger = X^{ABB'},$$

that is, $X^{ABB'}$ is invariant under swapping of B and B', where

$$\mathrm{SWAP}_{BB'} \coloneqq \sum_{i,j=0}^{d_B-1} |j,i\rangle\langle i,j| \in \mathrm{L}(\mathfrak{H}_B \otimes \mathfrak{H}_{B'}, \mathfrak{H}_{B'} \otimes \mathfrak{H}_B). \tag{3.1}$$

This definition of a symmetrically extendable operator is equivalent to the one provided since for any extension $X^{ABB'}$ invariant under swapping of B and B' we have that

$$\mathrm{Tr}_B[X^{ABB'}] = \mathrm{Tr}_{B'}[X^{ABB'}] = X^{AB},$$

with the last equality following by definition of $X^{ABB'}$ being an extension of X^{AB} to $\mathfrak{H}_{B'}$. Conversely, for any symmetric extension $P^{ABB'}$ satisfying the definition provided,

$$\frac{P^{ABB'} + (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathrm{SWAP}_{BB'}) P^{ABB'} (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathrm{SWAP}_{BB'})^\dagger}{2}$$

is invariant under swapping of B and B'.

From now on, throughout this thesis, by *symmetrically extendable* we will always mean symmetrically extendable to an operator on a copy of the second tensor factor. The set of symmetrically extendable operators in $\mathrm{Pos}(\mathfrak{H} \otimes \mathfrak{K})$ will be denoted $\mathrm{SymExt}(\mathfrak{H}, \mathfrak{K})$. In the following, we discuss properties of symmetrically extendable states relevant to this thesis. More information can be found in [ML09] (see also [Myh10]).

$\mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ is convex since for any $P_1^{AB}, P_2^{AB} \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ with symmetric extensions $P_1^{ABB'}$ and $P_2^{ABB'}$ it holds that $P^{AB} := pP_1^{AB} + (1-p)P_2^{AB}$ has symmetric extension $P^{ABB'} := pP_1^{ABB'} + (1-p)P_2^{ABB'}$ for all $p \in [0,1]$, so that $P^{AB} \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$. SymExt is also a *cone*, meaning that for any symmetrically extendable P, the operator αP is symmetrically extendable for all $\alpha \geq 0$.

All separable states are symmetrically extendable, since for any separable state

$$\rho^{AB} = \sum_{i=1}^{n} p_i \tau_i^A \otimes \xi_i^B$$

one has the symmetric extension

$$\rho^{ABB'} = \sum_{i=1}^{n} p_i \tau_i^A \otimes \xi_i^B \otimes \xi_i^{B'}.$$

This means that all states without symmetric extension must be entangled[1].

$\mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ is preserved under local unitaries, for if $V \in \mathrm{U}(\mathfrak{H}_A)$ and $W \in \mathrm{U}(\mathfrak{H}_B)$, then for all $P \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$

$$Q^{AB} := (V \otimes W) P^{AB} (V \otimes W)^\dagger$$

has symmetric extension

$$Q^{ABB'} := (V \otimes W \otimes W) P^{ABB'} (V \otimes W \otimes W)^\dagger,$$

where $P^{ABB'}$ is a symmetric extension of P^{AB}. More generally, $\mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ is preserved under any channel acting locally on $\mathfrak{H}_B$ and any CP map acting locally on $\mathfrak{H}_A$, that is, for all $P^{AB} \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$,

$$Q^{AB} := (\Phi \otimes \Psi)(P^{AB})$$

has symmetric extension

$$Q^{ABB'} := (\Phi \otimes \Psi \otimes \Psi)(P^{ABB'})$$

for all $\Phi \in \mathrm{CP}(\mathfrak{H}_A)$ and all $\Psi \in \mathrm{C}(\mathfrak{H}_B)$, where $P^{ABB'}$ is a symmetric extension of P^{AB}. Even more generally, $\mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ is preserved under one-way $A \to B$ LOCC channels [NH09] since such channels are of the form [Wat16]

$$\Xi = \sum_{a \in I} \Phi_a \otimes \Psi_a$$

for some finite set I, a collection $\{\Phi_a : a \in I\} \subset \mathrm{CP}(\mathfrak{H}_A)$ satisfying $\sum_{a \in I} \Phi_a \in \mathrm{C}(\mathfrak{H}_A)$ and a collection $\{\Psi_a : a \in I\} \subseteq \mathrm{C}(\mathfrak{H}_B)$.

[1] The separability of states turns out to be connected to the *infinitely symmetrically extendable* states, that is, to states that can be extended to arbitrarily many copies of B, not just to one copy of B. See [DPS02; DPS04] for more information.

The following theorem uses the correspondence between CP maps and positive semi-definite operators of Theorem 2.7 to draw a correspondence between anti-degradable CP maps and symmetrically extendable positive semi-definite operators. In particular, it tells us that $P \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ is symmetrically extendable if and only if its corresponding CP map $\Phi_P \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$ is anti-degradable.

Theorem 3.2

For every anti-degradable $\Phi \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$ there exists $P_\Phi \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$. Conversely, for every $P \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ there exists an anti-degradable $\Phi_P \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_B)$.

PROOF: Suppose Φ is anti-degradable with degrading channel $\mathcal{E} \in \mathrm{C}(\mathfrak{H}_E, \mathfrak{H}_{B'})$, where $d_{B'} = d_B$ and $d_E \geq \mathrm{rank}(J(\Phi))$. Let $P_\Phi^{AB} := J(\Phi)$. By Theorem 2.7, $P_\Phi^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$. Then, letting $|\psi\rangle_\Phi^{ABE}$ be a purification of P_Φ^{AB} in $\mathfrak{H}_E$, define

$$P_\Phi^{ABB'} := (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{AB})} \otimes \mathcal{E})(|\psi\rangle\langle\psi|_\Phi^{ABE}).$$

Since $\mathcal{E}$ is trace-preserving, it holds that $P_\Phi^{ABB'}$ is an extension of P_Φ^{AB} to $\mathfrak{H}_{B'}$. By Proposition 2.18,

$$\mathrm{Tr}_B[P_\Phi^{ABB'}] = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{E})\big(\underbrace{\mathrm{Tr}_B[|\psi\rangle\langle\psi|_\Phi^{ABE}]}_{J(\Phi^c)}\big) = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{E})(J(\Phi^c)) = J(\mathcal{E} \circ \Phi^c) = J(\Phi) = P_\Phi^{AB},$$

where the second-last equality holds due to the anti-degradability of Φ. So $P_\Phi^{AB} \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ with symmetric extension $P_\Phi^{ABB'}$.

Conversely, suppose $P^{AB} \in \mathrm{SymExt}(\mathfrak{H}_A, \mathfrak{H}_B)$ with symmetric extension $P^{ABB'} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B \otimes \mathfrak{H}_{B'})$. By Theorem 2.7 and (2.12), the map $\Phi_P \in \mathrm{T}(\mathfrak{H}_A, \mathfrak{H}_B)$ defined by

$$\Phi_P(X) = \mathrm{Tr}_A[(X^\mathsf{T} \otimes \mathbb{1}_B)P^{AB}] \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_A)$$

is completely-positive. Let $|\psi\rangle^{ABB'R}$ be a purification of $P^{ABB'}$ in $\mathfrak{H}_R$. It is also a purification of P^{AB} in $\mathfrak{H}_{B'} \otimes \mathfrak{H}_R$. By Proposition 2.18, $P^{AB'R} = \mathrm{Tr}_B[|\psi\rangle\langle\psi|^{ABB'R}] = J(\Phi_P^c)$, where $\Phi_P^c \in \mathrm{CP}(\mathfrak{H}_A, \mathfrak{H}_{B'} \otimes \mathfrak{H}_R)$ is a map complementary to Φ_P. Then, defining the channel $\mathcal{E} = \mathrm{Tr}_R$, we get that

$$J(\mathcal{E} \circ \Phi_P^c) = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{E})(J(\Phi_P^c)) = \mathrm{Tr}_R[P^{AB'R}] = P^{AB'} = P^{AB} = J(\Phi_P),$$

where we have used the fact that $P^{ABB'}$ is a symmetric extension of P^{AB}, so that $P^{AB'} = P^{AB}$. Since Choi representations of maps uniquely specify them, we have that $\mathcal{E} \circ \Phi_P^c = \Phi_P$, that is, Φ_P is anti-degradable. ■

There are two known analytical results about the existence of symmetric extensions. First is the one conjectured and proved for rank-2, Bell-diagonal, and $\sigma_z \otimes \sigma_z$-invariant two-qubit states in [ML09; Myh10], and later proved for arbitrary two-qubit states in [Che+14].

Theorem 3.3 Symmetric Extendability in $\mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ [Che+14]

A state $\rho^{AB} \in \mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is symmetrically extendable if and only if

$$\mathrm{Tr}[(\rho^B)^2] \geq \mathrm{Tr}[(\rho^{AB})^2] - 4\sqrt{\det(\rho^{AB})}. \tag{3.2}$$

The second result is in [Ran09] and pertains to states in $\mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ for any integer $d \geq 2$ with a certain symmetry. We will state and use the result in Chapter 6.

Since existence criteria for symmetric extendability do not exist for arbitrary quantum states, we will use two different strategies in this thesis to determine the symmetric extendability of a state for which no existence criteria exist: numerically searching using semi-definite programming, and attempting to explicitly construct a symmetric extension.

3.2 Symmetric Extendability as an SDP

The following semi-definite program (SDP) [Wat16; Myh10; VB96] can be used to determine the symmetric extendability of any $P^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$.

$$\begin{aligned} &\text{min.} && t \\ &\text{subject to} && R^{ABB'} + t\mathbb{1}^{ABB'} \geq 0, \\ &&& \mathrm{Tr}_B[R^{ABB'}] = P^{AB}, \\ &&& \mathrm{Tr}_{B'}[R^{ABB'}] = P^{AB}. \end{aligned} \tag{3.3}$$

Letting $t_{\mathrm{opt}}(P^{AB})$ be the optimal value[2] of t for P^{AB}, if an operator $R^{ABB'}$ satisfies the two partial trace conditions and is positive semi-definite, then $R^{ABB'}$ will be a symmetric extension of P^{AB} and t_{opt} will be equal to the negative of its smallest eigenvalue. If a positive semi-definite $R^{ABB'}$ satisfying the two trace conditions does not exist, then a symmetric extension of P^{AB} does not exist and the smallest eigenvalue of $R^{ABB'}$ will be negative, so t_{opt} will be equal to the negative of that eigenvalue, that is, t_{opt} will be positive. The sign of t_{opt} therefore indicates the existence of a symmetric extension of P^{AB}: if $t_{\mathrm{opt}} \leq 0$, then a symmetric extension exists; if $t_{\mathrm{opt}} > 0$, then a symmetric extension does not exist. The formulation of symmetric extendability as an SDP was first done by Doherty et al. [DPS04; DPS02] in the context of determining the separability of quantum states.

3.3 Constructing Symmetric Extensions

Writing an arbitrary $P^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$ as

$$P^{AB} = \sum_{k,k'=0}^{d_A-1} \sum_{\ell,\ell'=0}^{d_B-1} (P^{AB})_{\substack{k,\ell \\ k',\ell'}} |k,\ell\rangle \langle k',\ell'|,$$

we have that a symmetric extension $P^{ABB'} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B \otimes \mathfrak{H}_{B'})$ of P^{AB}, if it exists, must satisfy by definition

$$\mathrm{Tr}_B(P^{ABB'}) = \mathrm{Tr}_{B'}(P^{ABB'}) = P^{AB}.$$

Writing $P^{ABB'}$ as

$$P^{ABB'} = \sum_{i,i'=0}^{d_A-1} \sum_{\substack{j,k \\ j',k'=0}}^{d_B-1} x_{\substack{i,j,k \\ i',j',k'}} |i,j,k\rangle \langle i',j',k'|,$$

[2] We will omit the dependence of t_{opt} on P^{AB} if the operator is understood from the context.

we have the following constraints

$$\begin{aligned}
\mathrm{Tr}_{B'}(P^{ABB'}) = P^{AB}: &\quad \sum_{k=0}^{d_B-1} x_{\substack{i,j,k\\ i',j',k}} = (P^{AB})_{\substack{i,j\\ i',j'}} \;\; \forall\, 0 \le i,i' \le d_A-1,\;\; 0 \le j,j' \le d_B-1,\\
\mathrm{Tr}_{B}(P^{ABB'}) = P^{AB}: &\quad \sum_{j=0}^{d_B-1} x_{\substack{i,j,k\\ i',j,k'}} = (P^{AB})_{\substack{i,k\\ i',k'}} \;\; \forall\, 0 \le i,i' \le d_B-1,\;\; 0 \le k,k' \le d_B-1,\\
P^{ABB'} \text{ Hermitian}: &\quad x_{\substack{i,j,k\\ i',j',k'}} = \overline{x_{\substack{i',j',k'\\ i,j,k}}} \;\; \forall\, 0 \le i,i' \le d_A-1,\;\; 0 \le j,j',k,k' \le d_B-1.
\end{aligned}$$

The rest of the matrix elements of $P^{ABB'}$ must be chosen so that it has non-negative eigenvalues, which will ensure that $P^{ABB'}$ is positive semi-definite. There might be more than one way to choose them, which means that if a symmetric extension exists it will generally not be unique.

Now, given the spectral decomposition of P^{AB},

$$P^{AB} = \sum_{k=0}^{r-1} \lambda_k \left|v_k\right\rangle \left\langle v_k\right|,$$

where $r = \mathrm{rank}(P^{AB})$, we can form the following purification of it in $\mathfrak{H}_{E_1} \otimes \mathfrak{H}_{E_2}$, with $d_{E_1} = d_A$ and $d_{E_2} = d_B$,

$$\left|\psi\right\rangle^{ABE_1E_2} = \mathrm{vec}\left(\sqrt{P^{AB}}\right) = \sum_{k=0}^{r-1} \sqrt{\lambda_k}\left|v_k\right\rangle^{AB} \otimes \left|v_k\right\rangle^{E_1E_2}.$$

Writing $P^{ABB'}$ from above using the eigenbasis $\{|v_k\rangle : 0 \le k \le r-1\}$ of P^{AB}, we get

$$P^{ABB'} = \sum_{k,k'=0}^{r-1} \left|v_k\right\rangle \left\langle v_{k'}\right|^{AB} \otimes X_{\substack{k\\ k'}}^{B'}, \tag{3.4}$$

where

$$X_{\substack{k\\ k'}}^{B'} := (\langle v_k| \otimes \mathbb{1}_{B'}) P^{ABB'} (|v_{k'}\rangle \otimes \mathbb{1}_{B'}),$$

is a function of the matrix elements $\left\{ x_{\substack{i,j,k\\ i',j',k'}} \right\}_{\substack{i,j,k\\ i',j',k'}}$ of $P^{ABB'}$. By Theorem 2.22, P^{AB} is symmetrically extendable if and only if there exists a channel $\mathcal{E} \in \mathrm{C}(\mathfrak{H}_{E_1} \otimes \mathfrak{H}_{E_2}, \mathfrak{H}_{B'})$ such that

$$(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{AB})} \otimes \mathcal{E})(\left|\psi\right\rangle \left\langle\psi\right|^{ABE_1E_2}) = P^{ABB'}, \tag{3.5}$$

or, by (3.4),

$$\mathcal{E}\left(\left|v_k\right\rangle \left\langle v_{k'}\right|^{E_1E_2}\right) = \frac{X_{\substack{k\\ k'}}^{B'}}{\sqrt{\lambda_k \lambda_{k'}}} \quad \forall\, 0 \le k,k' \le r-1. \tag{3.6}$$

Equivalently, if P^{AB} is symmetrically extendable with symmetric extension $P^{ABB'}$, then by taking the partial trace over B on both sides of (3.5) and using the definition of symmetric extension, we get

$$(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathcal{E})(P^{AE_1E_2}) = P^{AB}. \tag{3.7}$$

This is nothing but the statement of the anti-degradability of the map $\Phi_{P^{AB}}$ defined by P^{AB} by (2.12) since $J(\Phi_{P^{AB}}) = P^{AB} \Rightarrow J(\Phi^c_{P^{AB}}) = P^{AE_1E_2} \Rightarrow \mathcal{E} \circ \Phi^c_{P^{AB}} = \Phi_{P^{AB}}$. This means that the existence of a channel $\mathcal{E}$ satisfying (3.7) is necessary and sufficient for the symmetric extendability[3] of P^{AB}. Fung et al. [Fun+14] examine this

[3]Though we have used a particular purification to prove this result, note that it is independent of the purification.

condition and determine necessary and sufficient criteria for the existence of the channel $\mathcal{E}$; however, these criteria are non-constructive and rephrase the problem in terms of the existence of other mathematical objects that is generally difficult to check.

To summarize, we have that P^{AB} is symmetrically extendable with symmetric extension $P^{ABB'}$ if and only if (3.6) and (3.7), which are equivalent, hold. (3.6) provides a way of analytically constructing $\mathcal{E}$, which we will do for a particular class of states in Chapter 5, while (3.7) can be used to numerically search for $\mathcal{E}$ using the following SDP.

$$\begin{array}{ll} \text{min.} & t \\ \text{subject to} & X^{E_1E_2B'} + t\mathbb{1}^{E_1E_2B'} \geq 0, \\ & \mathrm{Tr}_{B'}[X^{E_1E_2B'}] = \mathbb{1}_{E_1E_2}, \\ & \mathrm{Tr}_{E_1,E_2}\left[\left((P^{AE_1E_2})^{\mathsf{T}}_{E_1E_2} \otimes \mathbb{1}_{B'}\right)(\mathbb{1}_A \otimes X^{E_1E_2B'})\right] = P^{AB}. \end{array} \tag{3.8}$$

Like the previous SDP, if X satisfies the constraints and the optimal value of t is negative, then X is positive semi-definite, which means that P^{AB} is symmetrically extendable and X is the Choi representation of the channel $\mathcal{E}$ constructing the symmetric extension $P^{ABB'}$ of P^{AB} given by (3.5). If t is positive, on the other hand, then a symmetric extension of P^{AB} does not exist.

3.3.1 A Special Construction

Now, suppose $\mathcal{E}$ from (3.5)/(3.7) has the form

$$\mathcal{E} = \mathcal{N} \circ \mathrm{Tr}_{E_2} \tag{3.9}$$

for some $\mathcal{N} \in \mathrm{T}(\mathfrak{H}_{E_1}, \mathfrak{H}_{B'})$. In the natural representation, this decomposition becomes, by (2.14),

$$K(\mathcal{E}) = K(\mathcal{N})K(\mathrm{Tr}_{E_2}).$$

The statement that P^{AB} is symmetrically extendable, equivalently the requirement that $\mathcal{E}$ satisfies $\mathcal{E} \circ \Phi^c_{P^{AB}} = \Phi_{P^{AB}}$, then becomes

$$\mathcal{N} \circ \mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}} = \Phi_{P^{AB}} \Leftrightarrow K(\mathcal{N})K(\mathrm{Tr}_{E_2})K(\Phi^c_{P^{AB}}) = K(\Phi_{P^{AB}}).$$

We can combine $K(\mathrm{Tr}_{E_2})K(\Phi^c_{P^{AB}})$ to $K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})$, and since $d_{E_1} = d_A$, the operator $K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})$ is square. If it is invertible, then $\mathcal{N}$ satisfies

$$K(\mathcal{N}) = K(\Phi_{P^{AB}})K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})^{-1}. \tag{3.10}$$

If $\mathcal{N}$ is completely-positive and trace-preserving, then a symmetric extension of P^{AB} exists and it is given by (3.5). If $\mathcal{N}$ is not completely-positive, then a symmetric extension of P^{AB} might still exist since symmetric extensions are not unique. In other words, it could be that a map $\mathcal{E}$ of a different form satisfies (3.5)/(3.7)[4]. The shuffling map S, which satisfies $S(J(\mathcal{N})) = K(\mathcal{N})$ by Proposition 2.10, can be used to find the Choi representation of $\mathcal{N}$, using which the complete-positivity of $\mathcal{N}$ can be determined. We prove in Appendix A that the Choi representation of $\mathcal{N}$ is equal to

$$J(\mathcal{N}) = S^{-1}\left[S\left(P^{AB}\right) S\left(S\left(\sqrt{P^{AB}}\right)^{\mathsf{T}} \overline{S\left(\sqrt{P^{AB}}\right)}\right)^{-1}\right]. \tag{3.11}$$

This formula allows us to calculate $J(\mathcal{N})$ for any $P^{AB} \in \mathrm{Pos}(\mathfrak{H}_A \otimes \mathfrak{H}_B)$. As stated before, if $J(\mathcal{N})$ is positive semi-definite and $\mathrm{Tr}_{B'}[J(\mathcal{N})] = \mathbb{1}_{E_1}$, then P^{AB} is symmetrically extendable with symmetric extension

$$P^{ABB'} = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{AB})} \otimes \mathcal{N})(P^{ABE_1}) = \mathrm{Tr}_{E_1}\left[\left((P^{ABE_1})^{\mathsf{T}_{E_1}} \otimes \mathbb{1}_{B'}\right)(\mathbb{1}_{AB} \otimes J(\mathcal{N}))\right]. \tag{3.12}$$

[4] See §3 of [Bra15] for more information about the non-uniqueness of degrading maps.

If not, then the symmetric extendability of P^{AB} can still be determined by running either one of the SDPs (3.3) or (3.8).

The inspiration for this particular choice (3.9) of the degrading map $\mathcal{E}$ comes from the fact that it constructs a symmetric extension throughout the symmetric extendability region for particular classes of states that will be considered in Chapters 5 and 6.

3.4 Two-Qubit Bell-Diagonal States

By applying the necessary and sufficient condition (3.2) to the two-qubit Bell-diagonal state $\rho_{\text{Bell}}^{AB}(\vec{p})$ of (2.21), we get that it is symmetrically extendable to a copy of B if and only if

$$\frac{1}{2} \geq p_I^2 + p_x^2 + p_y^2 + p_z^2 - 4\sqrt{p_I p_x p_y p_z}.$$

When this holds, there exists a symmetric extension of the form

$$\begin{aligned}\rho_{\text{Bell}}^{ABB'}(\vec{p},\vec{\beta}) \coloneqq \frac{1}{8}(&\mathbb{1}_{\mathbb{C}^2}\otimes\mathbb{1}_{\mathbb{C}^2}\otimes\mathbb{1}_{\mathbb{C}^2} + \beta_x\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_x\otimes\sigma_x + \alpha_x\sigma_x\otimes\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_x \\ &+ \alpha_x\sigma_x\otimes\sigma_x\otimes\mathbb{1}_{\mathbb{C}^2} + \beta_y\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_y\otimes\sigma_y + \alpha_y\sigma_y\otimes\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_y \\ &+ \alpha_y\sigma_y\otimes\sigma_y\otimes\mathbb{1}_{\mathbb{C}^2} + \beta_z\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_z\otimes\sigma_z + \alpha_z\sigma_z\otimes\mathbb{1}_{\mathbb{C}^2}\otimes\sigma_z \\ &+ \alpha_z\sigma_z\otimes\sigma_z\otimes\mathbb{1}_{\mathbb{C}^2}),\end{aligned} \tag{3.13}$$

for some choice of the open parameters $\vec{\beta} = (\beta_x, \beta_y, \beta_z)$ such that it is positive semi-definite, where $\alpha_x, \alpha_y, \alpha_z$ are given by (2.28). The proof of this can be found in [Myh10]. We will use this result in Chapter 5.

Chapter 4

Two-Way Protocols & Breaking Symmetric Extendability

The goal of this thesis is to determine whether there exist two-way post-processing protocols better than advantage distillation that allow Alice and Bob to distill a secret key using measurement data from either the six-state or the BB84 signal states with equal QBER Q in each basis. Specifically, we want to know whether such two-way protocols exist in the interval $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$ for the six-state signal states and $\frac{1}{5} \leq Q < \frac{1}{4}$ for the BB84 signal states. Recall that within these intervals Alice and Bob's initial correlations are symmetrically extendable, which means that any successful two-way protocol must first break the symmetric extendability of the correlations so that they can then proceed to the one-way error-correction and privacy amplification protocols.

In this chapter, we look at general two-way post-processing protocols that might break the symmetric extendability of Alice and Bob's correlations. As shown in [Myh+09], the problem can be simplified if all we care about is whether a secret key can be distilled and not about the rate of key distillation. We recapitulate those arguments and then show that the simplification leads to a manageable class of effective protocols involving announcements of a relatively simple type on blocks of data, which can be modelled on the quantum states as a local, independent post-selection by Alice and Bob. The remainder of the chapter is devoted to examining the post-selected states and reducing the search of protocols within the simplified class of effective protocols by determining announcements that are equivalent for the purpose of breaking symmetric extendability.

4.1 General Two-Way Protocols & Reduction to an Effective Protocol

As shown in Figure 4.1, the most general two-way protocol consists of a sequence of one-way communication rounds in alternating directions, which continuously alters the effective state shared between Alice and Bob, followed by a final round of one-way communication that we assume is from Alice to Bob and consists of error-correction and privacy amplification. By Theorem 2.24, the effective state just before error-correction and privacy amplification must not have a symmetric extension in order to successfully create a secret key. This means that the symmetric extendability of the initial state ρ_0^{AB} must be broken in one of the rounds prior to the final round, and the round that breaks it has to be a one-way communication round from Bob to Alice since symmetric extendability is preserved under one-way Alice-to-Bob communication, as we have seen in Chapter 3. Bob's action in the round that breaks the symmetric extendability of the initial state can be described by some

completely-positive map. Letting $\{K_i\}_i$ be the Kraus operators of the map corresponding to this round, we must have that

$$\sigma^{AB} := \sum_i (\mathbb{1}_A \otimes K_i)\tau^{AB}(\mathbb{1}_A \otimes K_i)^\dagger = \sum_i p_i \sigma_i^{AB}$$

is *not* symmetrically extendable, where τ^{AB} is the state prior to the round, $p_i = \mathrm{Tr}[(\mathbb{1}_A \otimes K_i)\tau^{AB}(\mathbb{1}_A \otimes K_i)^\dagger]$ and $\sigma_i^{AB} = \frac{1}{p_i}(\mathbb{1}_A \otimes K_i)\tau^{AB}(\mathbb{1}_A \otimes K_i)^\dagger$ for all i. For this state to not be symmetrically extendable, *at least one of the states σ_i^{AB} must not be symmetrically extendable*, that is, at least one of the Kraus operators alone must break the symmetric extendability of τ^{AB}. On the other hand, if all σ_i^{AB} are symmetrically extendable, then so will σ^{AB} by convexity of the set of symmetrically extendable states. This means that for the purpose of determining whether a secret key can be distilled, it is enough to look at filtering operations (that is, CP maps with one Kraus operator) performed by Bob.

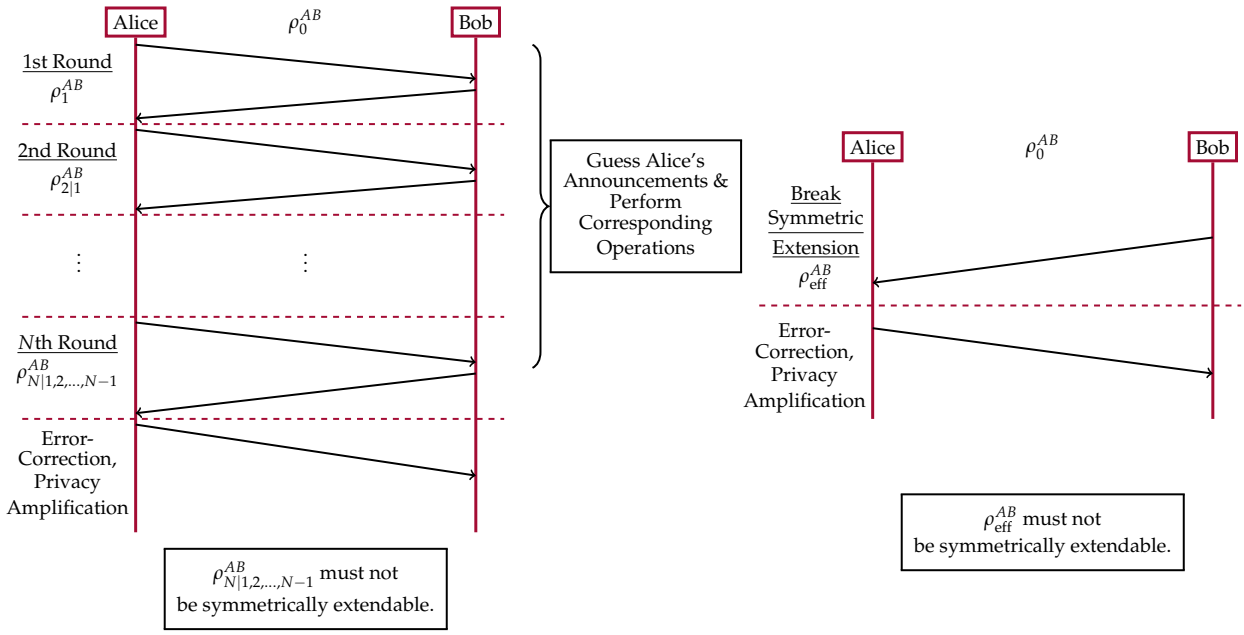


Figure 4.1: A general two-way post-processing protocol to break the symmetric extendability of the initial state ρ_0^{AB} followed by the error-correction and privacy amplification protocols to distill a secret key. If all we care about is whether a secret key can be distilled after such a protocol and not about the rate of key distillation, then the two-way protocol can be reduced to simply one round of Bob-to-Alice communication, which must break the symmetric extendability of the initial state, followed by error-correction and privacy amplification.

Next, we can reduce the finite number of one-way rounds to two. As shown in Figure 4.1, for each of the blocks being processed prior to the final round (that is, prior to the Nth round) of two-way communication, Bob can guess Alice's announcement and perform the corresponding operations on his blocks. In the Nth round, Bob will announce the results of his operations to Alice. Then, in the final round, Alice will announce to Bob her results for each of the blocks. Based on this announcement, Bob will know whether or not his guesses were correct. For the tiny fraction of blocks in which Bob guessed correctly, Alice and Bob can proceed to the remaining one-way error-correction and privacy amplification steps as long as the symmetric extendability of the initial state was broken during Bob's announcement. This means that if a successful two-way protocol with multiple rounds can break the symmetric extendability of the initial state, then the same protocol reduced to only two rounds as just described can also break the symmetric extendability of the initial state, albeit with

possibly lower success probability and lower key rate.

So far, we have shown (as was originally done in [Myh+09]) how a general two-way protocol can be reduced to one round of local operations by Bob on a block of his data. In this thesis, we are considering QKD protocols with the BB84 and six-state signal states, which means that after parameter estimation Alice and Bob merely hold classical bits resulting from their measurements. The conditional quantum states in Figure 4.1 are then defined by appropriately representing the operations on the classical bits quantum-mechanically such that if the initial measurement had been *delayed* until after the quantum operation then the resulting statistics would be the same as the statistics obtained from the classical operations on the classical bits[1].

Now, the only possible classical operations on blocks of data are functions of the form $f : \{0,1\}^n \to \{0,1\}^k$ for some function f (for some n and k) and/or *post-selection* (that is, keeping data of some desired types and discarding the rest). Most generally, the block size as well as the functions and post-selection performed, will vary from round to round; however, as argued above, for our purposes it is enough to simply consider *one round* of such operations *performed by Bob*. The post-selection is defined by the triple $(n, m, \mathcal{P})$, where $n, m \geq 1$ and the post-selection set $\mathcal{P} = \{P_k\}_{k=0}^{m-1} \subseteq \{0,1\}^n$ is a set of n-bit strings with n being the block size. Quantum-mechanically, this purely classical post-selection can be described by the Kraus operator[2]

$$A_{\mathcal{P}} := \sum_{k=0}^{m-1} |k\rangle \langle P_k| . \tag{4.1}$$

The result of any function f performed before or after post-selection can always be incorporated by appropriately modifying the post-selection. This means that we only have to consider post-selection operations.

The initial correlations between Alice and Bob on a block of their data of size n are described by the state $(\rho^{AB})^{\otimes n}$, where ρ^{AB} as before describes Alice and Bob's correlations after one round of signal state distribution and measurement. The state resulting from one round of post-selection on $\mathcal{P}$ performed by Bob is then

$$(\mathbb{1}_{A^n} \otimes A_{\mathcal{P}})(\rho^{A^nB^n})(\mathbb{1}_{A^n} \otimes A_{\mathcal{P}})^\dagger, \tag{4.2}$$

where

$$\rho^{A^nB^n} := W \left(\rho^{AB}\right)^{\otimes n} W^\dagger, \tag{4.3}$$

and $W \in \mathrm{U}(\mathfrak{H}_{A_1B_1} \otimes \mathfrak{H}_{A_2B_2} \cdots \otimes \mathfrak{H}_{A_nB_n}, \mathfrak{H}_{A_1A_2\cdots A_n} \otimes \mathfrak{H}_{B_1B_2\cdots B_n})$ rearranges the subsystems as follows:

$$W |a_1, b_1, a_2, b_2, \ldots, a_n, b_n\rangle^{A_1B_1A_2B_2\cdots A_nB_n} = |a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\rangle^{A_1A_2\cdots A_nB_1B_2\cdots B_n} \tag{4.4}$$

for all $0 \leq a_1, \ldots, a_n, b_1, \ldots, b_n \leq 1$. In what follows, we will also allow Alice to perform a post-selection defined by a Kraus operator of the type (4.1) since doing so will make the problem mathematically simpler, as we will see later.

Now, with the class of filters (4.1), we can define an *effective* protocol as follows: after Alice and Bob agree on a block size n and on sets $\mathcal{P} = \{P_k\}_{k=0}^{m_A-1}$ and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_B-1}$ of n-bit strings:

1. Alice checks if her block of data is contained in $\mathcal{P}$ and announces either "yes" or "no" to Bob.

[1] Delaying measurements until after a quantum computation and replacing any intermediate classical processing of measurement data by quantum operations is called the *principle of deferred measurement* [NC00].

[2] Note that the form of the Kraus operator assumes that the data results from measurement in the z-basis only; however, since we are only considering QKD protocols with the BB84 and six-state signal states in the case of equal QBER in each basis, the measurement statistics are the same in each basis, so nothing is gained by using, for example, a filter like $|0\rangle \langle + + +| + |1\rangle \langle + - +| + \cdots$, which corresponds to data from measurement in the x-basis.

2. Bob similarly checks if his block of data is in $\mathcal{Q}$, announcing to Alice either "yes" or "no".

If both Alice and Bob announce "yes", they each retain the set index of the string obtained; if not (that is, either Alice, Bob, or both announce "no"), then the entire block of data is discarded. In this effective protocol, Alice and Bob merely perform an *independent post-selection* on their data according to the sets $\mathcal{P}, \mathcal{Q}$, which we will call *announcement sets*. The advantage distillation protocol is a special case of this effective protocol in which $\mathcal{P} = \mathcal{Q} = \{\underline{0}^n, \underline{1}^n\}$. We will examine these sets in the context of breaking symmetric extendability in Chapter 5.

With the BB84 and six-state signal states, the data held by Alice and Bob after their measurements can be described by multiple copies of the Bell-diagonal states (2.42) and (2.44):

$$\begin{aligned}\rho_{Q,x}^{AB} &= (1-2Q+x)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (Q-x)\left|\Phi^-\right\rangle\left\langle\Phi^-\right| \\ &\quad + (Q-x)\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + x\left|\Psi^-\right\rangle\left\langle\Psi^-\right|, \quad 0 \leq x \leq Q \quad \text{(BB84)}, \\ \rho_{Q}^{AB} &= \left(1-\frac{3}{2}Q\right)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{Q}{2}\left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \frac{Q}{2}\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \frac{Q}{2}\left|\Psi^-\right\rangle\left\langle\Psi^-\right| \quad \text{(Six-State)}.\end{aligned}$$

If the effective protocol described above is successful, then using the six-state signal states the updated (unnormalized) state shared by Alice and Bob, which we denote $\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$, is

$$\boxed{\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}} \coloneqq (A_{\mathcal{P}} \otimes A_{\mathcal{Q}})(\rho_{Q}^{A^nB^n})(A_{\mathcal{P}} \otimes A_{\mathcal{Q}})^\dagger.} \tag{4.5}$$

The state $\rho_{Q,(\mathcal{B}_n,\mathcal{Q})}^{A^n\tilde{B}}$ corresponds to the case of Alice post-selecting on $\mathcal{B}_n \coloneqq \{0,1\}^n$, that is, on all bit strings, which is effectively not a post-selection at all since $A_{\mathcal{B}_n} = \mathbb{1}_{A^n}$. A natural choice of an announcement set for Alice that we will consider is $\mathcal{P} = \mathcal{Q}$, that is, Alice and Bob post-select on the same set. We will write $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ instead of $\rho_{Q,(\mathcal{P},\mathcal{P})}^{\tilde{A}\tilde{B}}$ when this is the case.

By taking the QBER Q to be within the gap $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$, we can now determine the existence of a two-way post-processing protocol that can be used to distill a secret key by determining whether there exist sets $\mathcal{P}, \mathcal{Q}$ such that the state $\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$ does *not* have a symmetric extension. If $\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$ *does* have a symmetric extension for all $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$ no matter the choice of sets $\mathcal{P}, \mathcal{Q}$, then there does not exist a two-way post-processing protocol to distill a secret key beyond the current bounds.

For the BB84 signal states, forming the corresponding filtered states as per (4.5), we obtain for each Q and every pair $(\mathcal{P}, \mathcal{Q})$ of announcement sets the states $\{\rho_{(Q,x),(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}\}_{x\in[0,Q]}$. Determining the symmetric extendability of these states in the gap $\frac{1}{5} \leq Q < \frac{1}{4}$ means determining the symmetric extendability of $\rho_{(Q,x),(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$ for each value of the open parameter $x \in [0, Q]$. For simplicity, we will throughout the rest of the thesis deal with only the six-state signal states and the corresponding filtered states $\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$.

Being subsets of the n-bit strings $\{0,1\}^n$, the sets $\mathcal{P}$ and $\mathcal{Q}$ used to form the filtered states $\rho_{Q,(\mathcal{P},\mathcal{Q})}^{\tilde{A}\tilde{B}}$ corresponding to the effective protocol described above can essentially be thought of as binary (classical) *error-correcting codes*—which by definition are subsets of $\{0,1\}^n$—with the strings P_k, Q_ℓ in the sets being the *codewords*[3]. It is common to write the codewords as the rows of a matrix, and we will do so throughout this thesis. We now go through some of the basic error-correction notation and terminology that will be used in later chapters.

[3] A good reference on error-correcting codes is [MS77].

The *bitwise XOR operation* $\oplus$ between two strings in $\{0,1\}^n$ is defined as the string in which each position of the string is obtained by performing the XOR operation on the corresponding positions of the two strings, where the XOR operation is defined as

$$0 \text{ XOR } 0 = 0, \quad 0 \text{ XOR } 1 = 1, \quad 1 \text{ XOR } 0 = 1, \quad 1 \text{ XOR } 1 = 0$$

The *bitwise AND operation* $\odot$ between two strings in $\{0,1\}^n$ is defined as the string in which each position of the string is obtained by performing the AND operation on the corresponding positions of the two strings, where the AND operation is defined as

$$0 \text{ AND } 0 = 0, \quad 0 \text{ AND } 1 = 0, \quad 1 \text{ AND } 0 = 0, \quad 1 \text{ AND } 1 = 1$$

The set $\{0,1\}^n$ together with the addition $\oplus$ and the scalars $\{0,1\}$ forms an n-dimensional vector space[4]. More generally, the set $\{0,1\}^n$ together with the addition $\oplus$ and the multiplication $\odot$ forms a ring.

For any $\alpha \in \{0,1\}^n$, $|\alpha|$ is called the *Hamming weight* of α and is defined as the number of ones in the string α. For any $\alpha, \beta \in \{0,1\}^n$, it holds that [MS77]

$$|\alpha \oplus \beta| = |\alpha| + |\beta| - 2|\alpha \odot \beta|. \tag{4.6}$$

For any $\alpha = \alpha_1 \cdots \alpha_n$ and $\beta = \beta_1 \cdots \beta_n$ in $\{0,1\}^n$, the *dot product* $\alpha \cdot \beta$ is defined as $\alpha \cdot \beta = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n \pmod 2$. For any $\alpha \in \{0,1\}^n$, $\overline{\alpha}$ is called the *complement* of α and is defined as the n-bit string with the 1s in α replaced by 0s and the 0s replaced by 1s. It holds that $\alpha \oplus \overline{\alpha} = 11\cdots11$ and $\alpha \odot \overline{\alpha} = 00\cdots00$ for all $\alpha \in \{0,1\}^n$.

Error-correcting codes $\mathcal{P} = \{P_k\}_{k=0}^{m-1}$ that are closed under addition are called *linear codes*. The closure property of linear codes ensures that the number m of codewords is equal to 2^k for some $k \leq n$. Since linear codes are themselves vector spaces of dimension k over the same scalar set $\{0,1\}$, there exists a *basis* $\{B_1, B_2, \ldots, B_k\}$ of the code such that any codeword $P_i \in \mathcal{P}$ can be written as $P_i = \alpha_{i,1}B_1 \oplus \alpha_{i,2}B_2 \oplus \cdots \oplus \alpha_{i,k}B_k$ for some string $\alpha_i = \alpha_{i,1}\alpha_{i,2}\cdots\alpha_{i,k} \in \{0,1\}^k$ for all $0 \leq i \leq 2^k - 1$. It follows that for each linear code $\mathcal{P}$ there exists a $n \times k$ binary matrix $G_{\mathcal{P}}$, called the *generator matrix* of $\mathcal{P}$, whose k columns are the strings $B_1, \ldots, B_k$, such that

$$P_i = G_{\mathcal{P}}\alpha_i \quad \forall\, 0 \leq i \leq 2^k - 1. \tag{4.7}$$

In this equation, the codewords P_i and the strings α_i are considered column vectors of size n and k, respectively. Linear codes are specified using the notation $[n, k, d]$ whenever the code has block size n, 2^k codewords, and minimum distance d. In Appendix E we examine in detail the filtered states resulting from post-selection on linear codes.

Non-linear codes are those that are not closed under addition. Their codewords cannot be written in the form (4.7). One might imagine that non-linear codes might be more powerful than linear codes and therefore capable of breaking the symmetric extendability of ρ_Q^{AB} beyond the current bounds. Both the numerical and analytical evidence we provide in this thesis indicates that this is not the case. In fact, all that appears to matter is the size of the code and not whether it is linear or non-linear.

4.2 Structure of the Filtered States

Starting with

$$A_{\mathcal{P}} = \sum_{k=0}^{m_A-1} |k\rangle \langle P_k|, \quad A_{\mathcal{Q}} = \sum_{\ell=0}^{m_B-1} |\ell\rangle \langle Q_\ell|$$

[4]The scalar multiplication is defined in the expected way: for any $\alpha \in \{0,1\}^n$, $0\alpha = \underline{0}^n$ and $1\alpha = \alpha$.

for some $\mathcal{P} = \{P_k\}_{k=0}^{m_A-1}$ and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_B-1}$, we can write the filtered state $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ defined by (4.5) as

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})} = \sum_{k=0}^{m_A-1}\sum_{\ell=0}^{m_B-1} \left(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right)_{\substack{k,\ell\\k',\ell'}} |k,\ell\rangle\langle k',\ell'|^{\tilde{A}\tilde{B}}, \tag{4.8}$$

where

$$\left(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right)_{\substack{k,\ell\\k',\ell'}} := \langle P_k, Q_\ell|\, \rho_Q^{A^nB^n}\, |P_{k'}, Q_{\ell'}\rangle = \langle P_{k,1}, Q_{\ell,1}|\, \rho_Q^{AB}\, |P_{k',1}, Q_{\ell',1}\rangle \cdots \langle P_{k,n}, Q_{\ell,n}|\, \rho_Q^{AB}\, |P_{k',n}, Q_{\ell',n}\rangle\,. \tag{4.9}$$

By writing ρ_Q^{AB} in the standard basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$ as

$$\rho_Q^{AB} = \begin{bmatrix} \frac{1-Q}{2} & 0 & 0 & \frac{1-2Q}{2} \\ 0 & \frac{Q}{2} & 0 & 0 \\ 0 & 0 & \frac{Q}{2} & 0 \\ \frac{1-2Q}{2} & 0 & 0 & \frac{1-Q}{2} \end{bmatrix}, \tag{4.10}$$

it holds that

$$\langle a,b|\, \rho_Q^{AB}\, |a',b'\rangle = \left(\frac{Q}{2}\right)^{a\oplus b} \left(\frac{1-2Q}{2}\right)^{(\overline{a\oplus b})(a\oplus a')} \left(\frac{1-Q}{2}\right)^{\overline{a\oplus b}-(\overline{a\oplus b})(a\oplus a')} \delta_{a\oplus b,a'\oplus b'}\delta_{(a\oplus b)(a\oplus a'),0}$$

for all $0 \le a,b,a',b' \le 1$. Therefore,

$$\begin{aligned}\left(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right)_{\substack{k,\ell\\k',\ell'}} = \left(\frac{Q}{2}\right)^{|P_k\oplus Q_\ell|} &\left(\frac{1-2Q}{2}\right)^{|\overline{(P_k\oplus Q_\ell)}\odot(P_k\oplus P_{k'})|} \\ &\times \left(\frac{1-Q}{2}\right)^{|\overline{P_k\oplus Q_\ell}|-|\overline{(P_k\oplus Q_\ell)}\odot(P_k\oplus P_{k'})|} \delta_{P_k\oplus Q_\ell,P_{k'}\oplus Q_{\ell'}}\delta_{(P_k\oplus Q_\ell)\odot(P_k\oplus P_{k'}),\underline{0}^n}.\end{aligned} \tag{4.11}$$

However, using the fact that

$$\begin{aligned}|\overline{P_k\oplus Q_\ell}| &= n - |P_k\oplus Q_\ell|,\\ |\overline{(P_k\oplus Q_\ell)}\odot(P_k\oplus P_{k'})| &= |P_k\oplus P_{k'}| - |(P_k\oplus Q_\ell)\odot(P_k\oplus P_{k'})|,\end{aligned}$$

we get

$$\begin{aligned}\left(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right)_{\substack{k,\ell\\k',\ell'}} = \left(\frac{1-2Q}{2}\right)^{|P_k\oplus P_{k'}|} &\left(\frac{Q}{2}\right)^{|P_k\oplus Q_\ell|} \\ &\times \left(\frac{1-Q}{2}\right)^{n-|P_k\oplus P_{k'}|-|P_k\oplus Q_\ell|} \delta_{P_k\oplus Q_\ell,P_{k'}\oplus Q_{\ell'}}\delta_{(P_k\oplus Q_\ell)\odot(P_k\oplus P_{k'}),\underline{0}^n}.\end{aligned} \tag{4.12}$$

The Kronecker delta $\delta_{P_k\oplus Q_\ell,P_{k'}\oplus Q_{\ell'}}$ indicates that the matrix elements of the filtered state are non-zero if and only if $P_k \oplus Q_\ell = P_{k'} \oplus Q_{\ell'}$, which means that the filtered state has a block structure with blocks characterized by the sums $P_k \oplus Q_\ell$. By defining the set

$$\mathcal{C} = \{P_k \oplus Q_\ell : 0 \le k \le m_A - 1,\ 0 \le \ell \le m_B - 1\}, \tag{4.13}$$

it holds that the (ordered) standard basis $\{|k,\ell\rangle^{\tilde{A}\tilde{B}} : 0 \le k \le m_A - 1,\ 0 \le \ell \le m_B - 1\}$ can be changed to the new (ordered) basis

$$\bigcup_{c\in\mathcal{C}} \{|k,\ell\rangle^{\tilde{A}\tilde{B}} : P_k \oplus Q_\ell = c\}$$

by a unitary V that simply reorders the standard basis elements and leaves the filtered state in a *block-diagonal* form:

$$V\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}V^\dagger = \bigoplus_{c\in\mathcal{C}} M^{(c)}_{Q,(\mathcal{P},\mathcal{Q})}, \tag{4.14}$$

where $M^{(c)}_{Q,(\mathcal{P},\mathcal{Q})}$ are the blocks. The state $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ can then be written as

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})} = \sum_{c\in\mathcal{C}} \sum_{\substack{(k,\ell,k',\ell')\\ \in\mathcal{I}_c\times\mathcal{I}_c}} \left(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right)_{\substack{k,\ell\\ k',\ell'}} |k,\ell\rangle\langle k',\ell'|, \tag{4.15}$$

where

$$\mathcal{I}_c := \{(k,\ell) : P_k \oplus Q_\ell = c\}. \tag{4.16}$$

4.2.1 No Post-selection by Alice

The state $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ resulting from no post-selection by Alice is

$$\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})} = (\mathbb{1}_{A^n}\otimes A_{\mathcal{Q}})\left(\rho^{A^nB^n}_Q\right)(\mathbb{1}_{A^n}\otimes A_{\mathcal{Q}})^\dagger.$$

If we order the set $\mathcal{B}_n$ such that the elements of $\mathcal{Q}$ come first, then as a matrix in the standard basis, $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ has the following block-matrix form:

$$\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})} = \begin{bmatrix} \rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{Q}} & X \\ X^\dagger & \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{Q}^c,\mathcal{Q})} \end{bmatrix},$$

where $X = (A_{\mathcal{Q}}\otimes A_{\mathcal{Q}})(\rho^{A^nB^n}_Q)(A_{\mathcal{Q}^c}\otimes A_{\mathcal{Q}})^\dagger$ and $\mathcal{Q}^c = \mathcal{B}_n \setminus \mathcal{Q}$.

4.3 Symmetric Extendability of the Filtered States

As stated earlier, the key to the existence of two-way post-processing protocols allowing Alice and Bob to distill a secret key in the gap is determining the symmetric extendability of the states $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ for all Q in the gap resulting from Alice post-selecting on set $\mathcal{P}$ and Bob post-selecting on set $\mathcal{Q}$. Equivalently, we can determine the anti-degradability of the CP maps $\Phi_{Q,(\mathcal{P},\mathcal{Q})} \in \mathrm{CP}(\mathfrak{H}_{\tilde{A}},\mathfrak{H}_{\tilde{B}})$ defined by $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ according to (2.12):

$$\Phi_{Q,(\mathcal{P},\mathcal{Q})}(X) = \mathrm{Tr}_{\tilde{A}}\left[(X^\intercal\otimes\mathbb{1}_{\tilde{B}})\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right] \quad \forall\, X\in \mathrm{L}(\mathfrak{H}_{\tilde{A}}). \tag{4.17}$$

Since general existence criteria for the symmetric extendability of states on spaces of arbitrary dimension are presently not known, as outlined in Chapter 3 we will be determining the symmetric extendability of the states $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ either using an SDP or by attempting an explicit construction (either numerically or analytically) of a symmetric extension of the state.

4.3.1 Estimating Threshold Error Rates

For given sets $\mathcal{P}$ and $\mathcal{Q}$, we obtain the one-parameter family $\left\{\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\right\}_{Q\in\left[0,\frac{1}{2}\right]}$ of states for which we can define the function $T_{\mathcal{P},\mathcal{Q}} : \left[0,\frac{1}{2}\right] \to \mathbb{R}$ by

$$T_{\mathcal{P},\mathcal{Q}}(Q) = t_{\text{opt}}(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}), \tag{4.18}$$

where $t_{\text{opt}}(\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})})$ is the solution to the SDP (3.3). Recall that the sign of t_{opt} indicates the symmetric extendability of the state: if t_{opt} is positive, then the state is not symmetrically extendable and if t_{opt} is non-positive, then the state is symmetrically extendable. This means that the zero(s) of $T_{\mathcal{P},\mathcal{Q}}$ will give us the threshold error(s) at which the symmetric extendability of the family of states changes. Since there is only one threshold of $\frac{1}{6}$ for the original isotropic states $\left\{\rho^{AB}_{Q}\right\}_{Q\in\left[0,\frac{1}{2}\right]}$, with the states being symmetrically extendable above it, we expect that for any sets $\mathcal{P},\mathcal{Q}$ there will be only one threshold, call it $Q^*_{\mathcal{P},\mathcal{Q}}$. In other words, we expect the parameter space of $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ to look something like Figure 4.2. We would like to find sets $\mathcal{P},\mathcal{Q}$ such that $Q^*_{\mathcal{P},\mathcal{Q}}$ is inside, or even right at the upper end of the gap at $\frac{1}{3}$, since this would indicate the existence of a two-way post-processing protocol distilling a secret key within the gap.

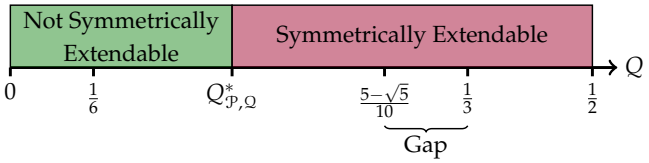


Figure 4.2: The expected parameter space of the state $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ for arbitrary $\mathcal{P},\mathcal{Q}$.

As stated earlier, it should be enough to break the symmetric extendability of ρ^{AB}_{Q} by post-selecting only on Bob's data. The following fact states that if post-selection by Bob only cannot break symmetric extendability, then post-selection by Alice as well will have no effect on breaking symmetric extendability.

Proposition 4.1

Suppose that for some announcement set $\mathcal{Q}$ the state $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ is symmetrically extendable with symmetric extension $\rho^{A^n\tilde{B}\tilde{B}'}_{Q,(\mathcal{B}_n,\mathcal{Q})}$. Then, for any announcement set $\mathcal{P}$, the state $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ is symmetrically extendable.

PROOF: We first observe that

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})} = (A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}})\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}(A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}})^\dagger.$$

Now, consider the state

$$\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,(\mathcal{P},\mathcal{Q})} := (A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}}\otimes\mathbb{1}_{\tilde{B}'})\rho^{A^n\tilde{B}\tilde{B}'}_{Q,(\mathcal{B}_n,\mathcal{Q})}(A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}}\otimes\mathbb{1}_{\tilde{B}'})^\dagger.$$

Then,

$$\text{Tr}_{\tilde{B}'}\left[\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,(\mathcal{P},\mathcal{Q})}\right] = (A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}})\text{Tr}_{\tilde{B}'}\left[\rho^{A^n\tilde{B}\tilde{B}'}_{Q,(\mathcal{B}_n,\mathcal{Q})}\right](A_{\mathcal{P}}\otimes\mathbb{1}_{\tilde{B}})^\dagger = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$$

and

$$\mathrm{Tr}_{\tilde{B}}\left[\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,(\mathcal{P},\mathcal{Q})}\right] = (A_{\mathcal{P}}\otimes \mathbb{1}_{\tilde{B}})\mathrm{Tr}_{\tilde{B}}\left[\rho^{A^n\tilde{B}\tilde{B}'}_{Q,(\mathcal{B}_n,\mathcal{Q})}\right](A_{\mathcal{P}}\otimes \mathbb{1}_{\tilde{B}})^\dagger = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})},$$

where we have used the fact that $\rho^{A^n\tilde{B}\tilde{B}'}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ is a symmetric extension of $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$. Therefore, by definition, $\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,(\mathcal{P},\mathcal{Q})}$ is a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$. Since $\mathcal{P}$ was arbitrary, the proof is complete. ■

The converse of this proposition is generally not true, meaning that if $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ is not symmetrically extendable, then a post-selection on $\mathcal{P}$ by Alice might make $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$ symmetrically extendable. This means that, in general, $Q^*_{\mathcal{P},\mathcal{Q}} \leq Q^*_{\mathcal{B}_n,\mathcal{Q}}$, which means that having Alice post-select has the undesired effect of potentially moving the threshold away from the gap. On the other hand, for the purpose of efficient numerical analysis using the SDP (3.3), letting Alice post-select is advantageous since this reduces the dimension of her system from 2^n to something smaller. Fortunately, supported by the data we will see in Chapter 8, and the analytic proof in §5.3 for a particular class of linear codes, we conjecture the following.

Conjecture 1

For all announcement sets $\mathcal{P}$,

$$Q^*_{\mathcal{P}} \equiv Q^*_{\mathcal{P},\mathcal{P}} = Q^*_{\mathcal{B}_n,\mathcal{P}}.$$

In other words, when Alice and Bob post-select on the *same* set, the converse of Proposition 4.1 appears to hold, meaning that we can let Alice and Bob post-select on the same set without compromising our ability to find thresholds within the gap.

4.3.2 Constructing Symmetric Extensions

The other way to determine the symmetric extendability of states that was described in Chapter 3 is explicitly constructing a channel on a purification of the state. In particular, we saw that for any state ρ^{AB} the existence of a channel $\mathcal{E}$ satisfying $(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)}\otimes\mathcal{E})(\rho^{AE_1E_2}) = \rho^{AB}$ is necessary and sufficient for the symmetric extendability of ρ^{AB}, where $\rho^{AE_1E_2} = \mathrm{Tr}_B[|\psi\rangle\langle\psi|^{ABE_1E_2}]$ and $|\psi\rangle^{ABE_1E_2} = \mathrm{vec}(\sqrt{\rho^{AB}})$ is a purification of ρ^{AB} in $\mathfrak{H}_{E_1E_2}$.

For the one-parameter family $\left\{\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right\}_{Q\in\left[0,\frac{1}{2}\right]}$ resulting from Alice and Bob post-selecting on the same set $\mathcal{P}$, we have the following conjecture about the form of a channel $\mathcal{E}_{Q,\mathcal{P}} \in \mathrm{C}(\mathfrak{H}_{E_1}\otimes\mathfrak{H}_{E_2}, \mathfrak{H}_{\tilde{B}'})$ such that

$$\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}} = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{\tilde{A}})}\otimes\mathcal{E}_{Q,\mathcal{P}})(\rho^{\tilde{A}E_1E_2})$$

for all $Q \geq Q^*_{\mathcal{P}}$:

Conjecture 2

For all announcement sets $\mathcal{P}$, there exists a channel $\mathcal{N}_{(Q,Q^*_{\mathcal{P}}),\mathcal{P}} \in \mathrm{C}(\mathfrak{H}_{\tilde{B}'}, \mathfrak{H}_{\tilde{B}'})$ for all $Q \geq Q^*_{\mathcal{P}}$ such that

$$\mathcal{E}_{Q,\mathcal{P}} = \mathcal{N}_{(Q,Q^*_{\mathcal{P}}),\mathcal{P}} \circ \mathcal{E}_{Q^*_{\mathcal{P}},\mathcal{P}}. \tag{4.19}$$

In other words, the channel constructing a symmetric extension can be split into two steps: the first that

on its own constructs a symmetric extension at the threshold $Q^*_{\mathcal{P}}$, and the second that acts as a post-processing step that completes the construction of a symmetric extension beyond the threshold. It necessarily holds due to the form of (4.19) that

$$\mathcal{N}_{(Q^*_{\mathcal{P}},Q^*_{\mathcal{P}}),\mathcal{P}} = \mathbb{1}_{\mathrm{L}(\mathfrak{H}_{\tilde{B}'})}.$$

The channel $\mathcal{E}_{Q^*_{\mathcal{P}},\mathcal{P}}$ constructing a symmetric extension at the threshold $Q^*_{\mathcal{P}}$ can be found numerically by first numerically estimating $Q^*_{\mathcal{P}}$ and then using the SDP (3.8).

Note that the special case $\mathcal{E} = \mathcal{N} \circ \mathrm{Tr}_{E_2}$ covered in §3.3 is also composed of two steps. As we will see in Chapters 5 and 6, it holds that $\mathcal{E}_{Q^*_{\mathcal{P}},\mathcal{P}} = \mathrm{Tr}_{E_2}$ whenever $\mathcal{P}$ is a repetition code or a simplex code. This special case will also provide a useful and efficient way of numerically checking the symmetric extendability within the gap of the filtered states for *arbitrary* $\mathcal{P}$, the results of which will be presented in Chapter 7.

4.4 Equivalent Announcement Sets

In this section, we show that announcement sets differing by certain basic operations, namely addition of each element of the set by some bit string and a permutation of each element in the set, leave the corresponding state unchanged, meaning that states generated using announcement sets differing by these operations will have exactly the same symmetric extendability bounds. Throughout this section, $\mathcal{S}_n$ refers to the permutation group on n elements.

Proposition 4.2 Invariance Under Addition and Permutation

For any announcement sets $\mathcal{P} = \{P_k\}_{k=0}^{m_A-1}$ and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_B-1}$ of n-bit strings, it holds that

1. For any $\alpha \in \{0,1\}^n$, the sets $\mathcal{P} \oplus \alpha := \{P_k \oplus \alpha\}_{k=0}^{m_A-1}$ and $\mathcal{Q} \oplus \alpha := \{Q_\ell \oplus \alpha\}_{\ell=0}^{m_B-1}$ satisfy

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P}\oplus\alpha,\mathcal{Q}\oplus\alpha)} = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})};$$

2. For any $\pi \in \mathcal{S}_n$, the sets $\pi(\mathcal{P}) := \{\pi(P_k)\}_{k=0}^{m_A-1}$ and $\pi(\mathcal{Q}) := \{\pi(Q_\ell)\}_{\ell=0}^{m_B-1}$ satisfy

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\pi(\mathcal{P}),\pi(\mathcal{Q}))} = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})},$$

where for $P_k = P_{k,1}P_{k,2}\cdots P_{k,n}$ the string $\pi(P_k)$ is defined as $\pi(P_k) = P_{k,\pi(1)}P_{k,\pi(2)}\cdots P_{k,\pi(n)}$.

PROOF:

1. For any $\alpha \in \{0,1\}^n$, we have by definition

$$A_{\mathcal{P}\oplus\alpha} = \sum_{k=0}^{m_A-1} |k\rangle \langle P_k \oplus \alpha| \quad \text{and} \quad A_{\mathcal{Q}\oplus\alpha} = \sum_{\ell=0}^{m_B-1} |\ell\rangle \langle Q_\ell \oplus \alpha| .$$

Now[5],

$$|P_k \oplus \alpha\rangle = (\sigma_x)^\alpha |P_k\rangle ,$$

and similarly for $|Q_\ell \oplus \alpha\rangle$. Therefore,

$$A_{\mathcal{P}\oplus\alpha} = A_{\mathcal{P}}(\sigma_x^A)^\alpha \quad \text{and} \quad A_{\mathcal{Q}\oplus\alpha} = A_{\mathcal{Q}}(\sigma_x^B)^\alpha.$$

Therefore,

$$\begin{aligned}\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P}\oplus\alpha,\mathcal{Q}\oplus\alpha)} &= (A_{\mathcal{P}\oplus\alpha}\otimes A_{\mathcal{Q}\oplus\alpha})(\rho_Q^{A^nB^n})(A_{\mathcal{P}\oplus\alpha}\otimes A_{\mathcal{Q}\oplus\alpha})^\dagger \\ &= (A_{\mathcal{P}}\otimes A_{\mathcal{Q}})((\sigma_x^A)^\alpha\otimes(\sigma_x^B)^\alpha)(\rho_Q^{A^nB^n})((\sigma_x^A)^\alpha\otimes(\sigma_x^B)^\alpha)^\dagger(A_{\mathcal{P}}\otimes A_{\mathcal{Q}})^\dagger.\end{aligned}$$

Since each copy ρ_Q^{AB} of $\rho_Q^{A^nB^n}$ is Bell-diagonal, which means that $(\sigma_x\otimes\sigma_x)\rho_Q^{AB}(\sigma_x\otimes\sigma_x)^\dagger = \rho_Q^{AB}$ as seen in (2.29), it holds that

$$((\sigma_x^A)^\alpha\otimes(\sigma_x^B)^\alpha)(\rho_Q^{A^nB^n})((\sigma_x^A)^\alpha\otimes(\sigma_x^B)^\alpha)^\dagger = \rho_Q^{A^nB^n}.$$

Therefore,

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P}\oplus\alpha,\mathcal{Q}\oplus\alpha)} = (A_{\mathcal{P}}\otimes A_{\mathcal{Q}})(\rho_Q^{A^nB^n})(A_{\mathcal{P}}\otimes A_{\mathcal{Q}})^\dagger = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})},$$

as required.

2. Defining the operator Φ_π as

$$\Phi_\pi = \sum_{\alpha\in\{0,1\}^n} |\pi(\alpha)\rangle\langle\alpha|,$$

it holds that

$$A_{\pi(\mathcal{P})} = \sum_{k=0}^{m_A-1} |k\rangle\langle\pi(P_k)| = \sum_{k=0}^{m_A-1} |k\rangle\langle P_k|\Phi_\pi^\dagger = A_{\mathcal{P}}\Phi_\pi^\dagger,$$

and similarly $A_{\pi(\mathcal{Q})} = A_{\mathcal{Q}}\Phi_\pi^\dagger$. But $\Phi_\pi^\dagger = \Phi_\pi^{-1}$ by the unitarity of Φ_π, and $\Phi_\pi^{-1} = \Phi_{\pi^{-1}}$, which can be easily verified. Therefore,

$$\begin{aligned}\rho^{\tilde{A}\tilde{B}}_{Q,(\pi(\mathcal{P}),\pi(\mathcal{Q}))} &= (A_{\pi(\mathcal{P})}\otimes A_{\pi(\mathcal{Q})})(\rho_Q^{A^nB^n})(A_{\pi(\mathcal{P})}\otimes A_{\pi(\mathcal{Q})})^\dagger \\ &= (A_{\mathcal{P}}\otimes A_{\mathcal{Q}})(\Phi_{\pi^{-1}}^{A^n}\otimes\Phi_{\pi^{-1}}^{B^n})(\rho_Q^{A^nB^n})(\Phi_{\pi^{-1}}^{A^n}\otimes\Phi_{\pi^{-1}}^{B^n})^\dagger(A_{\mathcal{P}}\otimes A_{\mathcal{Q}})^\dagger.\end{aligned}$$

Since $\rho_Q^{A^nB^n}$ is invariant under all permutations of the A and B sub-registers[6], meaning that for all $\sigma\in S_n$

$$(\Phi_\sigma^{A^n}\otimes\Phi_\sigma^{B^n})(\rho_Q^{A^nB^n})(\Phi_\sigma^{A^n}\otimes\Phi_\sigma^{B^n})^\dagger = \rho_Q^{A^nB^n} \quad \forall\sigma\in S_n,$$

we have that

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\pi(\mathcal{P}),\pi(\mathcal{Q}))} = (A_{\mathcal{P}}\otimes A_{\mathcal{Q}})(\rho_Q^{A^nB^n})(A_{\mathcal{P}}\otimes A_{\mathcal{Q}})^\dagger = \rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})},$$

as required. ■

We now prove the intuitively-expected result that the *ordering* of the strings in the sets $\mathcal{P}$ and $\mathcal{Q}$ is irrelevant to the question of the symmetric extendability of the filtered states.

[5]For any $\alpha = \alpha_1\alpha_2\cdots\alpha_n\in\{0,1\}^n$, $(\sigma_x)^\alpha$ stands for $\sigma_x^{\alpha_1}\otimes\sigma_x^{\alpha_2}\otimes\cdots\otimes\sigma_x^{\alpha_n}$, where $\sigma_x^0 = \mathbb{1}_{\mathbb{C}^2}$ and $\sigma_x^1 = \sigma_x$.

[6]This is simply due to the fact that $\rho_Q^{A^nB^n}$, as defined in (4.3), is formed from the tensor product $(\rho_Q^{AB})^{\otimes n}$.

Proposition 4.3 Unitary Invariance Under Permutation of Codewords

For any two announcement sets $\mathcal{P} = \{P_k\}_{k=0}^{m_A-1}$ and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_B-1}$, consider for any $\pi_A \in \mathcal{S}_{m_A}$ and any $\pi_B \in \mathcal{S}_{m_B}$ the announcement sets

$$\mathcal{P}^{(\pi_A)} := \{P_k^{(\pi_A)}\}_{k=0}^{m_A-1}, \quad \mathcal{Q}^{(\pi_B)} := \{Q_\ell^{(\pi_B)}\}_{\ell=0}^{m_B-1},$$

where

$$P_k^{(\pi_A)} = P_{\pi_A^{-1}(k)} \quad \forall\, 0 \leq k \leq m_A - 1, \qquad Q_\ell^{(\pi_B)} = Q_{\pi_B^{-1}(\ell)} \quad \forall\, 0 \leq \ell \leq m_B - 1.$$

It holds that

$$\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{P}^{(\pi_A)},\mathcal{Q}^{(\pi_B)})} = (\Phi_{\pi_A} \otimes \Phi_{\pi_B})\, \rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{P},\mathcal{Q})}\, (\Phi_{\pi_A} \otimes \Phi_{\pi_B})^\dagger,$$

where the unitaries Φ_{π_A} and Φ_{π_B} are defined as

$$\Phi_{\pi_A} = \sum_{k=0}^{m_A-1} |\pi_A(k)\rangle\langle k|, \quad \Phi_{\pi_B} = \sum_{\ell=0}^{m_B-1} |\pi_B(\ell)\rangle\langle \ell|.$$

PROOF: This follows from the fact that $P_k = P^{(\pi_A)}_{\pi_A(k)}$ for all $0 \leq k \leq m_A - 1$ and that $Q_\ell = Q^{(\pi_B)}_{\pi_B(\ell)}$ for all $0 \leq \ell \leq m_B - 1$, which means that

$$\Phi_{\pi_A} A_{\mathcal{P}} = \sum_{k=0}^{m_A-1} \Phi_{\pi_A} |k\rangle\langle P_k| = \sum_{k=0}^{m_A-1} |\pi_A(k)\rangle \left\langle P^{(\pi_A)}_{\pi_A(k)}\right| = \sum_{k'=0}^{m_A-1} |k'\rangle \left\langle P^{(\pi_A)}_{k'}\right| = A_{\mathcal{P}^{(\pi_A)}}$$

and

$$\Phi_{\pi_B} A_{\mathcal{Q}} = \sum_{\ell=0}^{m_B-1} \Phi_{\pi_B} |\ell\rangle\langle Q_\ell| = \sum_{\ell=0}^{m_B-1} |\pi_B(\ell)\rangle \left\langle P^{(\pi_B)}_{\pi_B(\ell)}\right| = \sum_{\ell'=0}^{m_B-1} |\ell'\rangle \left\langle P^{(\pi_B)}_{\ell'}\right| = A_{\mathcal{Q}^{(\pi_B)}}. \quad \blacksquare$$

Reordering the codewords therefore changes the states by some local unitaries, and since we know from Chapter 3 that symmetrically extendable states are preserved under local unitaries, it holds that reordering the codewords has no effect on the symmetric extendability bounds of the filtered states.

Proposition 4.4

For any two announcement sets $\mathcal{P} = \{P_k\}_{k=0}^{m_A-1}$ and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_B-1}$ of n-bit strings, consider the sets $\hat{\mathcal{P}}$ and $\hat{\mathcal{Q}}$ of $(n+x)$-bit strings defined by

$$\hat{\mathcal{P}} = \{\underline{0}^x P_k\}_{k=0}^{m_A-1}, \quad \hat{\mathcal{Q}} = \{\underline{0}^x Q_\ell\}_{k=0}^{m_B-1}$$

for some $x \geq 1$. It holds that[7]

$$\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\hat{\mathcal{P}},\hat{\mathcal{Q}})} = \left(\frac{1-Q}{2}\right)^x \rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{P},\mathcal{Q})}.$$

[7]More generally, this result holds for the sets $\hat{\mathcal{P}} = \{\alpha P_k\}_{k=0}^{m_A-1}$ and $\hat{\mathcal{Q}} = \{\alpha Q_\ell\}_{\ell=0}^{m_B-1}$ for any $\alpha \in \{0,1\}^n$, though for our purposes letting $\alpha = \underline{0}^n$ will be sufficient, as we will see shortly.

PROOF: We have by definition

$$\begin{aligned}\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\hat{\mathcal{P}},\hat{\mathcal{Q}})} &= (A_{\hat{\mathcal{P}}} \otimes A_{\hat{\mathcal{Q}}})(\rho_{\mathcal{Q}}^{A^{n+x}B^{n+x}})(A_{\hat{\mathcal{P}}} \otimes A_{\hat{\mathcal{Q}}})^\dagger \\ &= \sum_{k,k'=0}^{m_A-1} \sum_{\ell,\ell'=0}^{m_B-1} \langle \underline{0}^x P_k, \underline{0}^x Q_\ell | \, \rho_{\mathcal{Q}}^{A^{n+x}B^{n+x}} \, | \underline{0}^x P_{k'}, \underline{0}^x Q_{\ell'} \rangle \, |k,\ell\rangle \langle k',\ell'| \\ &= \langle \underline{0}^x, \underline{0}^x | \, \rho_{\mathcal{Q}}^{A^xB^x} \, | \underline{0}^x, \underline{0}^x \rangle \underbrace{\sum_{k,k'=0}^{m_A-1} \sum_{\ell,\ell'=0}^{m_B-1} \langle P_k, Q_\ell | \, \rho_{\mathcal{Q}}^{A^nB^n} \, | P_{k'}, Q_{\ell'} \rangle \, |k,\ell\rangle \langle k',\ell'|}_{\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{P},\mathcal{Q})}}.\end{aligned}$$

Now, from (4.10), one finds that

$$\langle 0,0 | \, \rho_{\mathcal{Q}}^{AB} \, |0,0\rangle = \frac{1-Q}{2},$$

so that

$$\langle \underline{0}^x, \underline{0}^x | \, \rho_{\mathcal{Q}}^{A^xB^x} \, | \underline{0}^x, \underline{0}^x \rangle = \underbrace{\langle 0,0 | \, \rho_{\mathcal{Q}}^{AB} \, |0,0\rangle \cdots \langle 0,0 | \, \rho_{\mathcal{Q}}^{AB} \, |0,0\rangle}_{x \text{ times}} = \left(\frac{1-Q}{2}\right)^x.$$

Therefore,

$$\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\hat{\mathcal{P}},\hat{\mathcal{Q}})} = \left(\frac{1-Q}{2}\right)^x \rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{P},\mathcal{Q})},$$

as required. ■

The previous proposition tells us that if all the codewords of both announcement sets $\mathcal{P}$ and $\mathcal{Q}$ have a zero in a common location, then removing those zeros from the codewords will not affect the symmetric extendability bounds of the filtered states since the set of symmetrically extendable states is a cone, as stated in Chapter 3.

Given Propositions 4.2 and 4.3 above, it suffices for our purposes to look at announcement sets which do not differ by any of the following:

1. A fixed constant added to each string. This means that we need only consider announcement sets beginning with the string $\underline{0}^n$.
2. A fixed permutation applied to each string.
3. A permutation of the strings themselves within the set. This means that we need only consider announcement sets written in, say, increasing numerical order.
4. A combination of 1 and 2.

For a given block size n and a given number of codewords m, by Proposition 4.4 we may also remove from all possible announcement sets those that contain a column of zeros when the announcement set is written as a matrix with each codeword forming a row. Note that this can only be done if the two announcement sets $\mathcal{P}$ and $\mathcal{Q}$ being used to form the state have a column of zeros of the same width (in Proposition 4.4, that width was x). If not, then this can only be done if (1) $\mathcal{P}$ can be written as $\mathcal{P} = |\mathcal{P}_1|\mathcal{P}_2|$ (this notation will be defined in §4.5.1), where the block size of $\mathcal{P}_1$ is x; (2) $\mathcal{P} = \mathcal{Q}$; or (3) if $\mathcal{P} = \mathcal{B}_n$ (which is a special case of (1)). Since the latter two cases are our main concern, we will always remove announcement sets that contain a column of zeros.

We can indeed exclude announcement sets with a column of zeros when $\mathcal{P} = \mathcal{B}_n$ since we will see in the next section that if $\mathcal{P} = \mathcal{B}_n$ and $\mathcal{Q} = \{\underline{0}^x \hat{Q}_\ell\}_\ell$ for some set $\hat{\mathcal{Q}} = \{\hat{Q}_\ell\}_\ell$ of $(n-x)$-bit strings, then since $\mathcal{B}_n = |\mathcal{B}_x|\mathcal{B}_{n-x}|$ and $\mathcal{Q} = |\{\underline{0}^x\}|\hat{\mathcal{Q}}|$, we have that

$$\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})} = W\left(\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{B}_x,\{\underline{0}^x\})} \otimes \rho^{\tilde{A}_2\tilde{B}_2}_{Q,(\mathcal{B}_{n-x},\hat{\mathcal{Q}})}\right) W^\dagger$$

for some unitary W. Since $\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{B}_x,\{\underline{0}^x\})}$ is separable ($\tilde{B}_1$ is one-dimensional), it is trivially symmetrically extendable, which means that $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ is symmetrically extendable if and only if $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{B}_{n-x},\hat{\mathcal{Q}})}$ is symmetrically extendable.

4.4.1 Number of Inequivalent Announcement Sets

For given block lengths n and announcement set sizes m, we can use the equivalences developed in the previous section to determine the inequivalent announcement sets as follows: take all combinations of announcement sets starting with the zero string and without any columns of zeros and search over all possible combinations of permutations and bit strings. Doing this for $(n, m) = (3, 3)$, we obtain only two inequivalent announcement sets:

$$\left\{\begin{array}{c}000\\101\\110\end{array}\right\}, \quad \left\{\begin{array}{c}000\\110\\111\end{array}\right\}.$$

When $(n, m) = (3, 4)$, there are five inequivalent announcement sets:

$$\left\{\begin{array}{c}000\\011\\100\\111\end{array}\right\}, \quad \left\{\begin{array}{c}000\\011\\101\\110\end{array}\right\}, \quad \left\{\begin{array}{c}000\\100\\101\\110\end{array}\right\}, \quad \left\{\begin{array}{c}000\\100\\110\\111\end{array}\right\}, \quad \left\{\begin{array}{c}000\\101\\110\\111\end{array}\right\}.$$

The search over all permutations and bit strings grows very rapidly with n since the number of permutations is $n!$ and the number of bit strings is 2^n. This means that for each n we have to search $n! \cdot 2^n$ combinations of permutations and bit strings to determine all the inequivalent sets. By doing this for some small (n, m) pairs, we obtain the following table giving us the number of inequivalent announcement sets.

n \ m	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	1	1												
3	1	2	5	3	3	1								
4	1	3	13	24	47	55	73	56	50	27	19	6	4	1
5	1	4	28	104										
6	1	6												
7	1	7												
8	1	9												
9	1													
10	1													
11	1													
12	1													

Table 4.1: Number of inequivalent announcement sets for some small block lengths n and announcement set sizes m. The highest possible m for each n such that the announcement set is non-trivial is $2^n - 1$. Blank cells are undetermined.

For all $n \geq 2$ and $m = 2$, there is always only one inequivalent announcement set, which is $\{\underline{0}^n, \underline{1}^n\}$.

4.5 New Announcement Sets from Old Ones

We now go through two methods of combining codes that are relevant to this thesis. The main reference for this section is [MS77], wherein one can find many more ways of combining codes to obtain new ones.

4.5.1 The Direct Sum Construction

For any code $\mathcal{P} = \{P_k\}_{k=0}^{m_1-1}$ of block length n_1 and any code $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_2-1}$ of block length n_2, the *direct sum* $|\mathcal{P}|\mathcal{Q}|$ *of* $\mathcal{P}$ *and* $\mathcal{Q}$ is defined as

$$|\mathcal{P}|\mathcal{Q}| = \{P_k Q_\ell : \ 0 \leq k \leq m_1 - 1, \ 0 \leq \ell \leq m_2 - 1\}^8. \tag{4.20}$$

It is natural to adopt the following two-index labelling of the elements of $|\mathcal{P}|\mathcal{Q}|$:

$$(|\mathcal{P}|\mathcal{Q}|)_{(i,j)} = P_i Q_j \quad \forall\, 0 \leq i \leq m_1 - 1, \ \forall\, 0 \leq j \leq m_2 - 1. \tag{4.21}$$

Then, by definition (4.1), the filter $A_{|\mathcal{P}|\mathcal{Q}|}$ used to post-select on $|\mathcal{P}|\mathcal{Q}|$ is

$$A_{|\mathcal{P}|\mathcal{Q}|} = \sum_{k=0}^{m_1-1} \sum_{\ell=0}^{m_2-1} {}^{\tilde{A}} \, |k, \ell\rangle \langle P_k Q_\ell|^{A^{n_1+n_2}}. \tag{4.22}$$

Note that $d_{\tilde{A}} = m_1 m_2$, so that $\mathfrak{H}_{\tilde{A}} \cong \mathfrak{H}_{\tilde{A}_1} \otimes \mathfrak{H}_{\tilde{A}_2}$, where $d_{\tilde{A}_1} = m_1$ and $d_{\tilde{A}_2} = m_2$. It then follows, as we show in Proposition B.1 of Appendix B, that for sets $\mathcal{P}_1 = \{P_{1,k}\}_{k=0}^{m_{A_1}-1}$ and $\mathcal{Q}_1 = \{Q_{1,\ell}\}_{\ell=0}^{m_{B_1}-1}$ of n_1-bit strings, and for

[8] The notation $P_k Q_\ell$ is meant to indicate that the two strings P_k and Q_ℓ are put together to form one larger $(n_1 + n_2)$-bit string. This is called the direct sum of $\mathcal{P}$ and $\mathcal{Q}$ because if both $\mathcal{P}$ and $\mathcal{Q}$ are linear codes with generator matrices $G_\mathcal{P}$ and $G_\mathcal{Q}$, respectively, then $G_{|\mathcal{P}|\mathcal{Q}|} = G_\mathcal{P} \oplus G_\mathcal{Q}$, that is, the generator matrix of $|\mathcal{P}|\mathcal{Q}|$ is the direct sum of the generator matrices of $\mathcal{P}$ and $\mathcal{Q}$.

sets $\mathcal{P}_2 = \{P_{2,k}\}_{k=0}^{m_{A_2}-1}$ and $\mathcal{Q}_2 = \{Q_{2,\ell}\}_{\ell=0}^{m_{B_2}-1}$ of n_2-bit strings, we have

$$\rho^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}_{\mathcal{Q},(|\mathcal{P}_1|\mathcal{P}_2|,\\ |\mathcal{Q}_1|\mathcal{Q}_2|)} = W\left(\rho^{\tilde{A}_1\tilde{B}_1}_{\mathcal{Q},(\mathcal{P}_1,\mathcal{Q}_1)} \otimes \rho^{\tilde{A}_2\tilde{B}_2}_{\mathcal{Q},(\mathcal{P}_2,\mathcal{Q}_2)}\right) W^\dagger, \tag{4.23}$$

where $W = \mathrm{SWAP}_{\tilde{A}_2\tilde{B}_1}$ is the unitary operator that swaps the $\mathfrak{H}_{\tilde{A}_2}$ and $\mathfrak{H}_{\tilde{B}_1}$ spaces and is defined analogously to (3.1). In other words the filtered state resulting from post-selection on direct sum of codes is equal (up to ordering of the tensor factors) to the *tensor product* of the filtered states resulting from post-selection on the codes forming the direct sum. It is then straightforward to show that $\rho^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}_{\mathcal{Q},(|\mathcal{P}_1|\mathcal{P}_2|,\\ |\mathcal{Q}_1|\mathcal{Q}_2|)}$ is symmetrically extendable if $\rho^{\tilde{A}_1\tilde{B}_1}_{\mathcal{Q},(\mathcal{P}_1,\mathcal{Q}_1)}$ *and* $\rho^{\tilde{A}_2\tilde{B}_2}_{\mathcal{Q},(\mathcal{P}_2,\mathcal{Q}_2)}$ are symmetrically extendable. This result can be extended to apply to announcement sets formed from a direct sum of an arbitrary number of announcement sets. If $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_k$ and $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_k$ are two sets of k announcement sets, with resulting filtered states $\rho^{\tilde{A}_1\tilde{B}_1}_{\mathcal{Q},(\mathcal{P}_1,\mathcal{Q}_1)}, \rho^{\tilde{A}_2\tilde{B}_2}_{\mathcal{Q},(\mathcal{P}_2,\mathcal{Q}_2)}, \ldots, \rho^{\tilde{A}_k\tilde{B}_k}_{\mathcal{Q},(\mathcal{P}_k,\mathcal{Q}_k)}$, then

$$\rho^{\tilde{A}_1\cdots\tilde{A}_k\tilde{B}_1\cdots\tilde{B}_k}_{\mathcal{Q},(|\mathcal{P}_1|\cdots|\mathcal{P}_k|,\\ |\mathcal{Q}_1|\cdots|\mathcal{Q}_k|)} = W\left(\rho^{\tilde{A}_1\tilde{B}_1}_{\mathcal{Q},(\mathcal{P}_1,\mathcal{Q}_1)} \otimes \cdots \otimes \rho^{\tilde{A}_k\tilde{B}_k}_{\mathcal{Q},(\mathcal{P}_k,\mathcal{Q}_k)}\right) W^\dagger,$$

where W performs the appropriate tensor factor swapping. Then, $\rho^{\tilde{A}_1\cdots\tilde{A}_k\tilde{B}_1\cdots\tilde{B}_k}_{\mathcal{Q},(|\mathcal{P}_1|\cdots|\mathcal{P}_k|,\\ |\mathcal{Q}_1\cdots|\mathcal{Q}_k|)}$ is symmetrically extendable if $\rho^{\tilde{A}_1\tilde{B}_1}_{\mathcal{Q},(\mathcal{P}_1,\mathcal{Q}_1)}, \ldots, \rho^{\tilde{A}_k\tilde{B}_k}_{\mathcal{Q},(\mathcal{P}_k,\mathcal{Q}_k)}$ are *all* symmetrically extendable.

4.5.2 Levenshtein's Construction

Let $\mathcal{P} = \{P_k\}_{k=0}^{m_1-1}$ be an announcement set of n_1-bit strings and $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m_2-1}$ be an announcement set of n_2-bit strings. The *Levenshtein construction from a copies of* $\mathcal{P}$ *and* b *copies of* $\mathcal{Q}$, denoted $a\mathcal{P} + b\mathcal{Q}$, is obtained by pasting a copies of the codewords of $\mathcal{P}$ side-by-side with b copies of the codewords of $\mathcal{Q}$ side-by-side and omitting the last $m_2 - m_1$ rows of $\mathcal{Q}$ (if $m_1 < m_2$) or omitting the last $m_1 - m_2$ rows of $\mathcal{P}$ (if $m_1 > m_2$), as shown in the diagram below.

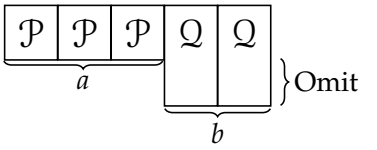


Figure 4.3: The Levenshtein construction $a\mathcal{P} + b\mathcal{Q}$.

$a\mathcal{P} + b\mathcal{Q}$ is a new announcement set with block size $n_1 + n_2$ and size $\min\{m_1, m_2\}$. If $m_1 = m_2 = m$, then we can write

$$a\mathcal{P} + b\mathcal{Q} = \{\underbrace{P_k \cdots P_k}_{a \text{ times}} \underbrace{Q_k \cdots Q_k}_{b \text{ times}} : 0 \leq k \leq m-1\}.$$

In this case, we show in Proposition B.2 that if Alice and Bob both filter on $a\mathcal{P} + b\mathcal{Q}$, then

$$\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},a\mathcal{P}+b\mathcal{Q}} = \left(\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},\mathcal{P}}\right)^{\circ a} \circ \left(\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},\mathcal{Q}}\right)^{\circ b}, \tag{4.24}$$

where $\circ$ denotes the *Hadamard product* (also sometimes called the *Schur product*), which for two matrices A and B of the same size is defined as

$$(A \circ B)_{\substack{k \\ \ell}} = A_{\substack{k \\ \ell}} B_{\substack{k \\ \ell}} \quad \forall\, k, \ell. \tag{4.25}$$

The Levenshtein construction $a\mathcal{P}$ of a copies of an announcement set $\mathcal{P}$ is a simple way of increasing the block length of a code while keeping the number of codewords constant. We will use this construction in Chapter 6.

Summary

In this chapter, we have looked at general two-way post-processing protocols that might break the symmetric extendability of Alice and Bob's initial correlations for QKD protocols using the six-state signal states whenever the QBER Q is in the gap $\left[\frac{5-\sqrt{5}}{10}, \frac{1}{3}\right]$. By not caring about the resulting rate of key distillation, we have managaed to reduce the problem to looking at the symmetric extendability of states resulting from Alice and Bob performing an independent post-selection on error-correcting codes. We have conjectured that it is sufficient to consider Alice and Bob post-selecting on the same code, and we have also conjectured a general way of constructing symmetric extensions of the resulting states. We have also looked at equivalence of codes and the effect of combining codes in particular ways on the post-selected states.

Having laid all of this groundwork, we are now ready to begin looking more closely at particular codes $\mathcal{P}, \mathcal{Q}$ and the symmetric extendability of the resulting filtered states $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}$. We will start with the repetition codes $\mathcal{R}_n$, then move to the more general simplex codes $\mathcal{S}(n, d, m)$.

Chapter 5

Repetition Codes

The *repetition codes $\mathcal{R}_n$ of block size n* are defined as

$$\mathcal{R}_n = \{\underline{0}^n, \underline{1}^n\} \quad \forall\, n \geq 1.$$

The post-selection protocol obtained from this code is advantage distillation, which as explained in the introduction currently provides the best-known lower bound of $\frac{5-\sqrt{5}}{10}$ for QKD with the six-state signal states. In this chapter, we will derive this bound using our new framework along with the condition (3.2), which determines the symmetric extendability of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ for all $n \geq 1$. This will reproduce the known result from [Myh+09] that advantage distillation cannot be used to break symmetric extendability beyond $\frac{5-\sqrt{5}}{10}$. The derivation provided here using our new framework is considerably simpler than that original one, which involved analytically solving the SDP associated with the updated states.

Next, we will use (3.11) to find the channel $\mathcal{N}$ such that $\mathcal{N} \circ \mathrm{Tr}_{E_2}$ constructs a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ and will discover that it works throughout the symmetrically extendable region of the states (that is, for all $Q \geq Q^*_{\mathcal{R}_n}$) for all $n \geq 1$. Finally, we will prove Conjecture 2 for repetition codes by showing, using the strategy given by (3.6), that Tr_{E_2} alone constructs a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ at $Q = Q^*_{\mathcal{R}_n}$ for all $n \geq 1$.

It is worth mentioning that the filter $A_{\mathcal{R}_n} = |0\rangle\langle\underline{0}^n| + |1\rangle\langle\underline{1}^n|$ that we will use here as part of our framework had been used previously in [KBR07] to generalize the one-way security proofs of QKD presented in [RGK05; KGR05].

5.1 Derivation of Current Security Bounds from Symmetric Extendability Criterion

Recalling that

$$\rho^{AB}_Q = \begin{bmatrix} \frac{1-Q}{2} & 0 & 0 & \frac{1-2Q}{2} \\ 0 & \frac{Q}{2} & 0 & 0 \\ 0 & 0 & \frac{Q}{2} & 0 \\ \frac{1-2Q}{2} & 0 & 0 & \frac{1-Q}{2} \end{bmatrix},$$

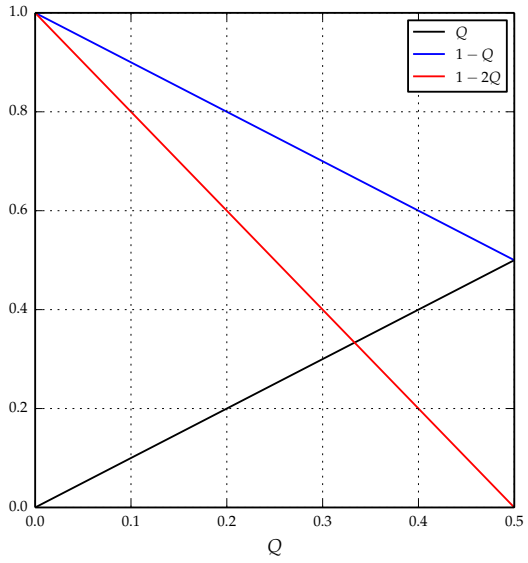
it can be shown using (4.12) that

$$\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}} = \begin{bmatrix} \left(\frac{1-Q}{2}\right)^n & 0 & 0 & \left(\frac{1-2Q}{2}\right)^n \\ 0 & \left(\frac{Q}{2}\right)^n & 0 & 0 \\ 0 & 0 & \left(\frac{Q}{2}\right)^n & 0 \\ \left(\frac{1-2Q}{2}\right)^n & 0 & 0 & \left(\frac{1-Q}{2}\right)^n \end{bmatrix}$$

Note that $\rho_{Q,\mathcal{R}_1}^{\tilde{A}\tilde{B}} = \rho_Q^{AB}$. For convenience, we define

$$q_0 = \left(\frac{Q}{2}\right)^n, \quad q_1 = \left(\frac{1-Q}{2}\right)^n, \quad q_2 = \left(\frac{1-2Q}{2}\right)^n,$$

which are non-negative for all $0 \leq Q \leq \frac{1}{2}$ and all $n \geq 1$. Also, using the figure below, we have that $q_1 \geq q_0$ and $q_1 \geq q_2$ for all $0 \leq Q \leq \frac{1}{2}$ and all $n \geq 1$, and $q_2 \geq q_0$ for all $0 \leq Q \leq \frac{1}{3}$ for all $n \geq 1$.



Now, we want to determine the symmetric extendability of the states $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ for each $n \geq 1$. Note first that these states are Bell-diagonal (recall the general form (2.21) of such states) with eigenvalues

$$p_I = q_1 + q_2, \quad p_z = q_1 - q_2, \quad p_x = q_0, \quad p_y = q_0 \tag{5.1}$$

in the canonical form (2.31). Their separability is therefore given by Proposition 2.23, using which we get that for all $n \geq 1$ $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ is separable for $Q \geq \frac{1}{3}$, the same as for the original states ρ_Q^{AB}. Since all separable states are symmetrically extendable, it must be that the symmetric extendability threshold $Q_{\mathcal{R}_n}^*$ is less than or equal to $\frac{1}{3}$ for all $n \geq 1$. Using (5.1), we find that

$$\det\left(\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}\right) = q_0^2(q_1^2 - q_2^2), \quad \text{Tr}\left[\left(\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}\right)^2\right] = 2q_0^2 + 2q_1^2 + 2q_2^2, \quad \text{and} \quad \text{Tr}\left[\left(\rho_{Q,\mathcal{R}_n}^{\tilde{B}}\right)^2\right] = 2q_1^2 + 2q_0^2 + 4q_0q_1.$$

Therefore, the condition

$$4\sqrt{\det\left(\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}\right)} \geq \mathrm{Tr}\left[\left(\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}\right)^2\right] - \mathrm{Tr}\left[\left(\rho_{Q,\mathcal{R}_n}^{\tilde{B}}\right)^2\right], \tag{5.2}$$

which is necessary and sufficient for the symmetric extendability of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$, becomes

$$4\sqrt{q_0^2(q_1^2 - q_2^2)} \geq 2q_2^2 - 4q_0q_1. \tag{5.3}$$

Squaring both sides of this inequality and simplifying gives

$$\begin{aligned} 16q_0^2q_1^2 - 16q_0^2q_2^2 &\geq 4q_2^4 - 16q_2^2q_0q_1 + 16q_0^2q_1^2 \\ \Rightarrow 4q_2^4 - 16q_2^2q_0q_1 + 16q_0^2q_2^2 &= 4q_2^2(q_2^2 - 4q_0q_1 + 4q_0^2) \leq 0 \\ \Rightarrow q_2^2 - 4q_0q_1 + 4q_0^2 &\leq 0. \end{aligned}$$

Substituting the definitions of q_0, q_1, q_2 into the last inequality above gives

$$4Q^{2n} - 4Q^n(1-Q)^n + (1-2Q)^{2n} \leq 0. \tag{5.4}$$

Let

$$f_n(Q) := 4Q^{2n} - 4Q^n(1-Q)^n + (1-2Q)^{2n}. \tag{5.5}$$

The root(s) of f_n give us $Q_n^* \equiv Q_{\mathcal{R}_n}^*$ for all $n \geq 1$, that is, the threshold error(s) beyond which $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ is symmetrically extendable. It turns out that in the interval $\left[0, \frac{1}{3}\right]$ there exists only one root, hence only one threshold error, for all n. Moreover, as shown in Figure 5.1, the threshold increases monotonically with n, which means that $Q_\infty^* := \lim_{n\to\infty} Q_n^*$ is the highest possible threshold with advantage distillation, and it is the number we seek.

n	Q_n^*
1	0.16666
2	0.21507
3	0.23441
4	0.24772
5	0.25105
6	0.25531
7	0.25836
8	0.26064
9	0.26241
10	0.26383

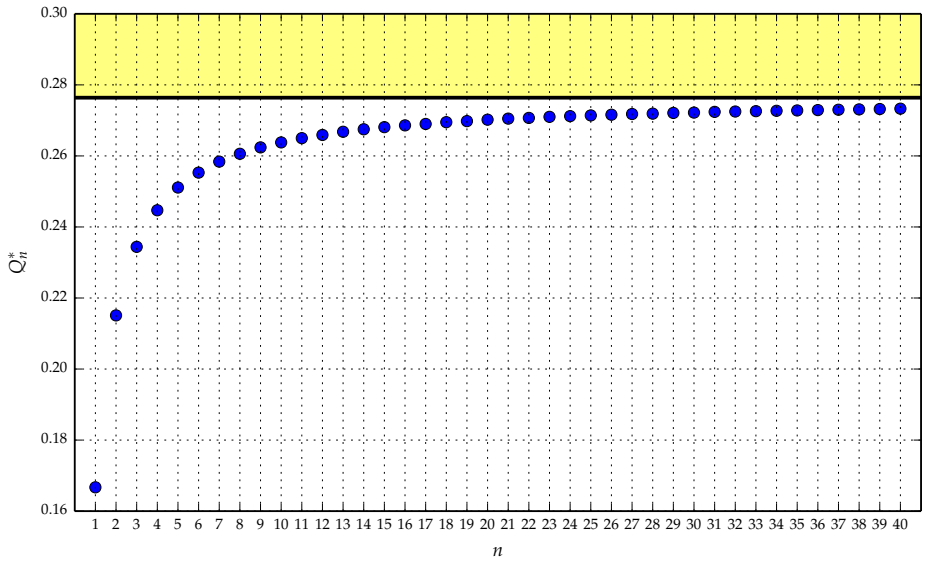


Figure 5.1: (Left) A table of Q_n^* from $n = 1$ to $n = 10$. (Right) A plot of Q_n^* from $n = 1$ to $n = 40$. Indicated in yellow is the gap.

Now, it holds that $4Q^{2n} \leq (1-2Q)^{2n}$ for all $Q \leq \frac{1}{2+2^{\frac{1}{n}}}$ for all $n \geq 1$. This means that as n increases, f_n tends to $\tilde{f}_n$ for all $Q \leq \frac{1}{3}$, where

$$\tilde{f}_n(Q) := -4Q^n(1-Q)^n + (1-2Q)^{2n}. \tag{5.6}$$

Therefore, we have that $Q_\infty^* = \tilde{Q}_\infty^*$, where $\tilde{Q}_\infty^* := \lim_{n\to\infty} \tilde{Q}_n^*$ and $\tilde{Q}_n^*$ is the root of $\tilde{f}_n$ in the interval $\left[0, \frac{1}{3}\right]$, which can be shown to be

$$\tilde{Q}_n^* = \frac{\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}}+1\right) - \sqrt{\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}}+1\right)^2 - 4\left(\frac{1}{4}\right)^{\frac{1}{n}}\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}}+1\right)}}{2\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}}+1\right)}.$$

Therefore,

$$\tilde{Q}_\infty^* = Q_\infty^* = \frac{5-\sqrt{5}}{10}.$$

This is exactly the current best-known lower bound for QKD with the six-state signal states and two-way classical post-processing that was first derived in [Cha02]. We have thus used our framework to show, as was originally done in [Myh+09] by analytically solving the SDP (3.3), that advantage distillation cannot break the symmetric extendability of Alice and Bob's initial correlations beyond $\frac{5-\sqrt{5}}{10}$.

The analysis for the BB84 signal states using $\rho_{Q,x}^{AB}$ is a bit more involved: since for every Q there exists a family $\{\rho_{Q,x}^{AB}\}_{x\in[0,Q]}$ consistent with Alice and Bob's measurement results, to determine the highest possible threshold with advantage distillation we must determine for each $n > 1$ the highest possible Q such that the set $\{\rho_{Q,x,\mathcal{R}_n}^{\tilde{A}\tilde{B}}\}_{x\in[0,Q]}$ does not contain a symmetrically extendable state, where $\rho_{Q,x,\mathcal{R}_n}^{\tilde{A}\tilde{B}} := (A_{\mathcal{R}_n} \otimes A_{\mathcal{R}_n})(\rho_{Q,x}^{A^nB^n})(A_{\mathcal{R}_n} \otimes A_{\mathcal{R}_n})^\dagger$. We go through the analysis in Appendix C.

5.2 The Special Construction of a Symmetric Extension

Let us now use the the special map $\mathcal{E} = \mathcal{N} \circ \mathrm{Tr}_{E_2}$ presented in §3.3 to explicitly construct a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$. Recall that whether or not the special map can construct a symmetric extension of any state depends on whether $\mathcal{N}$ is completely-positive, which depends on whether the eigenvalues of $J(\mathcal{N})$ are non-negative.

We will be making use of the following identities throughout this section:

$$\begin{aligned}
&1.\quad (q_2^*)^2 = 4q_0^*q_1^* - 4(q_0^*)^2;\\
&2.\quad \sqrt{(q_1^*)^2 - (q_2^*)^2} = q_1^* - 2q_0^*;\\
&3.\quad q_2^* = \sqrt{q_0^*}\left(\sqrt{q_1^*+q_2^*} + \sqrt{q_1^*-q_2^*}\right);\\
&4.\quad q_0^* = \tfrac{1}{2}\left(q_1^* - \sqrt{(q_1^*)^2-(q_2^*)^2}\right);\\
&5.\quad 2q_0^* = \sqrt{q_0^*}\left(\sqrt{q_1^*+q_2^*} - \sqrt{q_1^*-q_2^*}\right);\\
&6.\quad q_1^* = q_0^* + \tfrac{1}{2}q_1^* + \tfrac{1}{2}\sqrt{(q_1^*)^2-(q_2^*)^2},
\end{aligned} \tag{5.7}$$

where, for example, q_0^* refers to q_0 evaluated at the thresholds Q_n^*. These identities can be proved using (5.3), which at Q_n^* holds with equality.

We can use formula (3.11) to determine that the Choi representation of $\mathcal{N}$ is

$$\begin{aligned} J(\mathcal{N}) = &\underbrace{\left[\frac{q_1^2 - q_0^2 + \Delta}{2\Delta} + \frac{q_2}{\sqrt{q_0}\left(\sqrt{q_1+q_2}+\sqrt{q_1-q_2}\right)}\right]}_{\Lambda_1} \left|\Phi^+\right\rangle\left\langle\Phi^+\right| \\ &+ \underbrace{\left[\frac{q_1^2 - q_0^2 + \Delta}{2\Delta} - \frac{q_2}{\sqrt{q_0}\left(\sqrt{q_1+q_2}+\sqrt{q_1-q_2}\right)}\right]}_{\Lambda_2} \left|\Phi^-\right\rangle\left\langle\Phi^-\right| \\ &+ \underbrace{\left[\frac{\Delta - q_1^2 + q_0^2}{2\Delta}\right]}_{\Lambda_{3,4}} \left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right), \end{aligned} \tag{5.8}$$

where

$$\Delta \equiv q_0^2 + (q_1 + q_0)\sqrt{q_1^2 - q_2^2} + q_1 q_0.$$

It holds that

$$\mathrm{Tr}_{\tilde{B}'}[J(\mathcal{N})] = \left(\frac{q_1^2 - q_0^2 + \Delta}{\Delta} + \frac{\Delta - q_1^2 + q_0^2}{\Delta}\right)\left(\frac{\mathbb{1}_{\tilde{A}}}{2}\right) = \mathbb{1}_{\tilde{A}},$$

which means that $\mathcal{N}$ is trace-preserving.

The eigenvalues of $J(\mathcal{N})$ are in the square brackets of the expression above for $J(\mathcal{N})$, and for $\mathcal{N}$ to be completely-positive, and hence for a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ to be constructed using $\mathcal{N} \circ \mathrm{Tr}_{E_2}$, we need them to be non-negative for at least some subset of $Q \geq Q_n^*$ for all $n \geq 1$.

Writing Δ above as

$$\Delta = (q_0 + q_1)\left(q_0 + \sqrt{q_1^2 - q_2^2}\right),$$

the condition $\Lambda_{3,4} \geq 0$ can be simplified to

$$\begin{aligned} (q_0 + q_1)\left(q_0 + \sqrt{q_1^2 - q_2^2}\right) = \Delta &\geq q_1^2 - q_0^2 \\ \Rightarrow q_0 + \sqrt{q_1^2 - q_2^2} &\geq q_1 - q_0 \\ \Rightarrow \sqrt{q_1^2 - q_2^2} &\geq q_1 - 2q_0 \\ \Rightarrow q_1^2 - q_2^2 &\geq q_1^2 - 4q_0 q_1 + 4q_0^2 \\ \Rightarrow 4q_0^2 - 4q_0 q_1 + q_2^2 &\leq 0. \end{aligned}$$

The last line is the condition (5.4) for $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ to be symmetrically extendable. So $\Lambda_{3,4}$ vanishes at Q_n^* for all $n \geq 1$ and is positive for all $Q > Q_n^*$. Furthermore, by using identities 2 and 3 from (5.7), we obtain

$$\Delta|_{Q=Q_n^*} = -(q_0^*)^2 + (q_1^*)^2 \quad \forall n \geq 1,$$

which leads to

$$\Lambda_2|_{Q=Q_n^*} = \frac{(q_1^*)^2 - (q_0^*)^2 - (q_0^*)^2 + (q_1^*)^2}{-2(q_0^*)^2 + 2(q_1^*)^2} - 1 = \frac{2(q_1^*)^2 - 2(q_0^*)^2}{2(q_1^*)^2 - 2(q_0^*)^2} - 1 = 1 - 1 = 0 \quad \forall\, n \geq 1.$$

Therefore, Λ_2 also vanishes at Q_n^* for all $n \geq 1$ and $\Lambda_2 > 0$ for all $Q > Q_n^*$. And since $\Lambda_1 \geq 0$ for all $0 \leq Q \leq \frac{1}{2}$ and all $n \geq 1$[1], it holds that the eigenvalues of $J(\mathcal{N})$ are non-negative for all $Q \geq Q_n^*$ for all $n \geq 1$, which means that $\mathcal{N} \circ \mathrm{Tr}_{E_2}$ constructs a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ throughout its symmetrically extendable region for all $n \geq 1$. Not only that, but by using again identities 2 and 3 from (5.7) we obtain

$$J(\mathcal{N})|_{Q=Q_n^*} = (1+1)\left|\Phi^+\right\rangle\left\langle\Phi^+\right| = 2\left|\Phi^+\right\rangle\left\langle\Phi^+\right| = J(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{\tilde{B}'})}) \quad \forall\, n \geq 1.$$

In other words, for all $n \geq 1$, Tr_{E_2} alone constructs a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ when $Q = Q_n^*$. This proves for repetition codes Conjecture 2 that the channel constructing a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ can be decomposed into two steps, the first being the channel that on its own constructs a symmetric extension at the threshold Q_n^* and the second channel that, by virtue of being completely-positive and trace-preserving for all Q beyond the threshold, acts like a post-processing step that completes the construction of a symmetric extension for all $Q > Q_n^*$.

5.2.1 Derivation of the Channel at the Threshold

In this section, we go through the arguments that lead to the discovery that the channel Tr_{E_2}, as we have just seen, constructs a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ at the threshold value Q_n^* for all $n \geq 1$.

Now, $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ is Bell-diagonal, so writing the general symmetric extension (3.13) of a Bell-diagonal state in the Bell basis on $\mathfrak{H}_{\tilde{A}}, \mathfrak{H}_{\tilde{B}}$, we get

$$\begin{aligned}
\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}\tilde{B}'}(\vec{\beta}) = {} & \left|\Phi^+\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes (q_2+q_1)\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_z}{4} - \frac{q_0}{2} + \frac{q_1}{2}\right)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_x}{4} + \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_y}{4} + \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_z}{4} - \frac{q_0}{2} + \frac{q_1}{2}\right)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes (q_1-q_2)\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_y}{4} - \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_x}{4} - \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_x}{4} + \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{q_2}{2} - \frac{\beta_y}{4}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes q_0\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{q_1}{2} - \frac{q_0}{2} - \frac{\beta_z}{4}\right)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(-\frac{\beta_y}{4} - \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{\beta_x}{4} - \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{q_1}{2} - \frac{q_0}{2} - \frac{\beta_z}{4}\right)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes q_0\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'},
\end{aligned} \tag{5.9}$$

where recall that $\vec{\beta} = (\beta_x, \beta_y, \beta_z)$ are open parameters that need to be chosen such that the resulting operator is positive semi-definite. This expression is the analogue to (3.4).

[1]This is due to the fact that q_0, q_1, q_2 are non-negative for all $0 \leq Q \leq \frac{1}{2}$ for all $n \geq 1$ and that $q_1 \geq q_0$, so that $q_1^2 - q_0^2 \geq 0$.

Lemma 5.1

The choice

$$\beta_x = \beta_y = 4q_0, \quad \beta_z = 2q_1 - 6q_0$$

makes $\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,\mathcal{R}_n}(\vec{\beta})$ positive semi-definite for all $Q \geq Q^*_n$ for all $n \geq 1$.

PROOF: Substituting $\beta_x = \beta_y = 4q_0$ and $\beta_z = 2q_1 - 6q_0$ into (5.9) gives us

$$\begin{aligned}
\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,\mathcal{R}_n}(4q_0, 4q_0, 2q_1 - 6q_0) = {} & \left|\Phi^+\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes (q_2 + q_1)\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes (q_1 - 2q_0)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 + \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Phi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 + \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes (q_1 - 2q_0)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes (q_1 - q_2)\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 - \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Phi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 - \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 + \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes \left(\frac{q_2}{2} - q_0\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes q_0\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Psi^+\right|^{\tilde{A}\tilde{B}} \otimes (q_0)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} \\
& + \left|\Phi^+\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(-q_0 - \frac{q_2}{2}\right)\left(\frac{\mathrm{i}\sigma_y}{2}\right)^{\tilde{B}'} + \left|\Phi^-\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes \left(q_0 - \frac{q_2}{2}\right)\left(\frac{\sigma_x}{2}\right)^{\tilde{B}'} \\
& + \left|\Psi^+\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes (q_0)\left(\frac{\sigma_z}{2}\right)^{\tilde{B}'} + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|^{\tilde{A}\tilde{B}} \otimes q_0\left(\frac{\mathbb{1}}{2}\right)^{\tilde{B}'}.
\end{aligned} \tag{5.10}$$

As a matrix in the standard basis of $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, this is equal to

$$\rho^{\tilde{A}\tilde{B}\tilde{B}'}_{Q,\mathcal{R}_n}(4q_0, 4q_0, 2q_1 - 6q_0) = \begin{bmatrix}
q_1 - q_0 & 0 & 0 & 0 & 0 & \frac{q_2}{2} & \frac{q_2}{2} & 0 \\
0 & q_0 & q_0 & 0 & 0 & 0 & 0 & \frac{q_2}{2} \\
0 & q_0 & q_0 & 0 & 0 & 0 & 0 & \frac{q_2}{2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{q_2}{2} & 0 & 0 & 0 & 0 & q_0 & q_0 & 0 \\
\frac{q_2}{2} & 0 & 0 & 0 & 0 & q_0 & q_0 & 0 \\
0 & \frac{q_2}{2} & \frac{q_2}{2} & 0 & 0 & 0 & 0 & q_1 - q_0
\end{bmatrix},$$

and it has eigenvalues

$$0, \quad 0, \quad \frac{q_0 + q_1}{2} - \frac{1}{2}\sqrt{(3q_0 - q_1)^2 + 2q_2^2}, \quad \frac{q_0 + q_1}{2} + \frac{1}{2}\sqrt{(3q_0 - q_1)^2 + 2q_2^2},$$

each with multiplicity two. The fourth eigenvalue is non-negative for all $Q \in \left[0, \frac{1}{2}\right]$ and all $n \geq 1$ due to the non-negativity of q_0, q_1, q_2, while simplification shows that the third eigenvalue is non-negative if and only if

$$4Q^{2n} - 4Q^n(1 - Q)^n + (1 - 2Q)^{2n} \leq 0,$$

which is exactly the condition (5.4), so that the third eigenvalue is non-negative for all $Q \geq Q_n^*$ for all $n \geq 1$. This proves that $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}\tilde{B}'}(4q_0, 4q_0, 2q_1 - 6q_0)$ is positive semi-definite for all $Q \geq Q_n^*$ for all $n \geq 1$ and therefore is a symmetric extension of $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ throughout its symmetrically extendable region for all $n \geq 1$. ■

Now, from the purification

$$|\psi\rangle_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}E_1E_2} = \operatorname{vec}\left(\sqrt{\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}}\right) = \left|\Phi^+\right\rangle^{\tilde{A}\tilde{B}} \otimes \sqrt{q_1+q_2}\left|\Phi^+\right\rangle^{E_1E_2} + \left|\Phi^-\right\rangle^{\tilde{A}\tilde{B}} \otimes \sqrt{q_1-q_2}\left|\Phi^-\right\rangle^{E_1E_2} + \left|\Psi^+\right\rangle^{\tilde{A}\tilde{B}} \otimes \sqrt{q_0}\left|\Psi^+\right\rangle^{E_1E_2} + \left|\Psi^-\right\rangle^{\tilde{A}\tilde{B}} \otimes \sqrt{q_0}\left|\Psi^-\right\rangle^{E_1E_2},$$

a channel $\mathcal{E}_{Q,\mathcal{R}_n}$ such that $(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_{\tilde{A}\tilde{B}})} \otimes \mathcal{E}_{Q,\mathcal{R}_n})\left(|\psi\rangle\langle\psi|_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}E_1E_2}\right) = \rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}\tilde{B}'}(4q_0, 4q_0, 2q_1 - 6q_0)$ must satisfy

$$\begin{aligned}
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) = \frac{\mathbb{1}^{\tilde{B}'}}{2},\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Psi^+\right|\right) = \frac{q_0 + \frac{q_2}{2}}{\sqrt{q_0(q_1+q_2)}}\left(\frac{\sigma_x^{\tilde{B}'}}{2}\right),\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Phi^-\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Psi^-\right|\right) = \frac{q_0 - \frac{q_2}{2}}{\sqrt{q_0(q_1-q_2)}}\left(\frac{\sigma_x^{\tilde{B}'}}{2}\right),\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Phi^+\right|\right) = -\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Psi^-\right|\right) = \frac{q_0 + \frac{q_2}{2}}{\sqrt{q_0(q_1+q_2)}}\left(\frac{\mathrm{i}\sigma_y^{\tilde{B}'}}{2}\right),\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Psi^+\right|\right) = -\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Phi^-\right|\right) = \frac{\frac{q_2}{2} - q_0}{\sqrt{q_0(q_1-q_2)}}\left(\frac{\mathrm{i}\sigma_y^{\tilde{B}'}}{2}\right),\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Phi^-\right|\right) = \frac{q_1 - 2q_0}{\sqrt{q_1^2 - q_2^2}}\left(\frac{\sigma_z^{\tilde{B}'}}{2}\right),\\
&\mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Psi^+\right|\right) = \mathcal{E}_{Q,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Psi^-\right|\right) = \frac{\sigma_z^{\tilde{B}'}}{2}.
\end{aligned} \tag{5.11}$$

These conditions are the analogue to (3.6), and they define $\mathcal{E}_{Q,\mathcal{R}_n}$ on an orthonormal basis, which therefore uniquely defines it. It is manifestly trace-preserving.

Theorem 5.2

For all $n \geq 1$, $\mathcal{E}_{Q_n^*,\mathcal{R}_n} = \mathrm{Tr}_{E_2}$.

PROOF: Using identities 3 and 5 from (5.7), we get that at Q_n^* for all $n \geq 1$,

$$\sqrt{q_0^*\left(q_1^* + q_2^*\right)} = q_0^* + \frac{q_2^*}{2} \quad \text{and} \quad \sqrt{q_0^*\left(q_1^* - q_2^*\right)} = \frac{q_2^*}{2} - q_0^*.$$

Using as well identity 2 from (5.7) gives us after substitution into (5.11)

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) = \frac{\mathbb{1}^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Psi^+\right|\right) = \frac{\sigma_x^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Phi^-\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Psi^-\right|\right) = -\frac{\sigma_x^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Phi^+\right|\right) = -\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Psi^-\right|\right) = \frac{\mathrm{i}\sigma_y^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Psi^+\right|\right) = -\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Phi^-\right|\right) = \frac{\mathrm{i}\sigma_y^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^-\right\rangle\left\langle\Phi^+\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Phi^+\right\rangle\left\langle\Phi^-\right|\right) = \frac{\sigma_z^{\tilde{B}'}}{2},$$

$$\mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^-\right\rangle\left\langle\Psi^+\right|\right) = \mathcal{E}_{Q_n^*,\mathcal{R}_n}\left(\left|\Psi^+\right\rangle\left\langle\Psi^-\right|\right) = \frac{\sigma_z^{\tilde{B}'}}{2},$$

which one can verify after some work is equal to the action of Tr_{E_2} on the Bell basis. ■

5.3 No Post-Selection by Alice

We now consider the case of Bob post-selecting on a repetition code, as before, but Alice not post-selecting. The corresponding filtered states are $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$, and in this section we use the special map (3.9) to prove Conjecture 1 for repetition codes, that is, the following theorem.

Theorem 5.3

$Q^*_{\mathcal{B}_n,\mathcal{R}_n} = Q^*_{\mathcal{R}_n}$ for all $n \geq 1$. Therefore, $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$ is symmetrically extendable for all $\frac{5-\sqrt{5}}{10} \leq Q \leq \frac{1}{3}$ for all $n \geq 1$.

We know already from Proposition 4.1 that if $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$ is symmetrically extendable, then so is $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$, which implies that $Q^*_{\mathcal{B}_n,\mathcal{R}_n} \geq Q^*_{\mathcal{R}_n}$. We will now show that $Q^*_{\mathcal{B}_n,\mathcal{R}_n} \leq Q^*_{\mathcal{R}_n}$ also holds, that is, if $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ is symmetrically extendable, then so is $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$.

Since the repetition codes are linear, the states $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$ are a special case of the states $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ corresponding to no post-selection by Alice and post-selection by Bob on a linear code $\mathcal{Q}$, which are analysed in §E.2 of Appendix E. In that section, we have a general expression (E.19) for the eigenvalues of the Choi representation of $\mathcal{N}$ corresponding to the special map, and we apply those formulas to the repetition codes in §E.2.1. From the analysis in §E.2.1, we obtain the following results about the eigenvalues $\{\Lambda_{u,v} : 0 \leq u \leq 2^n - 1,\ 0 \leq v \leq 1\}$ of $J(\mathcal{N})$ for $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$:

1. The eigenvalues $\Lambda_{0,0}, \Lambda_{0,1}, \Lambda_{2^n-1,0}, \Lambda_{2^n-1,1}$ are equal to the eigenvalues $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$ of $J(\mathcal{N})$ for $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ from (5.8).

2. The remaining eigenvalues $\{\Lambda_{u,0}, \Lambda_{u,1} : 1 \leq u \leq 2^n - 2\}$ are equal to

$$\Lambda_{u,0} = \Lambda_{u,1} = \frac{Q^{|P_u|}(1-Q)^{n-|P_u|}}{Q^{|P_u|}(1-Q)^{n-|P_u|} + Q^{n-|P_u|}(1-Q)^{|P_u|}}, \tag{5.12}$$

   which are non-negative for all $0 \leq Q \leq \frac{1}{2}$ for all $n \geq 1$.

Therefore, from §5.2 above, we have that $\Lambda_{0,0}$ is non-negative for all $0 \leq Q \leq \frac{1}{2}$ for all $n \geq 1$, that $\Lambda_{0,1}$, $\Lambda_{2^n-1,0}$, and $\Lambda_{2^n-1,1}$ vanish at $Q^*_{\mathcal{R}_n}$ for all $n \geq 1$ (and are positive beyond $Q^*_{\mathcal{R}_n}$), and that for $1 \leq u \leq 2^n - 2$ the eigenvalues $\Lambda_{u,0}, \Lambda_{u,1}$ are non-negative for all $0 \leq Q \leq \frac{1}{2}$ for all $n \geq 1$. The map $\mathcal{N}$ is therefore completely-positive for all $Q \geq Q^*_{\mathcal{R}_n}$ for all $n \geq 1$, which means that $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$ is symmetrically extendable whenever $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ is symmetrically extendable. In other words, $Q^*_{\mathcal{B}_n,\mathcal{R}_n} \leq Q^*_{\mathcal{R}_n}$ for all $n \geq 1$. Therefore, $Q^*_{\mathcal{B}_n,\mathcal{R}_n} = Q^*_{\mathcal{R}_n}$ for all $n \geq 1$, as required, which proves Theorem 5.3.

Summary

In this chapter, we have used the framework developed in Chapter 4 to examine repetition codes. We proved the upper bound of $\frac{5-\sqrt{5}}{10}$ that had previously been proven in [Cha02] using entanglement distillation techniques adapted to a classical setting as described in §2.4.4 and proven in [Myh+09] using advantage distillation and symmetric extendability. We subsequently proved Conjecture 2 for repetition codes, which states that the channel constructing a symmetric extension of the filtered states can be decomposed into two channels, the first that alone constructs a symmetric extension at the thresholds $Q^*_{\mathcal{R}_n}$ and the second that constructs a symmetric extension for all QBERs beyond the thresholds. We then proved Conjecture 1 for repetition codes, which states that the thresholds with and without post-selection by Alice are the same.

Chapter 6

Simplex Codes

We now move on to announcement sets $\mathcal{P} = \{P_k\}_{k=0}^{m-1}$ of n-bit strings in which

$$|P_k \oplus P_{k'}| = d \quad \forall\, k \neq k'$$

for some $1 \leq d \leq n$. Such announcement sets are called *simplex codes*, and we will denote them $\mathcal{S}(n, d, m)$, where m is the number of codewords. We may omit the parameters in the specification of the code if they are understood from the context. These codes are a natural generalization of the repetition codes that we just looked at in the previous chapter. Indeed, notice that for all $n \geq 1$, $\mathcal{S}(n, n, 2) = \mathcal{R}_n$. In fact, up to the equivalences described in Chapter 4, the repetition codes are the *only* two-codeword simplex codes.

In this chapter, we will examine the states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ arising from Alice and Bob post-selecting on the same simplex code $\mathcal{S}$. We will derive an analytic expression for the map $\mathcal{N}$ in (3.9) and prove that, just like repetition codes, this map gives a symmetric extension of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ for any simplex code throughout its symmetrically extendable region, and that Tr_{E_2} alone works at the threshold. All of this analysis will be very similar to the analysis for repetition codes, and in fact we will find that simplex codes cannot beat the current best bound obtained from repetition codes.

Since without loss of generality we can always let the first codeword in the announcement set be $\underline{0}^n$, simplex codes of distance d will be such that each non-zero codeword has Hamming weight d. This leads to the following.

Proposition 6.1

For any simplex code $\mathcal{S}(n, d, m)$ such that $m > 2$, d must be even. In particular, $m = 2$ for all d odd.

PROOF: Suppose that $m > 2$. The distinct strings u, v (neither equal to $\underline{0}^n$) in $\mathcal{S}$ each have Hamming weight d by the paragraph above the statement of the proposition and they satisfy $|u \oplus v| = d$ by definition of the code. Now,

$$|u \oplus v| = |u| + |v| - 2|u \odot v|.$$

Letting $y = |u \odot v|$, $|u| = |v| = d = |u \oplus v|$ means that $2d - 2y = d \Rightarrow d = 2y$, that is, d is an even number. It follows that any simplex code of odd constant distance d must have size two. ■

In other words, simplex codes with more than two codewords can only have even distances, and odd-distance simplex codes can only have two codewords. Odd-distance simplex codes are therefore always repetition codes.

Simplex codes can be both linear and non-linear. An example of a linear simplex code with parameters $(n, d, m) = (3, 2, 4)$ is

$$\left\{ \begin{array}{c} 000 \\ 101 \\ 011 \\ 110 \end{array} \right\}.$$

An entire family of linear $[2^r - 1, r, 2^{r-1}]$ simplex codes $\mathcal{S}_r := \mathcal{S}(2^r - 1, 2^{r-1}, 2^r)$ (for $r \geq 2$) has generator matrices whose rows are equal to all the non-zero r-bit strings. For example, the code above corresponds to $r = 2$ and has generator matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$, and the code

$$\left\{ \begin{array}{c} 0000000 \\ 1010101 \\ 0110011 \\ 1100110 \\ 0001111 \\ 1011010 \\ 0111100 \\ 1101001 \end{array} \right\}$$

corresponding to $r = 3$ has generator matrix

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Another way of realizing these codes is as the rows of the rth-order Hadamard matrices $\tilde{H}^{\otimes r}$ with the 1 entries replaced by zeros, the -1 entries replaced by ones, and the first column omitted, where the *Hadamard matrix* $\tilde{H}$ is defined as

$$\tilde{H} := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{6.1}$$

So the $r = 2$ linear simplex code above is realized as

$$\tilde{H}^{\otimes 2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

and the $r = 3$ linear simplex code is realized as

$$\tilde{H}^{\otimes 3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Examples of non-linear simplex codes are

$$\left\{ \begin{matrix} 000, \\ 011, \\ 101 \end{matrix} \right\}, \quad \left\{ \begin{matrix} 0000, \\ 0011, \\ 0101, \\ 1001 \end{matrix} \right\}, \quad \text{and} \quad \left\{ \begin{matrix} 00000, \\ 00011, \\ 00101, \\ 01001, \\ 10001 \end{matrix} \right\}. \tag{6.2}$$

Each of these is a simplex code with constant distance two and is a member of the class $\mathcal{S}(n, 2, n)$ of codes ($n \geq 2$) with codewords

$$P_k = \underbrace{00\cdots00}_{\substack{n-k-1 \\ \text{times}}} 1 \underbrace{00\cdots00}_{\substack{k-1 \\ \text{times}}} 1, \quad k \neq 0. \tag{6.3}$$

(The codes displayed above are for $n = 3, 4, 5$.) More generally, for any code $\mathcal{S}(n, d, m)$, we can obtain codes with higher distances while keeping the number of codewords constant by pasting the code side-by-side with itself k times using Levenshtein's construction, giving codes $k\mathcal{S}(n, d, m) = \mathcal{S}(kn, kd, m)$ for all $n \geq 2$, $2 \leq m \leq n$, and $k \geq 1$. For example, for any $r \geq 2$ and $k > 1$, the codes $k\mathcal{S}_r$ are linear simplex codes that are not in the $\mathcal{S}_r$ class (that is, for any $k > 1$, $k\mathcal{S}_r$ is not equal to $\mathcal{S}_{r'}$ for some r').

6.1 Eigenvalues of the Filtered States

In this section, we provide analytic expressions for the eigenvalues of the states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ arising from post-selection by Alice and Bob on any simplex code $\mathcal{S}$.

First, consider the *discrete Weyl operators* $\{W_{a,b}\}_{a,b=0}^{m-1} \subseteq \mathrm{L}(\mathbb{C}^m)$ defined as [Wat16]

$$W_{a,b} = X(a)Z(b), \quad X(a) = \sum_{k=0}^{m-1} |k+a\rangle\langle k|, \quad Z(b) = \sum_{k=0}^{m-1} e^{\frac{2\pi i k b}{m}} |k\rangle\langle k|, \tag{6.4}$$

where the addition in X is modulo m. These operators are the generalizations to m dimensions of the Pauli operators (2.19) on qubits that we saw in Chapter 2. Using them, we define the m-dimensional generalizations of the qubit Bell states (2.22) as

$$|\Phi_{a,b}\rangle = (\mathbb{1}_{\mathbb{C}^m} \otimes X(a)Z(b)) |\Phi_{0,0}\rangle \quad \forall\, 0 \leq a, b \leq m-1, \tag{6.5}$$

where

$$|\Phi_{0,0}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k,k\rangle. \tag{6.6}$$

Like the qubit Bell states, these states form an orthonormal basis for $\mathbb{C}^m \otimes \mathbb{C}^m$.

In Proposition D.1 of Appendix D, we prove that the spectral decomposition of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is

$$\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}} = \sum_{a,b=0}^{m-1} \lambda_{a,b} \left|\Phi_{a,b}\right\rangle \left\langle\Phi_{a,b}\right|,$$

where the eigenvalues $\{\lambda_{a,b}\}_{a,b=0}^{m-1}$ are

$$\begin{aligned} \lambda_{0,0} &= \left(\frac{1-Q}{2}\right)^n + (m-1)\left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \\ \lambda_{0,1} = \lambda_{0,2} = \cdots = \lambda_{0,m-1} &= \left(\frac{1-Q}{2}\right)^n - \left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \\ \lambda_{1,0} = \lambda_{1,1} = \cdots = \lambda_{m-1,m-1} &= \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}, \end{aligned} \tag{6.7}$$

which can be written compactly as

$$\lambda_{a,b} = \left((\lambda_{0,0} - \lambda_{0,1})\delta_{b,0} + \lambda_{0,1} - \lambda_{1,0}\right)\delta_{a,0} + \lambda_{1,0}. \tag{6.8}$$

It holds that

$$\lambda_{0,0} \geq \lambda_{0,1} \geq \lambda_{1,0} \quad \forall\, 0 \leq Q \leq \frac{1}{2}, \quad \forall\, n, d \geq 1, \quad \forall\, m \geq 2. \tag{6.9}$$

The fact that $\lambda_{0,0} \geq \lambda_{0,1}$ is easy to see since $\lambda_{0,0} = \lambda_{0,1} + m\left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}$. To show that $\lambda_{0,1} \geq \lambda_{1,0}$, we use the inequality

$$(x+y)^n \geq x^n + y^n,$$

which holds for all $x, y \geq 0$ and $n \in \mathbb{N}$. From this, we obtain

$$(Q + 1 - 2Q)^d = (1-Q)^d \geq Q^d + (1-2Q)^d \Rightarrow 1 - \left(\frac{1-2Q}{1-Q}\right)^d \geq \left(\frac{Q}{1-Q}\right)^d.$$

Multiplying both sides by $\left(\frac{1-Q}{2}\right)^n$ gives

$$\underbrace{\left(\frac{1-Q}{2}\right)^n - \left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}}_{\lambda_{0,1}} \geq \underbrace{\left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}}_{\lambda_{1,0}},$$

which is our sought-after inequality.

To determine the separability of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$, we can *try* to use the PPT criterion by calculating $\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)^{\mathsf{T}_{\tilde{B}}}$ and determining when, if any, of its eigenvalues are negative. This is due to the fact that the PPT criterion is only necessary, not sufficient, for the separability of density operators on higher-dimensional spaces. This means that positivity of the eigenvalues of the partial transpose will give no indication as to the separability/entanglement of the state, while *negativity* of the eigenvalues of the partial transpose indicates that the state is entangled. Fortunately, as we prove in Proposition D.2, the partial transpose of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ has a negative eigenvalue, and it does so for $Q \leq \frac{1}{3}$ for all $\mathcal{S}$. Therefore, as with the repetition codes, we have that the separability of the filtered states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is unchanged from that of the original isotropic states ρ_Q^{AB}. This means that the symmetric extendability thresholds $Q_{\mathcal{S}}^*$ must satisfy $Q_{\mathcal{S}}^* \leq \frac{1}{3}$ for any simplex code $\mathcal{S}$.

6.1.1 The Corresponding Channels

Just as we saw in §2.2.1 that the Pauli channels (2.18) had Kraus operators proportional to the Pauli operators and Choi representation proportional to qubit Bell-diagonal states, the discrete Weyl operators (6.4) on $\mathbb{C}^m$ can be used to define a class of channels whose Choi representations are proportional to the m-dimensional Bell-diagonal states. These channels are of the form

$$\mathrm{Y}_{\vec{p}}(X) = \sum_{a,b=0}^{m-1} p_{a,b} W_{a,b} X W_{a,b}^\dagger \quad \forall\, X \in \mathrm{L}(\mathbb{C}^m), \tag{6.10}$$

where $\{p_{a,b}\}_{a,b=0}^{m-1}$ is a probability distribution. The Choi representation is then

$$J(\mathrm{Y}_{\vec{p}}) = m \sum_{a,b=0}^{m-1} p_{a,b} \left|\Phi_{a,b}\right\rangle \left\langle \Phi_{a,b}\right|. \tag{6.11}$$

Now, we have just seen that the states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ are Bell-diagonal. After normalizing, we have that $\mathrm{Tr}_{\tilde{B}}\left[\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right] = \frac{\mathbb{1}_{\tilde{A}}}{m}$, so that the states (after normalization) correspond to quantum channels. The states also have three distinct eigenvalues. Substituting the eigenvalues into (6.10), we obtain the channel $\Phi_{Q,\mathcal{S}} \in \mathrm{C}(\mathfrak{H}_{\tilde{A}}, \mathfrak{H}_{\tilde{B}})$ corresponding to $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$:

$$\Phi_{Q,\mathcal{S}}(X) = (\lambda_{0,0} - \lambda_{0,1})X + m^2 \lambda_{1,0} \Delta(X) + m(\lambda_{0,1} - \lambda_{1,0})\Omega(X) \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_{\tilde{A}}), \tag{6.12}$$

where Δ is the completely-depolarizing channel and Ω is the completely-dephasing channel, which are defined as [Wat16]

$$\Delta(X) = \frac{\mathrm{Tr}(X)}{m} \mathbb{1}_{\tilde{B}} = \frac{1}{m^2} \sum_{a,b=0}^{m-1} W_{a,b} X W_{a,b}^\dagger \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_{\tilde{A}})$$

and

$$\Omega(X) = \sum_{a=0}^{m-1} X_a^a \left|a\right\rangle \left\langle a\right| = \frac{1}{m} \sum_{c=0}^{m-1} W_{0,c} X W_{0,c}^\dagger \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_{\tilde{A}}).$$

6.2 Symmetric Extendability of the Filtered States

In this section, we use the result in [Ran09] to determine the thresholds $Q_{n,d,m}^* \equiv Q_{\mathcal{S}(n,d,m)}^*$ beyond which the filtered states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ are symmetrically extendable.

The result in [Ran09] pertains to a particular subclass of the Bell-diagonal states in $\mathrm{D}(\mathbb{C}^m \otimes \mathbb{C}^m)$, namely, those that are "U_2-invariant", where the set U_2 is defined as

$$\mathrm{U}_2 = \{U \otimes \overline{U} : U \in \mathrm{U}_1\},$$
$$\mathrm{U}_1 = \{U \in \mathrm{U}(\mathbb{C}^m) : U \text{ diagonal in the standard basis}\}.$$

As shown in that work, m-dimensional Bell-diagonal states that are U_2-invariant have only three distinct eigenvalues. In particular,

$$\rho = \sum_{k,\ell=0}^{m-1} x_{k,\ell} \left|\Phi_{k,\ell}\right\rangle \left\langle \Phi_{k,\ell}\right|$$

is U_2-invariant if and only if

$$x_{k,\ell} = \begin{cases} a & \text{if } k = \ell = 0, \\ b & \text{if } k \neq \ell = 0, \\ \frac{1-a-(m-1)b}{m(m-1)} & \text{otherwise} \end{cases} \tag{6.13}$$

for some $a, b \geq 0$, $a \geq b$ such that $x := a + (m-1)b \leq 1$. For all $m \geq 2$, such states are symmetrically extendable if and only if

$$a - b \leq 2\sqrt{\frac{(1-x)(2x-1)}{m-1}} + \frac{m-2}{m-1}(1-x). \tag{6.14}$$

Now, comparing the eigenvalues (6.13) of U_2-invariant states with the eigenvalues (6.7) of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ from the previous section, we find that after normalization they have exactly the same form as (6.13). This means that the states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ are U_2-invariant, which means that (6.14) can be used to determine their symmetric extendability. Before using (6.14), however, the eigenvalues of the state must be normalized. Using as in Chapter 5

$$q_0 = \left(\frac{Q}{2}\right)^d, \quad q_1 = \left(\frac{1-Q}{2}\right)^d, \quad q_2 = \left(\frac{1-2Q}{2}\right)^d,$$

and using the fact that

$$\mathrm{Tr}[\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}] = \lambda_{0,0} + (m-1)\lambda_{0,1} + m(m-1)\lambda_{1,0} = m\left(\frac{1-Q}{2}\right)^n + m(m-1)\left(\frac{Q}{2}\right)^d\left(\frac{1-Q}{2}\right)^{n-d},$$

we get that the normalized eigenvalues $\hat{\lambda}_{0,0} = \frac{\lambda_{0,0}}{\mathrm{Tr}[\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}]}$, $\hat{\lambda}_{0,1} = \frac{\lambda_{0,1}}{\mathrm{Tr}[\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}]}$ and $\hat{\lambda}_{1,0} = \frac{\lambda_{1,0}}{\mathrm{Tr}[\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}]}$ are

$$\hat{\lambda}_{0,0} = \frac{q_1 + (m-1)q_2}{mq_1 + m(m-1)q_0}, \quad \hat{\lambda}_{0,1} = \frac{q_1 - q_2}{mq_1 + m(m-1)q_0}, \quad \hat{\lambda}_{1,0} = \frac{q_0}{mq_1 + m(m-1)q_0}.$$

Additionally, using $x = 1 - m(m-1)\hat{\lambda}_{1,0}$, substitution into (6.14) gives us

$$m\frac{q_2}{X} - m(m-2)\frac{q_0}{X} \leq 2\sqrt{m\left(\frac{q_0}{X}\right)\left(1 - 2m(m-1)\left(\frac{q_0}{X}\right)\right)}$$

as the necessary and sufficient condition for the symmetric extendability of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$, where $X \equiv mq_1 + m(m-1)q_0$. After much simplification, this becomes

$$q_2^2 - 2(m-2)q_0q_2 - 4q_0q_1 + m^2q_0^2 \leq 0. \tag{6.15}$$

As a check, we may let $m = 2$ and $d = n$, so that the corresponding code is just the repetition code $\mathcal{R}_n$ examined in the previous chapter. This gives us $q_2^2 - 4q_0q_1 + 4q_0^2 \leq 0$, which is exactly the condition (5.4), as expected.

Now, substituting the definitions of q_0, q_1, q_2 into (6.15) gives us

$$g_{d,m}(Q) := (1-2Q)^{2d} - 2(m-2)Q^d(1-2Q)^d - 4Q^d(1-Q)^d + m^2Q^{2d} \leq 0. \tag{6.16}$$

The root(s) of $g_{d,m}$ gives us the threshold $Q_{n,d,m}^*$ beyond which $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is symmetrically extendable. Notice that this function depends only on the parameters d and m of the code and not on the block length n. This is a reflection of Proposition 4.4, which we recall tells us that adding extra zeros to codewords does nothing to the

symmetric extendability of the resulting state. It also tells us that, for example, the codes $\mathcal{S}(4,2,4) = \left\{ \begin{array}{c} 0000 \\ 0011 \\ 0101 \\ 1001 \end{array} \right\}$ (which is non-linear) and $\mathcal{S}(3,2,4) = \left\{ \begin{array}{c} 000 \\ 011 \\ 101 \\ 110 \end{array} \right\}$ (which is linear) have the *same* threshold.

Now, let us consider the linear simplex codes $\mathcal{S}_r$ described at the beginning of this chapter. Figure 6.1 below plots the thresholds for some of these codes. As with the repetition codes, the threshold increases monotonically with the distance (which, recall, is $d = 2^{r-1}$ for these codes) and appears to converge to $\frac{5-\sqrt{5}}{10}$.

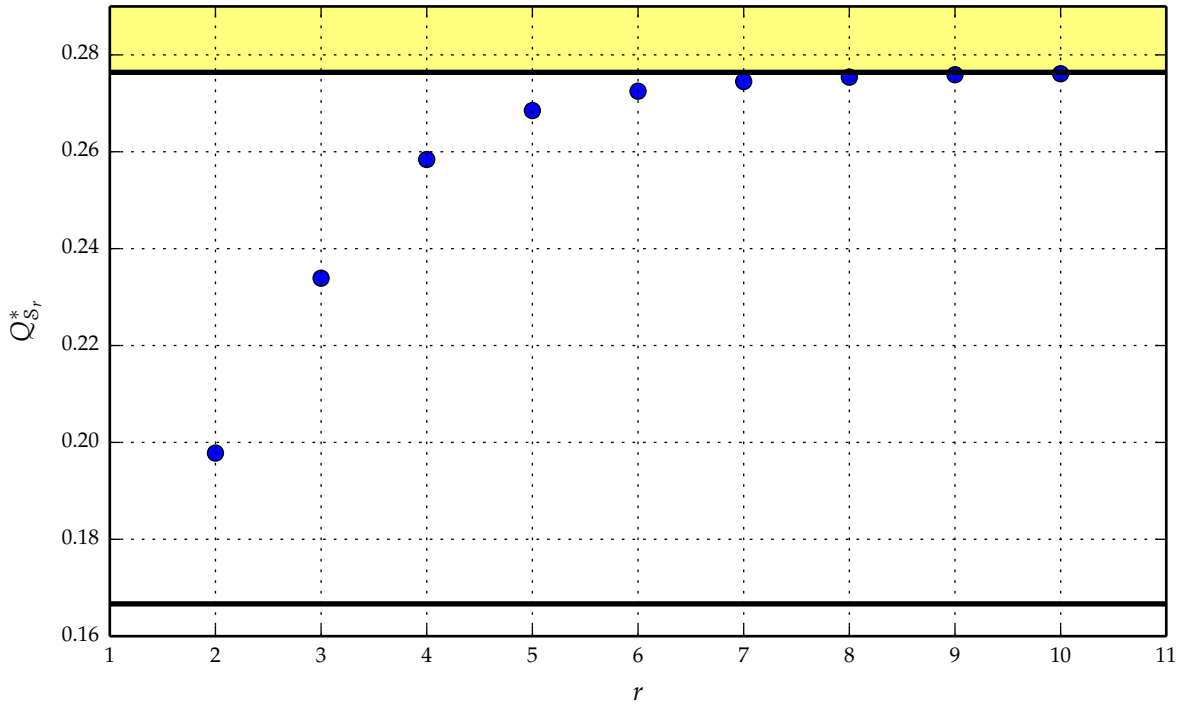


Figure 6.1: Thresholds for the simplex codes $\mathcal{S}_r$ up to $r = 10$. The region highlighted in yellow is the gap.

We can also consider the class of simplex codes $\mathcal{S}(mk, 2k, m)$ corresponding to Levenstein's constructions of the codes $\mathcal{S}(m, 2, m)$ defined in (6.3). Table 6.1 below contains the thresholds for some of these codes. For $m > 2$ and $k \geq 1$, all of these codes are non-linear. Note that for $m = 2$, $\mathcal{S}(2k, 2k, 2) = \mathcal{R}_{2k}$, that is, $m = 2$ simply gives us the even-order repetition codes.

m \ k	1	2	3	4	5	6	7	8	9
2	0.215080	0.244721	0.255315	0.260645	0.263831	0.265946	0.267452	0.268578	0.269453
3	0.205719	0.242574	0.254725	0.260470	0.263777	0.265929	0.267446	0.268577	0.269452
4	0.197825	0.240594	0.254155	0.260299	0.263723	0.265912	0.267441	0.268575	0.269452
5	0.191015	0.238757	0.253605	0.260129	0.263670	0.265894	0.267435	0.268573	0.269451
6	0.185041	0.237041	0.253072	0.259963	0.263617	0.265877	0.267429	0.268571	0.269450
7	0.179728	0.235432	0.252555	0.259798	0.263565	0.265860	0.267424	0.268569	0.269450
8	0.174952	0.233916	0.252054	0.259635	0.263512	0.265843	0.267418	0.268567	0.269449
9	0.170622	0.232483	0.251568	0.259475	0.263460	0.265826	0.267413	0.268565	0.269449
10	0.166667	0.231125	0.251095	0.259317	0.263409	0.265810	0.267407	0.268563	0.269448

Table 6.1: Thresholds for the simplex codes $\mathcal{S}(mk, 2k, m)$.

Noting that k parametrizes the distance of the code, we see that for each distance the repetition code (corresponding to the first row of the table) always has the highest threshold and that increasing the number of codewords decreases the threshold. Not only that, but as the distance increases the thresholds of $m > 2$ non-repetition codes appear to converge to the threshold of the repetition code. This convergence is clearer from Figure 6.2 below, in which the repetition code thresholds are indicated in black.

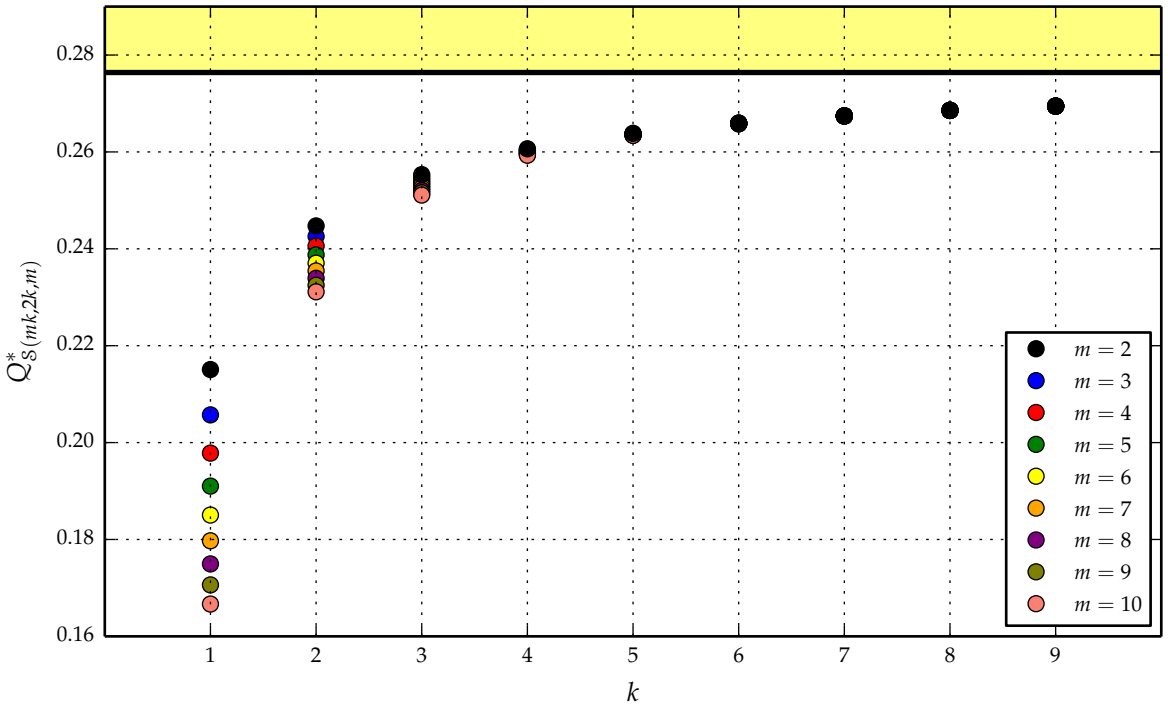


Figure 6.2: Thresholds for the simplex codes $\mathcal{S}(mk, 2k, m)$ from Table 6.1. The region highlighed in yellow is the gap.

Indeed, from (6.16) we see that for any simplex code, the contribution to $g_{d,m}$ from the m-dependent terms $2(m-2)Q^d(1-2Q)^d$ and m^2Q^{2d} diminishes compared to the other terms as the distance d increases. That is,

for any simplex code, by keeping m fixed and increasing d using Levenstein's construction, it holds that

1. $m^2Q^{2d} \leq (1-2Q)^{2d}$ for all $Q \leq \frac{1}{2+(m^2)^{\frac{1}{d}}}$;
2. $m^2Q^{2d} \leq 4Q^d(1-Q)^d$ for all $Q \leq \frac{1}{1+\left(\frac{m^2}{4}\right)^{\frac{1}{d}}}$;
3. $2(m-2)Q^d(1-2Q)^d \leq (1-2Q)^{2d}$ for all $Q \leq \frac{1}{2+(2(m-2))^{\frac{1}{d}}}$; and
4. $2(m-2)Q^d(1-2Q)^d \leq 4Q^d(1-Q)^d$ for all $Q \geq \frac{\left(\frac{m-2}{2}\right)^{\frac{1}{d}}-1}{2\left(\frac{m-2}{2}\right)^{\frac{1}{d}}-1}$.

This means that as d increases, $g_{d,m}$ tends to $(1-2Q)^{2d} - 4Q^d(1-Q)^d = \tilde{f}_d(Q)$, where we recall the function $\tilde{f}$ from (5.6) in Chapter 5. This means that $\frac{5-\sqrt{5}}{10}$, which is the root of $\tilde{f}_d$ as $d \to \infty$, is the best possible threshold that can be achieved with a simplex code. We have therefore proved the following theorem, which tells us that simplex codes cannot beat repetition codes, that is, simplex codes cannot break symmetric extendability in the gap.

Theorem 6.2

For any simplex code $\mathcal{S}$, $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{S}}$ is symmetrically extendable for all $\frac{5-\sqrt{5}}{10} \leq Q \leq \frac{1}{3}$.

Now, we have already seen in Table 6.1 and Figure 6.2 the trend that the simplex codes $\mathcal{S}(mk, 2k, m)$ with $m > 2$ of distance $2k$ cannot beat the repetition codes $\mathcal{R}_{2k} = \mathcal{S}(2k, 2k, 2)$ with the same distance. The same data reveal that increasing the number of codewords while keeping the distance constant has the effect of decreasing the threshold. We examine this effect more closely in Figure 6.3 by plotting the thresholds for $\mathcal{S}(mk, 2k, m)$ as a function of m instead of k.

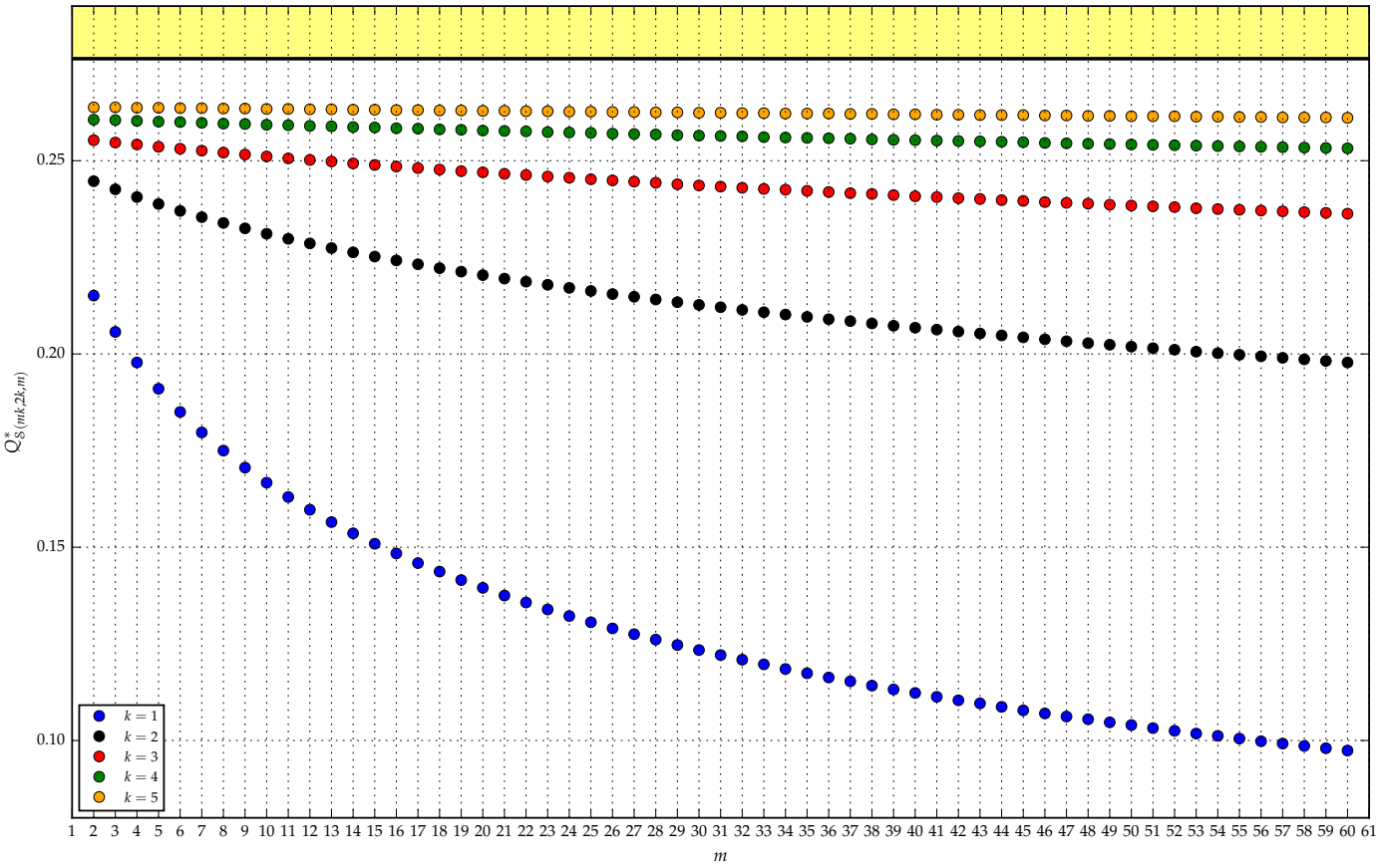


Figure 6.3: Thresholds for the simplex codes $\mathcal{S}(mk, 2k, m)$ as a function of the number of codewords m.

6.3 The Special Construction of a Symmetric Extension

We now show that the special map $\mathcal{N} \circ \mathrm{Tr}_{E_2}$ of §3.3.1 is optimal for simplex codes; that is, like repetition codes, the special map constructs a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{S}}$ for all simplex codes $\mathcal{S}$ throughout their symmetrically extendable regions. Furthermore, we show that the channel Tr_{E_2} alone constructs a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{S}}$ at the threshold $Q^*_{\mathcal{S}}$.

By using formula (3.11) for $J(\mathcal{N})$, we find that

$$J(\mathcal{N}) = \sum_{u',v'=0}^{m-1} \Lambda_{u',v'} \left|\Phi_{u',v'}\right\rangle \left\langle\Phi_{u',v'}\right|,$$

where the eigenvalues $\{\Lambda_{u',v'}\}_{u',v'=0}^{m-1}$ of $J(\mathcal{N})$ for $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{S}}$ are

$$\Lambda_{u',v'} = \frac{1}{m} - \frac{(\lambda_{0,0} + (m-1)\lambda_{0,1} - m\lambda_{1,0})\delta_{u',0} - \frac{1}{m}(\lambda_{0,0} + (m-1)\lambda_{0,1} - m\lambda_{1,0})}{2\sqrt{\lambda_{0,1}\lambda_{0,0}} + (m-2)\lambda_{0,1} + m(m-1)\lambda_{1,0}}$$
$$+ \frac{((\lambda_{0,0} - \lambda_{0,1})(m\delta_{v',0} - 1))\,\delta_{u',0}}{2\sqrt{\lambda_{1,0}\lambda_{0,0}} + 2(m-1)\sqrt{\lambda_{1,0}\lambda_{0,1}} + m(m-2)\lambda_{1,0}} \quad \forall\, 0 \leq u', v' \leq m-1,$$

which means that

$$\Lambda_{0,1} = \Lambda_{0,2} = \cdots = \Lambda_{0,m-1} \quad \text{and} \quad \Lambda_{1,1} = \Lambda_{1,2} = \cdots = \Lambda_{m-1,m-1}.$$

In other words, like the eigenvalues of the filtered states, there are only three distinct eigenvalues of $J(\mathcal{N})$, which are

$$\begin{aligned}\Lambda_{0,0} = \frac{1}{m} &+ \frac{\left(1-\frac{1}{m}\right)\left(\lambda_{0,0} + (m-1)\lambda_{0,1} - m\lambda_{1,0}\right)}{2\sqrt{\lambda_{0,1}\lambda_{0,0}} + (m-2)\lambda_{0,1} + m(m-1)\lambda_{1,0}} \\ &+ \frac{(m-1)(\lambda_{0,0} - \lambda_{0,1})}{2\sqrt{\lambda_{1,0}\lambda_{0,0}} + 2(m-1)\sqrt{\lambda_{1,0}\lambda_{0,1}} + m(m-2)\lambda_{1,0}},\end{aligned} \tag{6.17}$$

$$\begin{aligned}\Lambda_{0,1} = \frac{1}{m} &+ \frac{\left(1-\frac{1}{m}\right)\left(\lambda_{0,0} + (m-1)\lambda_{0,1} - m\lambda_{1,0}\right)}{2\sqrt{\lambda_{0,1}\lambda_{0,0}} + (m-2)\lambda_{0,1} + m(m-1)\lambda_{1,0}} \\ &+ \frac{\lambda_{0,1} - \lambda_{0,0}}{2\sqrt{\lambda_{1,0}\lambda_{0,0}} + 2(m-1)\sqrt{\lambda_{1,0}\lambda_{0,1}} + m(m-2)\lambda_{1,0}},\end{aligned} \tag{6.18}$$

and

$$\Lambda_{1,0} = \frac{1}{m} - \frac{1}{m}\frac{\lambda_{0,0} + (m-1)\lambda_{0,1} - m\lambda_{1,0}}{2\sqrt{\lambda_{0,1}\lambda_{0,0}} + (m-2)\lambda_{0,1} + m(m-1)\lambda_{1,0}}. \tag{6.19}$$

It holds that $\Lambda_{0,0} \geq \Lambda_{0,1}$, since $\lambda_{0,0} \geq \lambda_{0,1}$, and that $\Lambda_{0,0} \geq \Lambda_{1,0}$. Figure 6.4 below contains plots of the eigenvalues for some simplex codes.

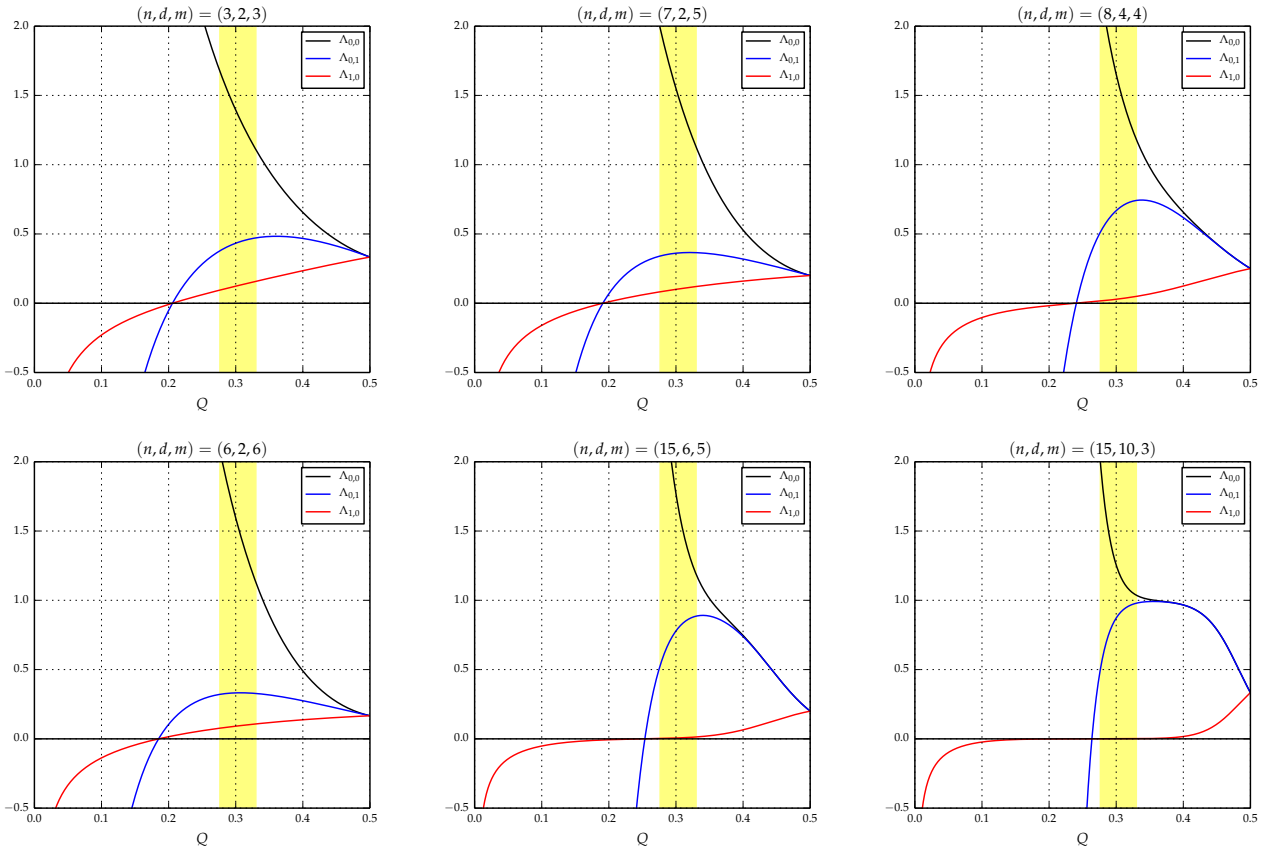


Figure 6.4: The eigenvalues $\Lambda_{0,0}$, $\Lambda_{0,1}$ and $\Lambda_{1,0}$ of $J(\mathcal{N})$ for six simplex codes. The region highlighted in yellow is the gap.

The plots above give the indication that $\Lambda_{0,0}$ is positive for all $0 \leq Q \leq \frac{1}{2}$—hence positive throughout the gap—for all simplex codes, and that $\Lambda_{0,1}$ and $\Lambda_{1,0}$ vanish at the same point in the interval $\left[0, \frac{1}{2}\right]$ for all simplex codes. The former is verified by examining (6.17) directly, while proof of the latter is given in Lemma D.3 of Appendix D.

Now, we require $\mathcal{N}$ to be a channel, which means that it must be completely-positive and trace-preserving. From the expression of $J(\mathcal{N})$ above, we find that $\text{Tr}_{\tilde{B}}[J(\mathcal{N})] = \mathbb{1}_{E_1}$, so that $\mathcal{N}$ is trace-preserving. It remains, therefore, to prove the complete-positivity of $\mathcal{N}$, which requires proving the non-negativity of the eigenvalues $\{\Lambda_{u',v'}\}_{u',v'=0}^{m-1}$ of $J(\mathcal{N})$. Since $\Lambda_{0,0}$ is positive for all $0 \leq Q \leq \frac{1}{2}$, and since by Lemma D.3 $\Lambda_{0,1}$ and $\Lambda_{1,0}$ vanish at the same point, it is sufficient to consider the non-negativity of the eigenvalue $\Lambda_{1,0}$. From the proof of the same lemma, we have that the condition $\Lambda_{1,0} \geq 0$ is equivalent to the condition $\sqrt{\lambda_{0,0}} - \sqrt{\lambda_{0,1}} \leq m\sqrt{\lambda_{1,0}}$. After using the definitions of $\lambda_{0,0}$, $\lambda_{0,1}$, $\lambda_{1,0}$, this condition becomes

$$2^{\frac{d}{2}} m\sqrt{Q^d} + 2^{\frac{d}{2}}\sqrt{(1-Q)^d - (1-2Q)^d} - 2^{\frac{d}{2}}\sqrt{(1-Q)^d + (m-1)(1-2Q)^d} \geq 0. \tag{6.20}$$

If we simplify this further, we obtain the condition

$$(1-2Q)^{2d} - (2m-4)(1-2Q)^d Q^d + m^2 Q^{2d} - 4Q^d(1-Q)^d \leq 0, \tag{6.21}$$

which is exactly the condition (6.16) obtained in the previous section using the necessary and sufficient condition for the symmetric extendability of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$. This means that $\Lambda_{0,1}$ and $\Lambda_{1,0}$ vanish at the thresholds $Q_{n,d,m}^*$ and are positive above it, which means that $\mathcal{N}$ is completely-positive for all $Q \geq Q_{n,d,m}^*$, which means that $\mathcal{N} \circ \text{Tr}_{E_2}$ can be used to construct a symmetric extension of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ throughout its symmetrically extendable region. In particular, at $Q_{n,d,m}^*$, the eigenvalue $\Lambda_{0,0}$ can be shown to be equal to

$$\Lambda_{0,0}^* = \frac{1}{m} + 1 - \frac{1}{m} - 1 + m = m.$$

Therefore,

$$J(\mathcal{N})|_{Q_{n,d,m}^*} = m\,|\Phi_{0,0}\rangle\langle\Phi_{0,0}| \Rightarrow \mathcal{N}(X) = X \quad \forall\, X,$$

that is, $\mathcal{N}$ is merely the identity map at the threshold, which means that Tr_{E_2} alone constructs a symmetric extension of $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ at the threshold, exactly as we observed with the repetition codes in the previous chapter. This proves Conjecture 2 for simplex codes.

Summary

In this chapter, we looked at the filtered states arising from Alice and Bob post-selecting on a simplex code $\mathcal{S}$, which is a generalization of the repetition codes $\mathcal{R}_n$ to more than two codewords in which the pairwise Hamming distance between distinct codewords is a constant. The class of states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ and $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ have essentially the same structure: while $\rho_{Q,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ is diagonal in the two-dimensional Bell basis, $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is diagonal in the m-dimensional Bell basis, where m is the size of the simplex code $\mathcal{S}$. As well, both classes of states have only three distinct eigenvalues, which extends to the eigenvalues of $J(\mathcal{N})$ corresponding to the special map $\mathcal{E} = \mathcal{N} \circ \text{Tr}_{E_2}$. We proved that this special map is optimal for the states $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ in the sense that it can be used to construct a symmetric extension of them throughout their symmetrically extendable regions. Furthermore, we showed that Tr_{E_2} alone constructs a symmetric extension at the thresholds. Most importantly, we proved that there does not exist a simplex code whose threshold is within the gap, proving that simplex codes cannot beat repetition codes, and therefore cannot break symmetric extendability in the gap.

Chapter 7

Testing the Special Map

In this chapter, we test the special map $\mathcal{E} = \mathcal{N} \circ \mathrm{Tr}_{E_2}$ from §3.3.1 to see how often it can construct symmetric extensions of the filtered states resulting from Alice and Bob post-selecting on the same code. We start with the special class of linear codes called first-order Reed-Muller codes and find that the special map is *not* able to construct a symmetric extension for some values in the gap even though the filtered states are symmetrically extendable throughout the gap. We then move on to numerical testing of the special map on around 540,000 randomly-selected codes. We find that all the filtered states are symmetrically extendable throughout the gap but that there were approximtely 1% of the codes for which the special map could not construct a symmetric extension.

7.1 First-Order Reed-Muller Codes

The rth first-order Reed-Muller code $\mathcal{RM}_r$ can be defined as $\mathcal{RM}_r = \mathcal{S}'_r \cup \overline{\mathcal{S}'_r}$, where $\mathcal{S}'_r := \mathcal{S}(2^r, 2^{r-1}, 2^r)$ is the linear simplex code $\mathcal{S}_r$ from Chapter 6 without the first column of zeros removed from the corresponding binary Hadamard matrix[1]. For example, with $r = 2$, we get

$$H^{\otimes 2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

so that

$$\mathcal{S}'_2 = \left\{ \begin{array}{c} 0000 \\ 0101 \\ 0011 \\ 0110 \end{array} \right\} \Rightarrow \mathcal{RM}_2 = \left\{ \begin{array}{c} 0000 \\ 0101 \\ 0011 \\ 0110 \\ 1111 \\ 1010 \\ 1100 \\ 1001 \end{array} \right\}.$$

[1] More generally, Reed-Muller codes are defined in terms of *Boolean functions*, as described in [MS77]. Conveniently, first-order Reed-Muller codes can be defined in the simpler way described here without the Boolean function formalism.

It is straightforward to use (E.10) to determine that the eigenvalues of the filtered state $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_r}$ corresponding to both Alice and Bob post-selecting on $\mathcal{RM}_r$ are

$$\begin{aligned}
\lambda_{0,b} &= \begin{cases} \left(\frac{1-Q}{2}\right)^n + \left(\frac{1-2Q}{2}\right)^n + 2(n\delta_{b,0}-1)\left(\frac{1-2Q}{2}\right)^{\frac{n}{2}}\left(\frac{1-Q}{2}\right)^{\frac{n}{2}}, & 0 \leq b \leq 2^r-1, \\ \left(\frac{1-Q}{2}\right)^n - \left(\frac{1-2Q}{2}\right)^n, & 2^r \leq b \leq 2\cdot 2^r - 1. \end{cases} \\
\lambda_{2^r,b} &= \left(\frac{Q}{2}\right)^n \quad \forall\, 0 \leq b \leq 2\cdot 2^r - 1, \\
\lambda_{a,b} &= \begin{cases} \left(\frac{Q}{2}\right)^{\frac{n}{2}}\left(\frac{1-Q}{2}\right)^{\frac{n}{2}} + (-1)^{\mathrm{Bin}_{r+1}(b)\cdot\mathrm{Bin}_{r+1}(a)}\left(\frac{1-2Q}{2}\right)^{\frac{n}{2}}\left(\frac{Q}{2}\right)^{\frac{n}{2}}, & a \neq 0, 2^r, \quad 0 \leq b \leq 2^r-1, \\ \left(\frac{Q}{2}\right)^{\frac{n}{2}}\left(\frac{1-Q}{2}\right)^{\frac{n}{2}} - (-1)^{\mathrm{Bin}_{r+1}(b)\cdot\mathrm{Bin}_{r+1}(a)}\left(\frac{1-2Q}{2}\right)^{\frac{n}{2}}\left(\frac{Q}{2}\right)^{\frac{n}{2}}, & a \neq 0, 2^r, \quad 2^r \leq b \leq 2\cdot 2^r - 1. \end{cases}
\end{aligned} \tag{7.1}$$

We can then use (E.15) to calculate the eigenvalues of $J(\mathcal{N})$ to see if these states are symmetrically extendable and, if they are symmetrically extendable, whether a symmetric extension can be constructed using our special construction.

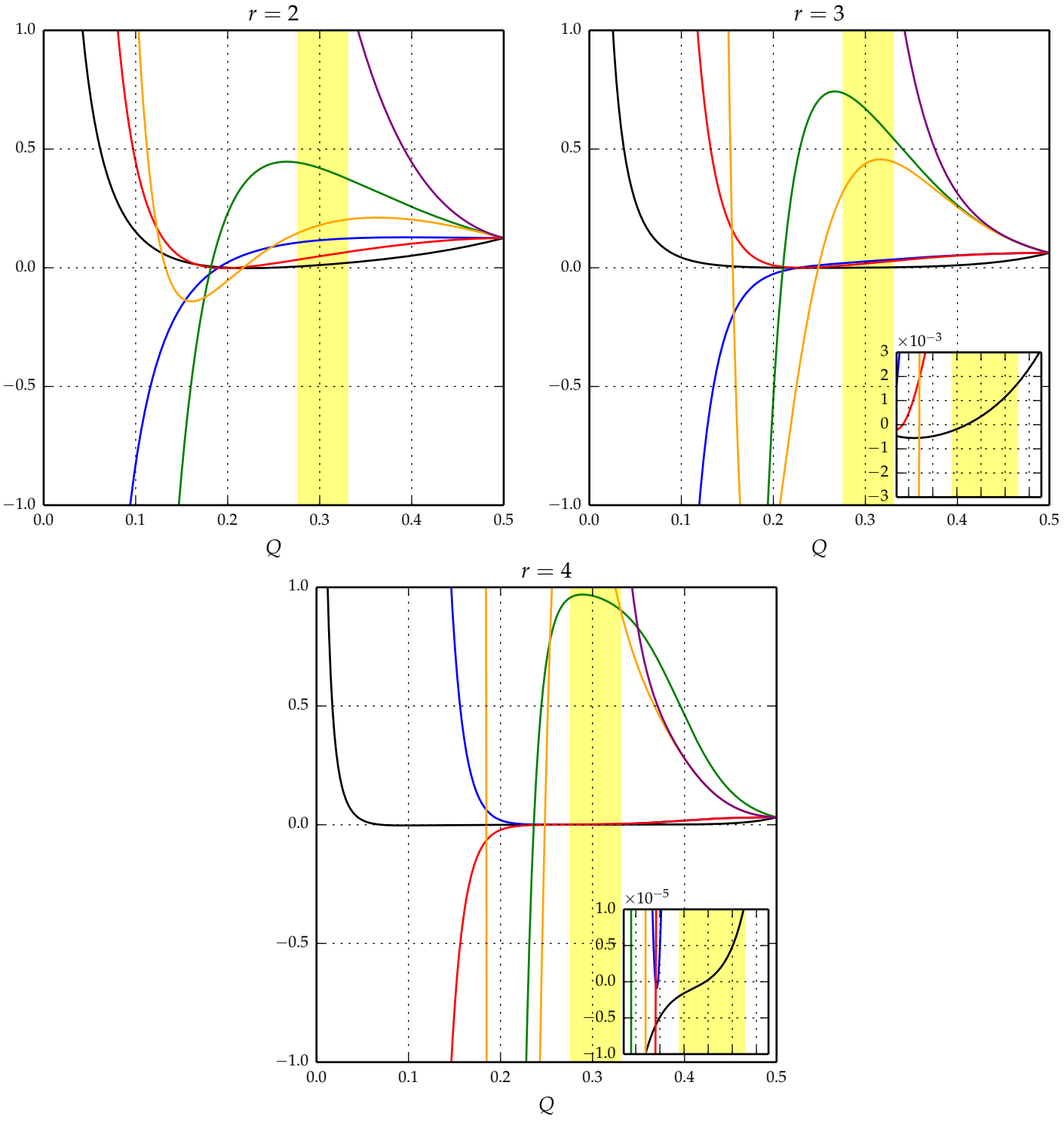


Figure 7.1: Eigenvalues of $J(\mathcal{N})$ for the Reed-Muller codes $\mathcal{RM}_2$, $\mathcal{RM}_3$, and $\mathcal{RM}_4$. The region highlighed in yellow is the gap.

The plots above are of the six distinct eigenvalues of $J(\mathcal{N})$ for the states $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_2}$, $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_3}$, and $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_4}$. Using the SDP (3.3), we have that all of these states are symmetrically extendable throughout the gap. Yet, while the $J(\mathcal{N})$ eigenvalues for $r = 2$ are all positive in the gap, looking closely at the eigenvalues for $r = 3$ and $r = 4$,

we find from looking at the insets that in each of these cases the eigenvalue corresponding to the black line is negative for some values at the lower end of the gap. This means that, though the states $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_3}$ and $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{RM}_4}$ are symmetrically extendable throughout the gap, a symmetric extension cannot be constructed throughout the gap using the special map. This trend of negative eigenvalues for $J(\mathcal{N})$ continues for increasing r. This example tells us that there exist linear codes for which the special map is not able to construct a symmetric extension throughout the gap even when the state is symmetrically extendable.

7.2 Numerical Testing

In this section, we use our special map (3.9) to numerically test the symmetric extendability of filtered states using an estimated 540,000 inequivalent announcement sets for block sizes up to $n = 20$. As mentioned in §3.3, if the second part $\mathcal{N}$ of the map is completely-positive, then the state is symmetrically extendable, which means that the SDP (3.3), which generally takes longer to complete, does not need to be run. The SDP is only run if $\mathcal{N}$ fails to be completely-positive. Table 7.1 below displays the results.

For each (n, m) pair in Table 7.1, if the number of inequivalent announcement sets was known (which was the case for the (n, m) pairs in Table 4.1), then all of them were tested. If not, then 5000 sets, not necessarily distinct, were chosen at random and tested. For each announcement set, we determined the smallest eigenvalue of $J(\mathcal{N})$ for the QBER values of 0.28, 0.29, 0.30, 0.31, 0.32, and 0.33 within the gap. If for each of these QBERs the smallest eigenvalue of $J(\mathcal{N})$ was positive, then $J(\mathcal{N})$ was positive-semidefinite and the corresponding filtered state was symmetrically extendable at that QBER; if not, then the SDP (3.3) was run using `yalmip` [Lof04] on `MATLAB` with the solver `SCS` [ODo+16].

Determining whether two announcement sets are equivalent (as per the equivalences determined in §4.4) is very similar to the process of determining the number of inequivalent announcement sets for a given (n, m) pair. As such, determining the equivalence of two announcement sets becomes very time-consuming, especially for larger block sizes. Therefore, to determine for each (n, m) class not in Table 4.1 how many of the 5000 randomly-selected sets were inequivalent, we used the fact that equivalent announcement sets would give the same set of eigenvalues of $J(\mathcal{N})$, in particular the same smallest eigenvalue. This fact allowed us to determine (up to numerical precision) how many of the 5000 sets selected were inequivalent (indicated in the "tested" columns of Table 7.1 below), which means that the number of inequivalent sets actually tested could be lower than the number shown. The "failed" columns indicate the number of announcement sets tested for which the smallest eigevalue of $J(\mathcal{N})$ was negative for at least one of the tested QBER values. In all cases, including those announcement sets in the failed columns, we found the corresponding filtered states were symmetrically extendable for all six values of the QBER tested within the gap.

Numerical results for inequivalent linear codes up to block length 9 and size 16 were obtained by Myhr in [Myh10] by solving the SDP (3.3). The results here include linear and non-linear codes of higher block lengths.

n \ m	3		4		5		6		7		8		9		10		11		12		13		14	
	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed	Tested	Failed
3	2	0	5	0	3	0	3	0	1	0														
4	3	0	13	0	24	0	47	0	55	0	73	0	56	0	50	0	27	2	19	3	6	2	4	1
5	4	0	28	0	104	0	4302	0	4723	0	4677	0	4337	0	3735	2								
6	6	0	1412	0	4078	0	4895	0	4975	0	4979	0	4957	1	4881	12								
7	7	0	2097	0	4579	0	4975	0	4997	0	5000	0	4998	0	4995	9								
8	9	0	2529	0	4779	0	4991	0	4999	0	5000	0	5000	4	5000	2	5000	6	5000	3	5000	13		
9	289	0	2877	0	4871	0	4996	0	5000	0	5000	0	5000	0	5000	0								
10	341	0	3201	0	4899	0	4996	0	5000	0	5000	0	5000	0	5000	3	5000	11						
11	325	0	3143	0	4861	0	4995	0	5000	0	5000	0	5000	0	5000	5								
12	327	0	3143	0	4871	0	4997	0	5000	0	5000	0	5000	0	5000	7								
13	297	0	3008	0	4835	0	4993	0	5000	0	5000	0	5000	0	5000	11								
14	268	0	2864	0	4778	0	4981	0	5000	0	5000	0	5000	3	5000	6								
15	254	0	2704	0	4724	0	4984	0	5000	0	5000	0	5000	0	5000	10								
16	201	0	2489	0	4653	0	4980	0	4999	0	5000	0	5000	0	5000	2								
17	204	0	2364	0	4543	0	4981	0	5000	0	5000	0	5000	0	5000	1								
18	130	0	2177	0	4471	0	4971	0	5000	0	5000	0	5000	0	5000	1								
19	100	0	1913	0	4359	0	4964	0	5000	0	5000	0	5000	0	5000	1								
20	74	0	1758	0	4280	0	4948	0	4998	0	5000	0	5000	0	5000	1	5000	1	5000	1	5000	1	5000	3

Table 7.1: Results of the numerical testing of the special construction for various (n, m) pairs. Blank cells were untested.

The exact total number of (estimated) inequivalent sets tested was 548,818. The total number of failed sets was 128, which amounts to a failure percentage of approximately 0.2%. Most of these sets failed only at $Q = 0.28$ and worked for all of the other five QBERs tested. We keep in mind that the actual total number of inequivalent sets tested might be less since equivalence of sets was determined using equality of the smallest eigenvalue of $J(\mathcal{N})$, which is accurate only up to numerical precision.

Chapter 8

Numerical Estimation of Thresholds

As described in §4.3.1, for a given pair of announcement sets $\mathcal{P}, \mathcal{Q}$, we can numerically search for the symmetric extendability threshold $Q^*_{\mathcal{P},\mathcal{Q}}$ corresponding to the one-parameter family $\{\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{P},\mathcal{Q})}\}_{Q\in\left[0,\frac{1}{2}\right]}$ of states. In this chapter, we go through the results of this numerical estimation for all the inequivalent announcement sets in Table 4.1 for the case of Alice and Bob performing the same post-selection.

The search for the thresholds was done as follows: for each announcement set $\mathcal{P}$, we selected 200 points in the interval $[0.16, 0.33]$ and found the SDP solution $t_{\text{opt}}(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}})$ for each of these points, giving us an estimate of the function $T_{(\mathcal{P},\mathcal{Q})}$ (defined in (4.18)) in the interval. By finding the curve of best fit to these points, we estimated the point at which the curve changed sign, which by definition is the threshold. The results are tabulated below and analyzed in §8.1.

(n,m)	Q^*															$Q^*_{\max}$
$(2,2)$	0.2151															0.2151
$(2,3)$	0.1824															0.1824
$(3,2)$	0.2344															0.2344
$(3,3)$	0.2057	0.2121														0.2121
$(3,4)$	0.2151	0.1978	0.1765	0.1949	0.2025											0.2151
$(3,5)$	0.2075	0.1955	0.1815													0.2075
$(3,6)$	0.1845	0.1824	0.2008													0.2008
$(3,7)$	0.1788															0.1788
$(4,2)$	0.2447															0.2447
$(4,3)$	0.2267	0.2281	0.2307													0.2307
$(4,4)$	0.2153	0.2344	0.2224	0.2154	0.1978	0.2073	0.2133	0.2209	0.2236	0.2230	0.2090	0.2144	0.2257			0.2344
$(4,5)$	0.2126	0.2164	0.2070	0.2287	0.2059	0.2068	0.2178	0.2195	0.2186	0.1713	0.2138	0.2034	0.1923	0.2044	0.1961	0.2287
	0.2026	0.2129	0.2028	0.2051	0.2036	0.2155	0.2179	0.2212	0.2078							
$(4,6)$	0.1971	0.2057	0.2011	0.2236	0.2162	0.2023	0.2120	0.2121	0.2121	0.2024	0.2151	0.2117	0.2000	0.2088	0.2042	0.2236
	0.2038	0.2102	0.1983	0.2042	0.2084	0.2109	0.2009	0.2235	0.2235	0.2128	0.2107	0.2107	0.2129	0.2129	0.2118	
	0.2146	0.2172	0.1792	0.1952	0.2057	0.1882	0.2064	0.1954	0.1989	0.2046	0.1963	0.2008	0.1952	0.2057	0.2022	
	0.2010	0.2130														
$(4,7)$	0.1993	0.2079	0.1892	0.1975	0.2050	0.1949	0.2133	0.1984	0.2190	0.2100	0.2099	0.2140	0.2081	0.2087	0.2082	0.2190
	0.2081	0.2081	0.2086	0.2069	0.1984	0.2047	0.2009	0.2006	0.2040	0.2131	0.2047	0.2098	0.2047	0.1999	0.1971	
	0.1971	0.2025	0.2023	0.2014	0.2058	0.2009	0.2040	0.1984	0.1973	0.2189	0.2084	0.2064	0.2084	0.2084	0.2103	
	0.1813	0.1999	0.1901	0.1900	0.1990	0.1914	0.1949	0.1986								
$(4,8)$	0.2151	0.1978	0.1903	0.1983	0.2030	0.2030	0.1970	0.1765	0.1949	0.1949	0.1841	0.2045	0.2034	0.2042	0.2005	0.2151
	0.2041	0.2123	0.1970	0.2025	0.2116	0.2072	0.2033	0.1987	0.1923	0.2072	0.1964	0.2015	0.1923	0.2015	0.2063	
	0.2012	0.2046	0.2062	0.2066	0.2047	0.2069	0.2094	0.2045	0.2045	0.2045	0.2064	0.2045	0.2015	0.2008	0.1955	
	0.1954	0.1963	0.1996	0.2031	0.1978	0.1958	0.2015	0.2062	0.2111	0.2062	0.1978	0.1984	0.2030	0.1902	0.1954	
	0.1952	0.1987	0.1951	0.2148	0.2148	0.2148	0.2025	0.2044	0.2044	0.1781	0.1825	0.1866	0.1909			
$(5,2)$	0.2511															0.2511
$(5,3)$	0.2384	0.2365	0.2401	0.2416												0.2416
$(5,4)$	0.2344	0.2447	0.2331	0.2358	0.2281	0.2224	0.2253	0.2262	0.2254	0.2299	0.2309	0.2339	0.2361	0.2331	0.2345	0.2447
	0.2225	0.2258	0.2235	0.2269	0.2230	0.2261	0.2274	0.2335	0.2356	0.2363	0.2278	0.2298	0.2381			
$(5,5)$	0.2305	0.2288	0.2284	0.2398	0.2323	0.2307	0.2199	0.2299	0.2202	0.2276	0.2177	0.2402	0.2233	0.2218	0.2217	0.2402
	0.2270	0.2270	0.2242	0.2262	0.2287	0.2315	0.2292	0.2311	0.2307	0.2331	0.2296	0.2312	0.2182	0.2333	0.2209	
	0.2138	0.2191	0.1910	0.2034	0.2188	0.2209	0.2122	0.2201	0.2045	0.2118	0.2102	0.2194	0.2226	0.2109	0.2182	
	0.2201	0.2164	0.2195	0.2209	0.2209	0.2326	0.2202	0.2224	0.2216	0.2236	0.2219	0.2242	0.2193	0.2234	0.2193	
	0.2200	0.2219	0.2242	0.2228	0.2201	0.2235	0.2279	0.2235	0.2248	0.2271	0.2287	0.2215	0.2224	0.2292	0.2292	
	0.2311	0.2296	0.2316	0.2284	0.2288	0.2288	0.2307	0.2304	0.2328	0.2331	0.2062	0.2113	0.2173	0.2191	0.2210	
	0.2209	0.2130	0.2182	0.2223	0.2212	0.2224	0.2240	0.2239	0.2254	0.2250	0.2292	0.2312	0.2349	0.2269		
$(6,2)$	0.2553															0.2553
$(6,3)$	0.2426	0.2430	0.2457	0.2439	0.2474	0.2484										0.2484
$(7,2)$	0.2584															0.2584
$(7,3)$	0.2494	0.2507	0.2478	0.2508	0.2502	0.2524	0.2530									0.2530
$(8,2)$	0.2606															0.2606
$(8,3)$	0.2536	0.2513	0.2540	0.2543	0.2513	0.2545	0.2545	0.2559	0.2563							0.2563

Table 8.1: Numerical estimation of thresholds with post-selection by Alice and Bob on the inequivalent announcement sets in Table 4.1. The last column indicates the highest threshold in the (n,m) class.

To test Conjecture 1, which is that $Q^*_{\mathcal{B}_n,\mathcal{P}} = Q^*_{\mathcal{P}}$ for all $\mathcal{P}$, we can perform exactly the same threshold estimation procedure for the states $\rho^{\tilde{A}\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{P})}$ corresponding to no post-selection by Alice and post-selection by Bob on the inequivalent sets $\mathcal{P}$ of Table 4.1. The results are tabulated in Table 8.2 and plotted in Figure 8.1.

$(2,2)$	$Q^*_{\mathcal{P}}$	0.2151														
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2151														
$(2,3)$	$Q^*_{\mathcal{P}}$	0.1824														
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.1824														
$(3,2)$	$Q^*_{\mathcal{P}}$	0.2344														
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2344														
$(3,3)$	$Q^*_{\mathcal{P}}$	0.2057	0.2121													
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2057	0.2121													
$(3,4)$	$Q^*_{\mathcal{P}}$	0.2151	0.1978	0.1765	0.1949	0.2025										
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2151	0.1978	0.1765	0.1966	0.2025										
$(3,5)$	$Q^*_{\mathcal{P}}$	0.2075	0.1955	0.1815												
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2075	0.1956	0.1833												
$(3,6)$	$Q^*_{\mathcal{P}}$	0.1845	0.1824	0.2008												
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.1845	0.1824	0.2008												
$(3,7)$	$Q^*_{\mathcal{P}}$	0.1788														
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.1788														
$(4,2)$	$Q^*_{\mathcal{P}}$	0.2447														
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2447														
$(4,3)$	$Q^*_{\mathcal{P}}$	0.2267	0.2281	0.2307												
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2267	0.2381	0.2307												
$(4,4)$	$Q^*_{\mathcal{P}}$	0.2153	0.2344	0.2224	0.2154	0.1978	0.2073	0.2133	0.2209	0.2236	0.2230	0.2090	0.2144	0.2257		
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2153	0.2344	0.2224	0.2197	0.1978	0.2074	0.2133	0.2209	0.2236	0.2230	0.2093	0.2159	0.2257		
$(4,5)$	$Q^*_{\mathcal{P}}$	0.2126	0.2164	0.2070	0.2287	0.2059	0.2068	0.2179	0.2195	0.2186	0.1713	0.2138	0.2034	0.1923	0.2044	0.1961
		0.2026	0.2129	0.2028	0.2051	0.2036	0.2155	0.2179	0.2212	0.2078						
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2126	0.2164	0.2102	0.2287	0.2088	0.2074	0.2179	0.2195	0.2186	0.1713	0.2138	0.2037	0.1947	0.2102	0.1961
		0.2026	0.2129	0.2030	0.2054	0.2058	0.2155	0.2179	0.2212	0.2080						
$(4,6)$	$Q^*_{\mathcal{P}}$	0.1971	0.2057	0.2011	0.2236	0.2162	0.2023	0.2120	0.2121	0.2121	0.2024	0.2151	0.2117	0.2000	0.2088	0.2042
		0.2038	0.2102	0.1983	0.2042	0.2084	0.2109	0.2009	0.2235	0.2235	0.2128	0.2107	0.2107	0.2129	0.2129	0.2118
		0.2146	0.2172	0.1792	0.1952	0.2057	0.1882	0.2064	0.1954	0.1989	0.2046	0.1963	0.2008	0.1952	0.2057	0.2022
		0.2010	0.2130													
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.1993	0.2057	0.2011	0.2236	0.2162	0.2041	0.2120	0.2121	0.2121	0.2026	0.2152	0.2117	0.2057	0.2088	0.2060
		0.2044	0.2102	0.1995	0.2075	0.2086	0.2109	0.2010	0.2235	0.2235	0.2128	0.2107	0.2107	0.2129	0.2129	0.2118
		0.2146	0.2172	0.1817	0.1975	0.2057	0.1908	0.2064	0.2021	0.1992	0.2049	0.2005	0.2008	0.1968	0.2057	0.2023
		0.2011	0.2130													
$(5,3)$	$Q^*_{\mathcal{P}}$	0.2384	0.2365	0.2401	0.2416											
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2384	0.2365	0.2401	0.2416											
$(5,4)$	$Q^*_{\mathcal{P}}$	0.2344	0.2447	0.2331	0.2358	0.2281	0.2224	0.2253	0.2262	0.2254	0.2299	0.2309	0.2339	0.2361	0.2331	0.2345
		0.2225	0.2258	0.2235	0.2269	0.2230	0.2261	0.2274	0.2335	0.2356	0.2363	0.2278	0.2298	0.2381		
	$Q^*_{\mathcal{B}_n,\mathcal{P}}$	0.2345	0.2447	0.2331	0.2358	0.2281	0.2224	0.2257	0.2262	0.2254	0.2299	0.2309	0.2339	0.2361	0.2331	0.2345
		0.2225	0.2258	0.2235	0.2288	0.2230	0.2261	0.2274	0.2335	0.2356	0.2363	0.2278	0.2298	0.2381		

Table 8.2: Comparison of thresholds with and without post-selection by Alice on the inequivalent announcement sets in Table 4.1 for each (n, m) pair indicated in the left-most column.

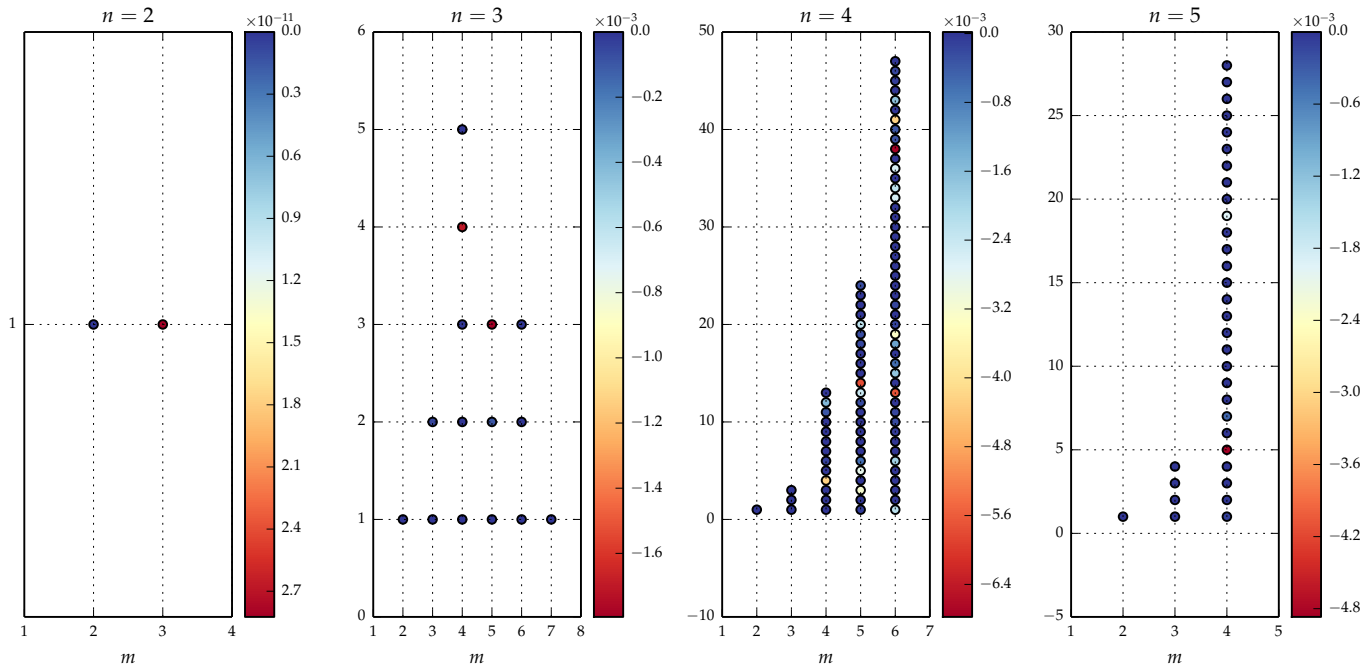


Figure 8.1: Comparison between the thresholds $Q^*_{\mathcal{P}}$ with and $Q^*_{\mathcal{B}_n,\mathcal{P}}$ without post-selection by Alice on the inequivalent announcement sets $\mathcal{P}$ in Table 4.1. The dots represent the announcement sets, and the colour of the dots, as given by the colorbars adjacent to the plots, indicate the difference between the thresholds.

We see that most of the thresholds $Q^*_{\mathcal{B}_n,\mathcal{P}}$ without post-selection by Alice are the same as the thresholds $Q^*_{\mathcal{P}}$ with post-selection by Alice up to at least four decimal places. There are some thresholds without post-selection that are the same as the corresponding thresholds with post-selection only up to two or three decimal places. It might be possible to get better agreement in these cases by taking more than 200 points in the estimation procedure. Overall, though, the data provides reasonably good evidence to support Conjecture 1 that $Q^*_{\mathcal{B}_n,\mathcal{P}} = Q^*_{\mathcal{P}}$ for all $\mathcal{P}$.

8.1 Trends and Analysis

By plotting $Q^*_{\max}$ for each (n, m) class from Table 8.1, we obtain the following.

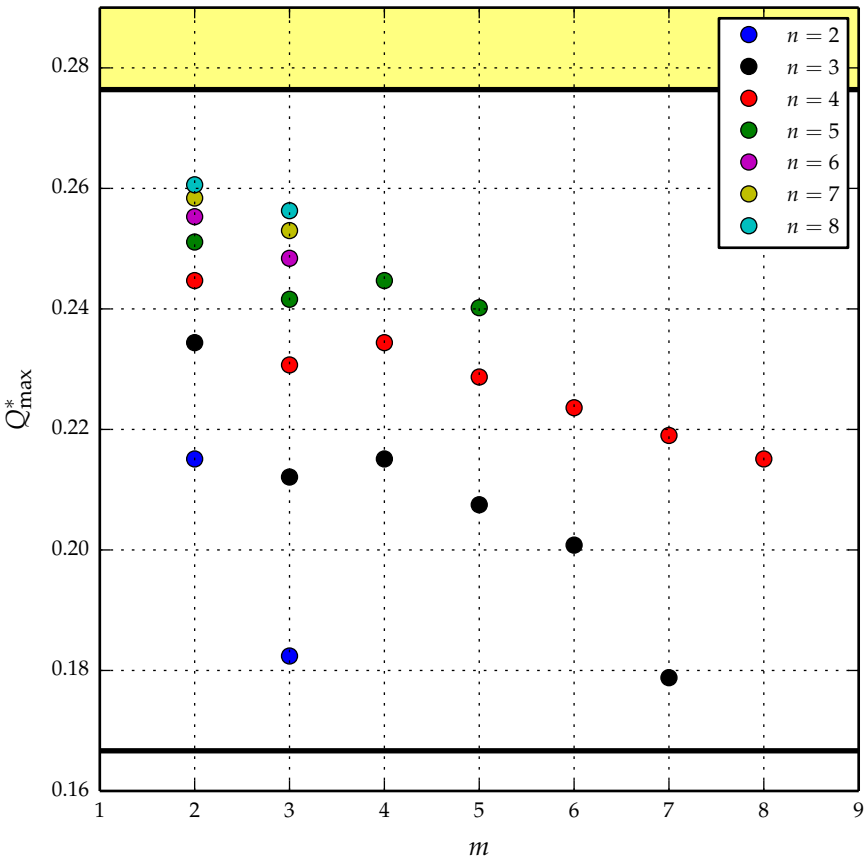


Figure 8.2: The highest thresholds $Q^*_{\max}$ as indicated in the right-most column of Table 8.1.

It is clear from this plot that for each n, the $m = 2$ announcement set, which is the repetition code $\mathcal{R}_n$, gives the highest threshold. As m increases beyond 2, the maximum threshold tends to decrease. As well, for fixed m, the maximum threshold increases with increasing n, with a clear indication that the thresholds converge towards the value $\frac{5-\sqrt{5}}{10}$ obtained using repetition codes. Along with the data from Chapter 7, this strengthens our belief that there does not exist a code whose corresponding filtered state is not symmetrically extendable within the gap, hence our belief that no successful two-way post-processing protocol exists within the gap.

On closer inspection of Table 8.1, we also observe that there are several instances in the $(n, m) = (4, 6)$, $(4, 7)$, $(4, 8)$, $(5, 4)$, and $(5, 5)$ classes in which two inequivalent announcement sets appear to have the same threshold since they agree up to at least six decimal places. The announcement sets are listed in the table below.

(n,m)	Q^*	Announcement Sets	
$(4,6)$	0.205719	2, 35, 44	$\left\{\begin{matrix}0000\\0101\\0110\\1000\\1101\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\1000\\1010\\1011\\1100\\1101\end{matrix}\right\}, \left\{\begin{matrix}0000\\1010\\1011\\1100\\1101\\1110\end{matrix}\right\}$
	0.212056	8, 9	$\left\{\begin{matrix}0000\\0110\\0111\\1000\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1000\\1110\\1111\end{matrix}\right\}$
	0.204239	15, 19	$\left\{\begin{matrix}0000\\0110\\1001\\1011\\1100\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1001\\1100\\1110\\1111\end{matrix}\right\}$
	0.223548	23, 24	$\left\{\begin{matrix}0000\\0111\\1000\\1011\\1100\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1000\\1100\\1110\\1111\end{matrix}\right\}$
	0.210679	26, 27	$\left\{\begin{matrix}0000\\0111\\1010\\1011\\1100\\1101\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1010\\1100\\1101\\1110\end{matrix}\right\}$
	0.212884	28, 29	$\left\{\begin{matrix}0000\\0111\\1010\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1010\\1100\\1110\\1111\end{matrix}\right\}$
$(4,7)$	0.199302	1, 49	$\left\{\begin{matrix}0000\\0010\\0011\\0100\\0101\\1000\\1001\end{matrix}\right\}, \left\{\begin{matrix}0000\\1000\\1010\\1011\\1100\\1101\\1110\end{matrix}\right\}$

0.208108	16, 17	$\left\{\begin{matrix}0000\\0110\\0111\\1000\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1000\\1100\\1110\\1111\end{matrix}\right\}$
0.204702	21, 26, 28	$\left\{\begin{matrix}0000\\0110\\0111\\1001\\1011\\1100\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1000\\1011\\1100\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1000\\1100\\1101\\1110\\1111\end{matrix}\right\}$
0.200910	22, 36	$\left\{\begin{matrix}0000\\0110\\0111\\1001\\1011\\1100\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1001\\1100\\1101\\1110\\1111\end{matrix}\right\}$
0.204004	24, 37	$\left\{\begin{matrix}0000\\0110\\0111\\1010\\1011\\1100\\1101\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1010\\1011\\1100\\1101\\1110\end{matrix}\right\}$
0.199949	29, 48	$\left\{\begin{matrix}0000\\0110\\1001\\1010\\1100\\1101\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\1000\\1001\\1010\\1100\\1110\\1111\end{matrix}\right\}$
0.197099	30, 31	$\left\{\begin{matrix}0000\\0110\\1001\\1010\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1001\\1010\\1100\\1110\\1111\end{matrix}\right\}$

	0.218946	40, 41	$\left\{\begin{matrix}0000\\0111\\1000\\1011\\1100\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1000\\1100\\1101\\1110\\1111\end{matrix}\right\}$
	0.208448	44, 45	$\left\{\begin{matrix}0000\\0111\\1010\\1011\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1010\\1100\\1101\\1110\\1111\end{matrix}\right\}$
$(4, 8)$	0.197825	2, 50, 56	$\left\{\begin{matrix}0000\\0011\\0101\\0110\\1000\\1011\\1101\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1010\\1011\\1100\\1101\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1000\\1010\\1011\\1100\\1101\\1110\end{matrix}\right\}$
	0.203015	5, 6	$\left\{\begin{matrix}0000\\0100\\0110\\1000\\1001\\1011\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0100\\0110\\1000\\1001\\1101\\1110\\1111\end{matrix}\right\}$
	0.204501	12, 38	$\left\{\begin{matrix}0000\\0100\\1000\\1011\\1100\\1101\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1000\\1010\\1100\\1101\\1111\end{matrix}\right\}$
	0.207208	21, 25	$\left\{\begin{matrix}0000\\0101\\0110\\1000\\1010\\1101\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0101\\0110\\1001\\1010\\1011\\1101\\1110\end{matrix}\right\}$

	0.192260	24, 28	$\left\{\begin{matrix}0000\\0101\\0110\\1001\\1010\\1011\\1100\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0101\\0110\\1001\\1010\\1100\\1110\\1111\end{matrix}\right\}$
	0.201461	27, 52	$\left\{\begin{matrix}0000\\0101\\0110\\1001\\1010\\1100\\1101\\1110\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1000\\1001\\1010\\1100\\1110\\1111\end{matrix}\right\}$
	0.204547	39, 40, 42	$\left\{\begin{matrix}0000\\0110\\0111\\1000\\1011\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1000\\1011\\1100\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\0111\\1000\\1100\\1101\\1110\\1111\end{matrix}\right\}$
	0.206155	53, 55	$\left\{\begin{matrix}0000\\0110\\1000\\1001\\1011\\1100\\1110\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0110\\1000\\1001\\1100\\1101\\1110\\1111\end{matrix}\right\}$
	0.214757	64, 65	$\left\{\begin{matrix}0000\\0111\\1000\\1010\\1011\\1100\\1101\\1111\end{matrix}\right\}, \left\{\begin{matrix}0000\\0111\\1000\\1010\\1100\\1101\\1110\\1111\end{matrix}\right\}$
$(5, 4)$	0.233074	3, 14	$\left\{\begin{matrix}00000\\01111\\10110\\11001\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11010\\11100\end{matrix}\right\}$

$(5,5)$	0.229194	$22, 74, 75$	$\left\{\begin{matrix}00000\\01111\\10110\\11000\\11101\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11000\\11011\\11100\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11000\\11100\\11110\end{matrix}\right\}$
	0.231085	$23, 76$	$\left\{\begin{matrix}00000\\01111\\10110\\11000\\11111\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11000\\11100\\11111\end{matrix}\right\}$
	0.218156	$28, 45$	$\left\{\begin{matrix}00000\\10000\\10110\\11001\\11111\end{matrix}\right\}, \left\{\begin{matrix}00000\\10100\\11000\\11110\\11111\end{matrix}\right\}$
	0.228442	$3, 79$	$\left\{\begin{matrix}00000\\01011\\01100\\10010\\10101\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11001\\11010\\11100\end{matrix}\right\}$
	0.220949	$36, 49$	$\left\{\begin{matrix}00000\\10011\\10100\\11000\\11111\end{matrix}\right\}, \left\{\begin{matrix}00000\\10101\\10110\\11000\\11111\end{matrix}\right\}$
	0.230704	$6, 24$	$\left\{\begin{matrix}00000\\01100\\01111\\10001\\10010\end{matrix}\right\}, \left\{\begin{matrix}00000\\01111\\10110\\11001\\11111\end{matrix}\right\}$
	0.223458	$66, 68$	$\left\{\begin{matrix}00000\\10110\\11001\\11011\\11100\end{matrix}\right\}, \left\{\begin{matrix}00000\\10110\\11001\\11100\\11110\end{matrix}\right\}$
	0.222430	$73, 96$	$\left\{\begin{matrix}00000\\10110\\11010\\11100\\11111\end{matrix}\right\}, \left\{\begin{matrix}00000\\11001\\11010\\11100\\11111\end{matrix}\right\}$
	0.228821	$80, 81$	$\left\{\begin{matrix}00000\\10111\\11010\\11100\\11101\end{matrix}\right\}, \left\{\begin{matrix}00000\\10111\\11010\\11100\\11110\end{matrix}\right\}$

Table 8.3: Inequivalent announcement sets from Table 4.1 that appear to have the same thresholds, as indicated by the results in Table 8.1. The numbers beside the threshold indicate the location of the set in Table 8.1.

In almost all cases, the two (or three) sets differ by only one codeword, and that one codeword is almost always a permutation of the codeword from the other set. Of course, the thresholds may merely be very close to each other and not the same, though we cannot exclude the possibility that they are the same and that therefore there exists an additional equivalence relation between announcement sets, one that is much deeper than the ones determined in §4.4. It remains to be explored the effects of making very small changes to a code on the symmetric extendability of the corresponding filtered state.

Summary

This thesis investigated the existence of two-way classical post-processing proctocols distilling secret keys for QKD protocols using the six-state and BB84 signal states with equal QBER in each basis. Specifically, we wanted to know whether there exist two-way protocols whenever the QBER Q of the protocol is within the gap $\left[\frac{5-\sqrt{5}}{10}, \frac{1}{3}\right)$ (with the six-state signal states) and $\left[\frac{1}{5}, \frac{1}{4}\right)$ (with the BB84 signal states). Since quantum entanglement distillation protocols are known to distill secret keys right up to the entanglement limits of $\frac{1}{3}$ and $\frac{1}{4}$, the question of key distillation within the gap using two-way classical post-processing protocols is equivalent to the question of whether classical key distillation protocols are just as good as quantum ones for distilling secret keys. The answer appears to be no, that is, there does not exist a two-way post-processing protocol distilling secret key within the gap.

Below is a summary of the results of this thesis:

- (Chapter 3) A method more efficient than SDPs for checking the symmetric extendability of bipartite states based on the special map (3.9).
- (Chapter 4) A new framework, building on the arguments presented in [Myh+09], for determining the existence of two-way post-processing protocols distilling secret keys. In this framework, we need only to check the symmetric extendability of Alice and Bob's correlations after post-selection by Bob on a block of his data according to some error-correcting code, though we allow Alice to perform post-selection as well. We determine equivalences of codes based on symmetric extendability and determine the number of inequivalent codes for small block lengths and code sizes in Table 4.1. We conjecture (Conjecture 1) that allowing Alice and Bob to post-select on the same code is equivalent (in terms of symmetric extendability) to allowing only Bob to post-select. We also conjecture (Conjecture 2) a two-step procedure for constructing symmetric extensions of the post-selected states.
- Proof, using the new framework, of the result known from [Myh+09] that advantage distillation (corresponding to post-selection on repetition codes) cannot break symmetric extendability beyond $\frac{5-\sqrt{5}}{10}$ using the six-state signal states (Chapter 5) and beyond $\frac{1}{5}$ for the BB84 signal states (Appendix C). We also prove Conjecture 1 and Conjecture 2, both using the special map from Chapter 3.
- (Chapter 6) Proof that post-selection on simplex codes, which generalizes advantage distillation, cannot break symmetric extendability in the gap. We also prove Conjecture 2 using the special map from Chapter 3.
- (Chapter 7) When Alice and Bob post-select on a first-order Reed-Muller code, the special map from Chapter 3 is not always able to construct a symmetric extension within the gap even though the resulting states are symmetrically extendable. We then show the results of testing over 540,000 codes using the special method from Chapter 3. We found that all of the resulting states were symmetrically extendable

within the gap and that the special method failed to construct a symmetric extension within the gap for less than 1% of the codes.

- (Chapter 8) Numerical estimation of the symmetric extendability thresholds from post-selection by Alice and Bob on the inequivalent codes in Table 4.1 reveal that for any given block length, the repetition code threshold is always the highest, with thresholds decreasing as the number of codewords increases. We also provide evidence for the truth of Conjecture 1 in Table 8.2 and Figure 8.1.

All the results of this thesis strengthen our belief that in the gap two-way post-processing protocols distilling secret keys do not exist for QKD protocols using the six-state signal states with equal QBER in each basis. In particular, the value $\frac{5-\sqrt{5}}{10}$ of the QBER appears to be a point beyond which classical correlations arising from entangled quantum states cannot be used to distill secret key. As mentioned in the introduction, this suggests the existence of bound information, which was first conjectured in [GW00] and discussed subsequently in [GRW01; GRW02; CP02; RW03; AG05]. In these works, the authors discuss the possibility that bound information might arise from measurement of bound entangled states. Though an example of a bound entangled state with positive distillable key upon measurement was then found in [Hor+05], this result does not completely rule out the existence of bound information arising from bound entangled states, so that the existence of bound information remains an open problem. Our results add to the possibilities by indicating that bound information might arise even upon measuring entangled states with distillable entanglement.

Bibliography

[Ací+06] A. Acín et al. "Secrecy properties of quantum channels". In: *Phys. Rev. A* 73 (1 Jan. 2006), p. 012327. DOI: 10.1103/PhysRevA.73.012327.

[AG05] Antonio Acín and Nicolas Gisin. "Quantum Correlations and Secret Bits". In: *Phys. Rev. Lett.* 94 (2 Jan. 2005), p. 020501. DOI: 10.1103/PhysRevLett.94.020501.

[AMG03] Antonio Acín, Lluis Masanes, and Nicolas Gisin. "Equivalence between Two-Qubit Entanglement and Secure Key Distribution". In: *Phys. Rev. Lett.* 91 (16 Oct. 2003), p. 167901. DOI: 10.1103/PhysRevLett.91.167901.

[BA07] Joonwoo Bae and Antonio Acín. "Key distillation from quantum channels using two-way communication protocols". In: *Phys. Rev. A* 75 (1 Jan. 2007), p. 012334. DOI: 10.1103/PhysRevA.75.012334.

[BB84] C. H. Bennett and G. Brassard. "Quantum cryptography: public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*. 1984, pp. 175–179.

[BB85] C.H. Bennett and G. Brassard. "Quantum Public Key Distribution". In: *IBM Technical Disclosure Bulletin* 28 (1985), pp. 3153–3163.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. "Privacy Amplification by Public Discussion". In: *SIAM Journal on Computing* 17.2 (1988), pp. 210–229. URL: http://dx.doi.org/10.1137/0217014.

[Ben+95] C. H. Bennett et al. "Generalized privacy amplification". In: *IEEE Transactions on Information Theory* 41.6 (Nov. 1995), pp. 1915–1923. ISSN: 0018-9448. DOI: 10.1109/18.476316.

[Ben+96a] Charles H. Bennett et al. "Mixed-state entanglement and quantum error correction". In: *Phys. Rev. A* 54 (5 Nov. 1996), pp. 3824–3851. DOI: 10.1103/PhysRevA.54.3824.

[Ben+96b] Charles H. Bennett et al. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". In: *Phys. Rev. Lett.* 76 (5 Jan. 1996), pp. 722–725. DOI: 10.1103/PhysRevLett.76.722.

[Ben02] M. Ben-Or. "Simple security proof for quantum key distribution". In: (2002). URL: http://www.msri.org/realvideo/ln/msri/2002/qip/ben-or/1/index.html.

[BG99] H. Bechmann-Pasquinucci and N. Gisin. "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography". In: *Phys. Rev. A* 59 (6 June 1999), pp. 4238–4248. DOI: 10.1103/PhysRevA.59.4238.

[Bha07] Rajendra Bhatia. *Positive Definite Matrices*. Princeton University Press, 2007.

[Bra15] Kamil Bradler. "The Pitfalls of Deciding Whether a Quantum Channel is (Conjugate) Degradable and How to Avoid Them". In: *Open Systems and Information Dynamics* 22.04 (2015), p. 1550026. DOI: 10.1142/S1230161215500262.

[Bru+03] Dagmar Bruß et al. "Tomographic Quantum Cryptography: Equivalence of Quantum and Classical Key Distillation". In: *Phys. Rev. Lett.* 91 (9 Aug. 2003), p. 097901. DOI: 10.1103/PhysRevLett.91.097901. URL: http://link.aps.org/doi/10.1103/PhysRevLett.91.097901.

[Bru98] Dagmar Bruß. "Optimal Eavesdropping in Quantum Cryptography with Six States". In: *Phys. Rev. Lett.* 81 (14 Oct. 1998), pp. 3018–3021. DOI: 10.1103/PhysRevLett.81.3018.

[Cha02] H. F. Chau. "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate". In: *Phys. Rev. A* 66 (6 Dec. 2002), p. 060302. DOI: 10.1103/PhysRevA.66.060302.

[Che+14] Jianxin Chen et al. "Symmetric extension of two-qubit states". In: *Phys. Rev. A* 90 (3 Sept. 2014), p. 032318. DOI: 10.1103/PhysRevA.90.032318.

[Chr+07] Matthias Christandl et al. "Unifying Classical and Quantum Key Distillation". In: *Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007. Proceedings*. Ed. by Salil P. Vadhan. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 456–478. ISBN: 978-3-540-70936-7. DOI: 10.1007/978-3-540-70936-7_25.

[CKR09] Matthias Christandl, Robert König, and Renato Renner. "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography". In: *Phys. Rev. Lett.* 102 (2 Jan. 2009), p. 020504. DOI: 10.1103/PhysRevLett.102.020504.

[CLL04] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. "Entanglement as a Precondition for Secure Quantum Key Distribution". In: *Phys. Rev. Lett.* 92 (21 May 2004), p. 217903. DOI: 10.1103/PhysRevLett.92.217903.

[CP02] Daniel Collins and Sandu Popescu. "Classical analog of entanglement". In: *Phys. Rev. A* 65 (3 Feb. 2002), p. 032321. DOI: 10.1103/PhysRevA.65.032321. URL: http://link.aps.org/doi/10.1103/PhysRevA.65.032321.

[Cub] Toby Cubitt. URL: http://www.dr-qubit.org/Matlab_code.html.

[Deu+96] David Deutsch et al. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". In: *Phys. Rev. Lett.* 77 (13 Sept. 1996), pp. 2818–2821. DOI: 10.1103/PhysRevLett.77.2818.

[DPS02] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Distinguishing Separable and Entangled States". In: *Phys. Rev. Lett.* 88 (18 Apr. 2002), p. 187904. DOI: 10.1103/PhysRevLett.88.187904.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Complete family of separability criteria". In: *Phys. Rev. A* 69 (2 Feb. 2004), p. 022308. DOI: 10.1103/PhysRevA.69.022308.

[Fun+14] Chi-Hang Fred Fung et al. "Conditions for degradability of tripartite quantum states". In: *Journal of Physics A: Mathematical and Theoretical* 47.11 (2014), p. 115306. URL: http://stacks.iop.org/1751-8121/47/i=11/a=115306.

[GL03] D. Gottesman and Hoi-Kwong Lo. "Proof of security of quantum key distribution with two-way classical communications". In: *IEEE Transactions on Information Theory* 49.2 (Feb. 2003), pp. 457–475. ISSN: 0018-9448. DOI: 10.1109/TIT.2002.807289.

[GRW01] Nicolas Gisin, Renato Renner, and Stefan Wolf. "Bound Information: The Classical Analog to Bound Quantum Entanglement". In: *European Congress of Mathematics: Barcelona, July 10–14, 2000 Volume II*. Ed. by Carles Casacuberta et al. Basel: Birkhäuser Basel, 2001, pp. 439–447. ISBN: 978-3-0348-8266-8. DOI: 10.1007/978-3-0348-8266-8_38.

[GRW02] Gisin, Renner, and Wolf. "Linking Classical and Quantum Key Agreement: Is There a Classical Analog to Bound Entanglement?" In: *Algorithmica* 34.4 (2002), pp. 389–412. ISSN: 1432-0541. DOI: 10.1007/s00453-002-0972-7.

[GW00] Nicolas Gisin and Stefan Wolf. "Linking Classical and Quantum Key Agreement: Is There "Bound Information"?" In: *Advances in Cryptology — CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings*. Ed. by Mihir Bellare. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 482–500. ISBN: 978-3-540-44598-2. DOI: 10.1007/3-540-44598-6_30.

[GW99] N. Gisin and S. Wolf. "Quantum Cryptography on Noisy Channels: Quantum versus Classical Key-Agreement Protocols". In: *Phys. Rev. Lett.* 83 (20 Nov. 1999), pp. 4200–4203. DOI: 10.1103/PhysRevLett.83.4200.

[HH99] Michał Horodecki and Paweł Horodecki. "Reduction criterion of separability and limits for a class of distillation protocols". In: *Phys. Rev. A* 59 (6 June 1999), pp. 4206–4216. DOI: 10.1103/PhysRevA.59.4206.

[HHH96] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. "Separability of mixed states: necessary and sufficient conditions". In: *Physics Letters A* 223.1 (1996), pp. 1–8. ISSN: 0375-9601. DOI: http://dx.doi.org/10.1016/S0375-9601(96)00706-2.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?" In: *Phys. Rev. Lett.* 80 (24 June 1998), pp. 5239–5242. DOI: 10.1103/PhysRevLett.80.5239.

[Hor+05] Karol Horodecki et al. "Secure Key from Bound Entanglement". In: *Phys. Rev. Lett.* 94 (16 Apr. 2005), p. 160502. DOI: 10.1103/PhysRevLett.94.160502.

[Hor+09] K. Horodecki et al. "General Paradigm for Distilling Classical Key From Quantum States". In: *IEEE Transactions on Information Theory* 55.4 (Apr. 2009), pp. 1898–1929. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2009798.

[Hor97] Pawel Horodecki. "Separability criterion and inseparable mixed states with positive partial transposition". In: *Physics Letters A* 232.5 (1997), pp. 333–339. ISSN: 0375-9601. DOI: http://dx.doi.org/10.1016/S0375-9601(97)00416-7. URL: http://www.sciencedirect.com/science/article/pii/S0375960197004167.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. "Pseudo-random Generation from One-way Functions". In: *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*. STOC '89. Seattle, Washington, USA: ACM, 1989, pp. 12–24. ISBN: 0-89791-307-8. DOI: 10.1145/73007.73009. URL: http://doi.acm.org/10.1145/73007.73009.

[Joh16] Nathaniel Johnston. *QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9*. http://qetlab.com. Jan. 2016. DOI: 10.5281/zenodo.44637.

[KBR07] Barbara Kraus, Cyril Branciard, and Renato Renner. "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses". In: *Phys. Rev. A* 75 (1 Jan. 2007), p. 012316. DOI: 10.1103/PhysRevA.75.012316. URL: http://link.aps.org/doi/10.1103/PhysRevA.75.012316.

[KGR05] B. Kraus, N. Gisin, and R. Renner. "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication". In: *Phys. Rev. Lett.* 95 (8 Aug. 2005), p. 080501. DOI: 10.1103/PhysRevLett.95.080501.

[KMR05] R. Konig, U. Maurer, and R. Renner. "On the power of quantum memory". In: *IEEE Transactions on Information Theory* 51.7 (July 2005), pp. 2391–2401. ISSN: 0018-9448. DOI: 10.1109/TIT.2005.850087.

[LC99] Hoi-Kwong Lo and H. F. Chau. "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* 283.5410 (1999), pp. 2050–2056. ISSN: 0036-8075. DOI: 10.1126/science.283.5410.2050.

[Lo01] Hoi-Kwong Lo. "Proof of Unconditional Security of Six-state Quatum Key Distribution Scheme". In: *Quantum Info. Comput.* 1.2 (Aug. 2001), pp. 81–94. ISSN: 1533-7146. URL: http://dl.acm.org/citation.cfm?id=2011333.2011337.

[Lof04] J. Lofberg. "YALMIP : a toolbox for modeling and optimization in MATLAB". In: *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*. Sept. 2004, pp. 284–289. DOI: 10.1109/CACSD.2004.1393890.

[Lüt14] Norbert Lütkenhaus. "Quantum Key Distribution". In: *Quantum Information and Coherence*. Ed. by Erika Andersson and Patrick Öhberg. Springer, 2014. Chap. 10, pp. 107–146.

[Mat04] Artur Ekert Matthias Christandl Renato Renner. "A Generic Security Proof for Quantum Key Distribution". In: (Feb. 2004). URL: http://arxiv.org/abs/quant-ph/0402131v2.

[Mau93] U. M. Maurer. "Secret key agreement by public discussion from common information". In: *IEEE Transactions on Information Theory* 39.3 (May 1993), pp. 733–742. ISSN: 0018-9448. DOI: 10.1109/18.256484.

[MCL06] Tobias Moroder, Marcos Curty, and Norbert Lütkenhaus. "One-way quantum key distribution: Simple upper bound on the secret key rate". In: *Phys. Rev. A* 74 (5 Nov. 2006), p. 052301. DOI: 10.1103/PhysRevA.74.052301.

[ML09] Geir Ove Myhr and Norbert Lütkenhaus. "Spectrum conditions for symmetric extendible states". In: *Phys. Rev. A* 79 (6 June 2009), p. 062307. DOI: 10.1103/PhysRevA.79.062307.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

[Myh+09] Geir Ove Myhr et al. "Symmetric extension in two-way quantum key distribution". In: *Phys. Rev. A* 79 (4 Apr. 2009), p. 042329. DOI: 10.1103/PhysRevA.79.042329.

[Myh10] Geir Ove Myhr. "Symmetric Extension of Bipartite Quantum States and its Use in Quantum Key Distribution with Two-Way Postprocessing". PhD thesis. Friedrich-Alexander-Universität Erlangen-Nüremberg, Aug. 2010.

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000. ISBN: 9780521635035.

[NH09] Marcin L Nowakowski and Pawel Horodecki. "A simple test for quantum channel capacity". In: *Journal of Physics A: Mathematical and Theoretical* 42.13 (2009), p. 135306. URL: http://stacks.iop.org/1751-8121/42/i=13/a=135306.

[ODo+16] Brendan O'Donoghue et al. "Conic Optimization via Operator Splitting and Homogeneous Self-Dual Embedding". In: *Journal of Optimization Theory and Applications* 169.3 (2016), pp. 1042–1068. ISSN: 1573-2878. DOI: 10.1007/s10957-016-0892-3. URL: http://dx.doi.org/10.1007/s10957-016-0892-3.

[Per96] Asher Peres. "Separability Criterion for Density Matrices". In: *Phys. Rev. Lett.* 77 (8 Aug. 1996), pp. 1413–1415. DOI: 10.1103/PhysRevLett.77.1413.

[Ran09] Kedar S. Ranade. "Symmetric extendibility for a class of qudit states". In: *Journal of Physics A: Mathematical and Theoretical* 42.42 (2009), p. 425302. URL: http://stacks.iop.org/1751-8121/42/i=42/a=425302.

[Ren05] Renato Renner. "Security of Quantum Key Distribution". PhD thesis. Swiss Federal Institute of Technology Zürich, Sept. 2005.

[Ren07] Renato Renner. "Symmetry of large physical systems implies independence of subsystems". In: *Nature Physics* 3 (9 Sept. 2007), pp. 645–649. DOI: http://dx.doi.org/10.1038/nphys684.

[RGK05] Renato Renner, Nicolas Gisin, and Barbara Kraus. "Information-theoretic security proof for quantum-key-distribution protocols". In: *Phys. Rev. A* 72 (1 July 2005), p. 012332. DOI: 10.1103/PhysRevA.72.012332.

[RK05] Renato Renner and Robert König. "Universally Composable Privacy Amplification Against Quantum Adversaries". In: *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings*. Ed. by Joe Kilian. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 407–425. ISBN: 978-3-540-30576-7. DOI: 10.1007/978-3-540-30576-7_22. URL: http://dx.doi.org/10.1007/978-3-540-30576-7_22.

[RW03] Renato Renner and Stefan Wolf. "New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction". In: *Advances in Cryptology — EUROCRYPT 2003*. Ed. by Eli Biham. Vol. 2656. Lecture Notes in Computer Science. Springer-Verlag, May 2003, pp. 562–577.

[SP00] Peter W. Shor and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Phys. Rev. Lett.* 85 (2 July 2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441.

[VB96] Lieven Vandenberghe and Stephen Boyd. "Semidefinite Programming". In: *SIAM Review* 38.1 (1996), pp. 49–95. DOI: 10.1137/1038003. eprint: http://dx.doi.org/10.1137/1038003. URL: http://dx.doi.org/10.1137/1038003.

[Wat16] John Watrous. "Theory of Quantum Information". 2016. URL: https://cs.uwaterloo.ca/~watrous/TQI/.

[Wer89] Reinhard F. Werner. "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". In: *Phys. Rev. A* 40 (8 Oct. 1989), pp. 4277–4281. DOI: 10.1103/PhysRevA.40.4277.

Appendix A

Proof of Formula (3.11)

By (3.10) and Proposition 2.10, we have

$$K(\mathcal{N}) = S(J(\mathcal{N})) = K(\Phi_{P^{AB}})K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})^{-1} \Rightarrow J(\mathcal{N}) = S^{-1}\left[K(\Phi_{P^{AB}})K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})^{-1}\right].$$

But

$$K(\Phi_{P^{AB}}) = S(J(\Phi_{P^{AB}})) = S(P^{AB}), \quad K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})^{-1} = \left(S(J(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}}))\right)^{-1},$$

and using the purification

$$|\psi\rangle^{ABE_1E_2} = \sum_{k,k'=0}^{d_A-1}\sum_{\ell,\ell'=0}^{d_B-1}\left(\sqrt{P^{AB}}\right)_{\substack{k,\ell\\k',\ell'}}|k,\ell\rangle^{AB} \otimes |k',\ell'\rangle^{E_1E_2} = \mathrm{vec}\left(\sqrt{P^{AB}}\right) \tag{A.1}$$

of P^{AB} in $\mathfrak{H}_{E_1E_2}$, we get by Proposition 2.18 that

$$J(\Phi^c_{P^{AB}}) = \mathrm{Tr}_B[|\psi\rangle\langle\psi|^{ABE_1E_2}] = P^{AE_1E_2} \Rightarrow J(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}}) = (\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)} \otimes \mathrm{Tr}_{E_2})J(\Phi^c_{P^{AB}}) = P^{AE_1},$$

which means that

$$K(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}})^{-1} = \left(S(J(\mathrm{Tr}_{E_2} \circ \Phi^c_{P^{AB}}))\right)^{-1} = S(P^{AE_1})^{-1}.$$

Now, using (A.1),

$$P^{AE_1} = \mathrm{Tr}_{B,E_2}\left[|\psi\rangle\langle\psi|^{ABE_1E_2}\right] = \sum_{\substack{k,k'\\i,i'=0}}^{d_A-1}\left(\sum_{\ell,\ell'=0}^{d_B-1}\left(\sqrt{P^{AB}}\right)_{\substack{k,\ell\\k',\ell'}}\overline{\left(\sqrt{P^{AB}}\right)_{\substack{i,\ell\\i',\ell'}}}\right)|k,k'\rangle\langle i,i'|^{AE_1}.$$

By definition of the shuffling map,

$$\left(\sqrt{P^{AB}}\right)_{\substack{k,\ell\\k',\ell'}} = S\left(\sqrt{P^{AB}}\right)_{\substack{\ell,\ell'\\k,k'}} = \left(S\left(\sqrt{P^{AB}}\right)^{\mathsf{T}}\right)_{\substack{k,k'\\\ell,\ell'}} \quad \forall\, 0 \le k,k' \le d_A-1,\ 0 \le \ell,\ell' \le d_B-1$$

and

$$\overline{\left(\sqrt{P^{AB}}\right)_{\substack{i,\ell\\i',\ell'}}} = \overline{S\left(\sqrt{P^{AB}}\right)_{\substack{\ell,\ell'\\i,i'}}} = \left(\overline{S\left(\sqrt{P^{AB}}\right)}\right)_{\substack{\ell,\ell'\\i,i'}} \quad \forall\, 0 \le i,i' \le d_A-1,\ 0 \le \ell,\ell' \le d_B-1,$$

which means that

$$P^{AE_1} = \sum_{\substack{k,k'\\i,i'=0}}^{d_A-1}\left(S\left(\sqrt{P^{AB}}\right)^{\mathsf{T}}\overline{S\left(\sqrt{P^{AB}}\right)}\right)_{\substack{k,k'\\i,i'}}|k,k'\rangle\langle i,i'|^{AE_1} \Rightarrow P^{AE_1} = S\left(\sqrt{P^{AB}}\right)^{\mathsf{T}}\overline{S\left(\sqrt{P^{AB}}\right)}.$$

Therefore,

$$J(\mathcal{N}) = S^{-1}\left[S\left(P^{AB}\right) S\left(S\left(\sqrt{P^{AB}}\right)^{\intercal} \overline{S\left(\sqrt{P^{AB}}\right)}\right)^{-1}\right],$$

as required.

Appendix B

Chapter 4 Proofs

Proposition B.1

For sets $\mathcal{P}_1 = \{P_{1,k}\}_{k=0}^{m_{A_1}-1}$ and $\mathcal{Q}_1 = \{Q_{1,\ell}\}_{\ell=0}^{m_{B_1}-1}$ of n_1-bit strings, and for sets $\mathcal{P}_2 = \{P_{2,k}\}_{k=0}^{m_{A_2}-1}$ and $\mathcal{Q}_2 = \{Q_{2,\ell}\}_{\ell=0}^{m_{B_2}-1}$ of n_2-bit strings, it holds that

$$\rho^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}_{Q,'^{(|\mathcal{P}_1|\mathcal{P}_2|,}_{|\mathcal{Q}_1|\mathcal{Q}_2|)}} = W\left(\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{P}_1,\mathcal{Q}_1)} \otimes \rho^{\tilde{A}_2\tilde{B}_2}_{Q,(\mathcal{P}_2,\mathcal{Q}_2)}\right) W^\dagger,$$

where $W = \mathrm{SWAP}_{\tilde{A}_2\tilde{B}_1}$ is the unitary operator that swaps the $\mathfrak{H}_{\tilde{A}_2}$ and $\mathfrak{H}_{\tilde{B}_1}$ spaces and is defined analogously to (3.1).

PROOF: By (4.22), it holds that

$$\begin{aligned}\rho^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}_{Q,'^{(|\mathcal{P}_1|\mathcal{P}_2|,}_{|\mathcal{Q}_1|\mathcal{Q}_2|)}} &= (A_{|\mathcal{P}_1|\mathcal{P}_2|} \otimes A_{|\mathcal{Q}_1|\mathcal{Q}_2|})(\rho_Q^{A^{n_1+n_2}B^{n_1+n_2}})(A_{|\mathcal{P}_1|\mathcal{P}_2|} \otimes A_{|\mathcal{Q}_1|\mathcal{Q}_2|})^\dagger \\ &= \sum_{i,i'=0}^{m_{A_1}-1}\sum_{j,j'=0}^{m_{A_2}-1}\sum_{k,k'=0}^{m_{B_1}-1}\sum_{\ell,\ell'=0}^{m_{B_2}-1} |i,j,k,\ell\rangle\langle i',j',k',\ell'| \left\langle P_{1,i}P_{2,j}, Q_{1,k}Q_{2,\ell}\right| \rho_Q^{A^{n_1+n_2}B^{n_1+n_2}} \left|P_{1,i'}P_{2,j'}, Q_{1,k'}Q_{2,\ell'}\right\rangle.\end{aligned}$$

Then, by (4.9),

$$\begin{aligned}&\left\langle P_{1,i}P_{2,j}, Q_{1,k}Q_{2,\ell}\right| \rho_Q^{A^{n_1+n_2}B^{n_1+n_2}} \left|P_{1,i'}P_{2,j'}, Q_{1,k'}Q_{2,\ell'}\right\rangle \\ &\quad= \langle P_{1,i}, Q_{1,k}| \rho_Q^{A^{n_1}B^{n_1}} |P_{1,i'}, Q_{2,k'}\rangle \langle P_{2,j}, Q_{2,\ell}| \rho_Q^{A^{n_2}B^{n_2}} |P_{2,j'}, Q_{2,\ell'}\rangle \\ &\quad= \left(\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{P}_1,\mathcal{Q}_1)}\right)_{\substack{i,k\\i',k'}} \left(\rho^{\tilde{A}_2\tilde{B}_2}_{Q,(\mathcal{P}_2,\mathcal{Q}_2)}\right)_{\substack{j,\ell\\j',\ell'}}\end{aligned}$$

for all $0 \le i, i' \le m_{A_1} - 1$, $0 \le k, k' \le m_{B_1} - 1$, $0 \le j, j' \le m_{A_2} - 1$, $0 \le \ell, \ell' \le m_{B_2} - 1$. Also, by definition of $W = \mathrm{SWAP}_{\tilde{A}_2\tilde{B}_1}$

$$W\,|i,k,j,\ell\rangle^{\tilde{A}_1\tilde{B}_1\tilde{A}_2\tilde{B}_2} = |i,j,k,\ell\rangle^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}$$

for all $0 \leq i \leq m_{A_1} - 1, 0 \leq k \leq m_{B_1} - 1, 0 \leq j \leq m_{A_2} - 1, 0 \leq \ell \leq m_{B_2} - 1$, so that

$$\begin{aligned}\rho^{\tilde{A}_1\tilde{A}_2\tilde{B}_1\tilde{B}_2}_{Q,_{|\mathcal{Q}_1||\mathcal{Q}_2|)}^{(|\mathcal{P}_1||\mathcal{P}_2|,}} &= W\left(\sum_{i,i'=0}^{m_{A_1}-1}\sum_{j,j'=0}^{m_{A_2}-1}\sum_{k,k'=0}^{m_{B_1}-1}\sum_{\ell,\ell'=0}^{m_{B_2}-1}\left(\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{P}_1,\mathcal{Q}_1)}\right)_{\substack{i,k\\i',k'}}\left(\rho^{\tilde{A}_2\tilde{B}_2}_{Q,(\mathcal{P}_2,\mathcal{Q}_2)}\right)_{\substack{j,\ell\\j',\ell'}}|i,k\rangle\langle i',k'|^{\tilde{A}_1\tilde{B}_1}\otimes|j,\ell\rangle\langle j',\ell'|^{\tilde{A}_2\tilde{B}_2}\right)W^\dagger \\ &= W\left(\rho^{\tilde{A}_1\tilde{B}_1}_{Q,(\mathcal{P}_1,\mathcal{Q}_1)}\otimes\rho^{\tilde{A}_2\tilde{B}_2}_{Q,(\mathcal{P}_2,\mathcal{Q}_2)}\right)W^\dagger,\end{aligned}$$

as required. ■

Proposition B.2

For the Levenshtein construction of a copies of $\mathcal{P} = \{P_k\}_{k=0}^{m-1}$ of n_1-bit strings and b copies of $\mathcal{Q} = \{Q_\ell\}_{\ell=0}^{m-1}$ of n_2-bit strings, it holds that

$$\rho^{\tilde{A}\tilde{B}}_{Q,a\mathcal{P}+b\mathcal{Q}} = \left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)^{\circ a}\circ\left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{Q}}\right)^{\circ b}$$

PROOF: By definition (4.9) for the matrix elements of the filtered state in the standard basis, for all $0 \leq k, k', \ell, \ell' \leq m-1$ we have

$$\begin{aligned}&\left(\rho^{\tilde{A}\tilde{B}}_{Q,a\mathcal{P}+b\mathcal{Q}}\right)_{\substack{k,\ell\\k',\ell'}} \\ &= \langle P_k\cdots P_kQ_k\cdots Q_k, P_\ell\cdots P_\ell Q_\ell\cdots Q_\ell|\,\rho_Q^{A^{an_1+bn_2}B^{an_1+bn_2}}\,|P_{k'}\cdots P_{k'}Q_{k'}\cdots Q_{k'}, P_{\ell'}\cdots P_{\ell'}Q_{\ell'}\cdots Q_{\ell'}\rangle \\ &= \left(\langle P_k, P_\ell|\,\rho_Q^{A^{n_1}B^{n_1}}\,|P_{k'}, P_{\ell'}\rangle\right)^a\left(\langle Q_k, Q_\ell|\,\rho_Q^{A^{n_2}B^{n_2}}\,|Q_{k'}, Q_{\ell'}\rangle\right)^b \\ &= \left(\left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k,\ell\\k',\ell'}}\right)^a\left(\left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{Q}}\right)_{\substack{k,\ell\\k',\ell'}}\right)^b.\end{aligned}$$

The result follows by definition (4.25) of the Hadamard product. ■

Appendix C

Repetition Codes with the BB84 Signal States

In the standard basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$,

$$\rho_{Q,x}^{AB} = \begin{bmatrix} \frac{1-Q}{2} & 0 & 0 & \frac{1}{2} - \frac{3Q}{2} + x \\ 0 & \frac{Q}{2} & \frac{Q}{2} - x & 0 \\ 0 & \frac{Q}{2} - x & \frac{Q}{2} & 0 \\ \frac{1}{2} - \frac{3Q}{2} + x & 0 & 0 & \frac{1-Q}{2} \end{bmatrix}, \tag{C.1}$$

so that the filtered state $\rho_{Q,x,\mathcal{R}_n}^{\tilde{A}\tilde{B}}$ after post-selection on repetition codes is

$$\rho_{Q,x,n}^{\tilde{A}\tilde{B}} = \begin{bmatrix} q_1 & 0 & 0 & q_2 \\ 0 & q_0 & q_3 & 0 \\ 0 & q_3 & q_0 & 0 \\ q_2 & 0 & 0 & q_1 \end{bmatrix}, \tag{C.2}$$

where we define

$$q_0 = \left(\frac{Q}{2}\right)^n, \quad q_1 = \left(\frac{1-Q}{2}\right)^n, \quad q_2 = \left(\frac{1}{2} - \frac{3Q}{2} + x\right)^n, \quad q_3 = \left(\frac{Q}{2} - x\right)^n. \tag{C.3}$$

This state is Bell-diagonal with eigenvalues

$$q_1 + q_2, \quad q_1 - q_2, \quad q_0 + q_3, \quad q_0 - q_3. \tag{C.4}$$

The eigenvalues of $\left(\rho_{Q,x,n}^{\tilde{A}\tilde{B}}\right)^{\mathsf{T}_{\tilde{B}}}$ are

$$q_1 + q_3, \quad q_1 - q_3, \quad q_0 + q_2, \quad q_0 - q_2.$$

Similar to the analysis in §2.4.3, finding for each $n > 1$ the highest Q such that the states $\{\rho_{Q,x,n}^{\tilde{A}\tilde{B}}\}_{x\in[0,Q]}$ are entangled, we obtain by the PPT criterion

$$q_1 + q_3 < 0, \quad q_1 - q_3 < 0, \quad q_0 + q_2 < 0, \quad q_0 - q_2 < 0.$$

The first and third of these conditions is never satisfied as q_0, q_1, q_2, q_3 are non-negative for all $n \geq 1$, for all $0 \leq Q \leq \frac{1}{2}$, and for all $0 \leq x \leq Q$. The second and fourth conditions lead to

$$\frac{1}{2} - Q + x < 0 \quad \text{and} \quad 2Q - x - \frac{1}{2} < 0$$

for all $n > 1$, which are the same conditions obtained in §2.4.3 for the original unfiltered states. Therefore, for all $n > 1$, the separability boundary for the class of states $\{\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}\}_{x\in[0,Q]}$ is $\frac{1}{4}$, just as for the unfiltered states. Now,

$$\begin{aligned} \det\left(\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}\right) &= (q_1^2 - q_2^2)(q_0^2 - q_3^2), \\ \mathrm{Tr}\left[\left(\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}\right)^2\right] &= 2q_1^2 + 2q_2^2 + 2q_0^2 + 2q_3^2, \\ \mathrm{Tr}\left[\left(\rho^{\tilde{B}}_{Q,x,\mathcal{R}_n}\right)^2\right] &= 2q_0^2 + 2q_1^2 + 2q_0q_1. \end{aligned} \tag{C.5}$$

Therefore, the condition (3.2) for the symmetric extendability of $\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}$ is

$$4\sqrt{(q_1^2 - q_2^2)(q_0^2 - q_3^2)} \geq 2q_2^2 + 2q_3^2 - 4q_0q_1. \tag{C.6}$$

Squaring both sides of this inequality and simplifying gives

$$q_3^2(4q_1^2 - 2q_2^2 - 4q_0q_1 + q_3^2) + q_2^2(4q_0^2 - 4q_0q_1 + q_2^2) \leq 0. \tag{C.7}$$

The thresholds Q_n^* are defined as the largest Q such that the set $\{\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}\}_{x\in[0,Q]}$ does *not* contain a symmetrically extendable state. To determine them, we must find for each n the largest Q such that the left-hand side of (C.7) is *positive* for all $0 \leq x \leq Q$, as positivity of the left-hand side of (C.7) means that $\rho^{\tilde{A}\tilde{B}}_{Q,x,n}$ is *not* symmetrically extendable. Doing this for up to $n = 40$, we obtain the plot in Figure C.1. As with the six-state signal states, the threshold increases monotonically with n, gradually approaching $\frac{1}{5}$.

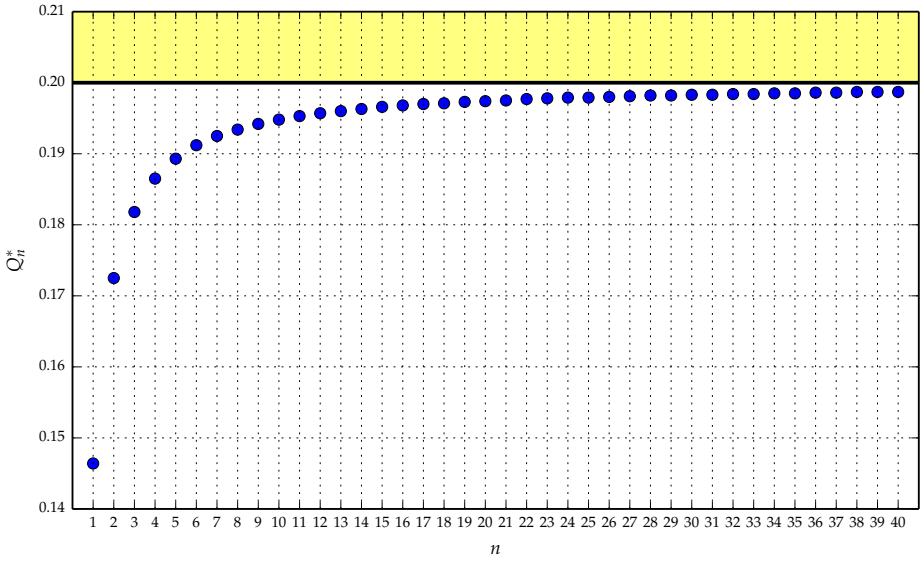


Figure C.1: Advantage distillation thresholds for the BB84 signal states from $n = 1$ to $n = 40$. Indicated in yellow is the gap.

Like in the analysis for the six-state signal states, we want to determine the threshold in the limit $n \to \infty$ and confirm that it is $\frac{1}{5}$. Similar to that analysis, it holds that as n increases q_0, q_3 vanish more quickly relative

to q_1, q_2, so that for large n the inequality (C.7) tends to $-4q_0q_1 + q_2^2 \leq 0$, which becomes after substituting the defintions of q_0, q_1, q_2 and simplifying

$$-4Q^n(1-Q)^n + (1-3Q+2x)^{2n} \leq 0. \tag{C.8}$$

Simplifying further leads to $(1-3Q+2x)^2 \leq 4^{\frac{1}{n}}Q(1-Q)$. Therefore, in the limit $n \to \infty$, we obtain $(1-3Q+2x)^2 \leq Q(1-Q)$. Simplifying this condition leads to

$$h_Q(x) := 4x^2 + (4-12Q)x + 1 - 7Q + 10Q^2 \leq 0. \tag{C.9}$$

This condition is necessary and sufficient for $\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}$ to be symmetrically extendable in the limit $n \to \infty$. We would like to determine, in this limit, the highest possible Q such that $\rho^{\tilde{A}\tilde{B}}_{Q,x,n}$ is *not* symmetrically extendable for all $0 \leq x \leq Q$. This means that we must determine the highest Q such that $h_Q(x) > 0$ for all $0 \leq x \leq Q$.

It holds that h_Q is a quadratic function of x and is convex (or "concave up", which is due to the fact that $h''_Q(x) = 8$ for all $0 \leq x \leq Q$). Also, its vertex is at $\frac{3}{2}Q - \frac{1}{2}$, which is negative for all $Q < \frac{1}{3}$, and the value of the vertex is $-Q + Q^2$. h_Q will be positive for all x if its vertex is positive, but the condition $-Q + Q^2 > 0$ leads to $Q < 0$ or $Q > 1$, neither of which are permissible. Therefore, in our interval of interest of $0 \leq Q \leq \frac{1}{2}$ the vertex of h_Q will be negative, which means that for F_Q to be positive for all $0 \leq x \leq Q$ both of the zeros of F_Q must be negative. The roots of F_Q are

$$\frac{-(4-12Q) \pm 4\sqrt{Q(1-Q)}}{8}. \tag{C.10}$$

The root with the negative sign is negative for all $0 \leq Q < \frac{1}{2}$, while negativity of the root with the positive sign leads to $4\sqrt{Q(1-Q)} < 4 - 12Q$, which has solution $Q < \frac{1}{5}$. Equivalently, the root with the positive sign is negative if and only if $h_Q(0)$ is positive, that is, when $1 - 7Q + 10Q^2 > 0$. This holds for $Q > \frac{1}{2}$, which is not permissible, and for $Q < \frac{1}{5}$, as before. This means that for all $Q \geq \frac{1}{5}$ there exists $x \in [0, Q]$ such that $\rho^{\tilde{A}\tilde{B}}_{Q,x,\mathcal{R}_n}$ is symmetrically extendable, meaning that symmetric extendability cannot be broken beyond $\frac{1}{5}$. We have thus used our framework to reproduce the known result that for the BB84 signal states advantage distillation cannot break the symmetric extendability of Alice and Bob's initial correlations beyond $\frac{1}{5}$.

Appendix D

Chapter 6 Proofs

Proposition D.1

For any simplex code $\mathcal{S}(n,d,m)$, the resulting state $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is diagonal in the m-dimensional Bell Basis (6.5).

PROOF: From (4.12), we have that the block $M_{Q,\mathcal{S}}^{(\underline{0}^n)}$ has off-diagonal elements $\left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}$ and diagonal elements $\left(\frac{1-Q}{2}\right)^n$, so that in general the elements of the $M_{Q,\mathcal{S}}^{(\underline{0}^n)}$ block are

$$\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\\ \ell,\ell}} = \left(\frac{1-Q}{2}\right)^n \left(\delta_{k,\ell} + (1-\delta_{k,\ell}) \left(\frac{1-Q}{2}\right)^{-d} \left(\frac{1-2Q}{2}\right)^d\right) \quad \forall\, 0 \leq k,\ell \leq m-1.$$

For $c \neq \underline{0}^n$, each block $M_{Q,\mathcal{S}}^{(c)}$ is diagonal since the strings of the set always have at least one common position with a 1, so that the condition $c \odot (P_k \oplus P_{k'}) = \underline{0}^n$—the condition for non-zero off-diagonal elements—is never satisfied.

Therefore, $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ has the form

$$\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}} = \underbrace{\sum_{k,\ell=0}^{m-1} \left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\\ \ell,\ell}} |k,k\rangle \langle \ell,\ell|}_{M_{Q,\mathcal{S}}^{(\underline{0}^n)}} + \sum_{c\neq\underline{0}^n} \underbrace{\sum_{(k,\ell)\in\mathcal{J}_c} \left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\ k,\ell}} |k,\ell\rangle \langle k,\ell|}_{M_{Q,\mathcal{S}}^{(c)},\ c\neq\underline{0}^n}. \tag{D.1}$$

Writing the first term of this expression in the m-dimensional Bell basis gives

$$\begin{aligned}
&\sum_{k,\ell=0}^{m-1}\sum_{\substack{a,b\\a',b'=0}}^{m-1}\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\\\ell,\ell}}|\Phi_{a,b}\rangle\ \underbrace{\langle\Phi_{a,b}|k,k\rangle}_{\frac{1}{\sqrt{m}}e^{-\frac{2\pi ibk}{m}}\delta_{k,k+a}}\ \underbrace{\langle\ell,\ell|\Phi_{a',b'}\rangle}_{\frac{1}{\sqrt{m}}e^{\frac{2\pi ib'\ell}{m}}\delta_{\ell,\ell+a'}}\ \langle\Phi_{a',b'}|\\
&=\sum_{k,\ell=0}^{m-1}\sum_{\substack{a,b\\a',b'=0}}^{m-1}\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\\\ell,\ell}}e^{-\frac{2\pi ibk}{m}}e^{\frac{2\pi ib'\ell}{m}}\delta_{a,0}\delta_{a',0}\,|\Phi_{a,b}\rangle\,\langle\Phi_{a',b'}|\\
&=\underbrace{\sum_{k,\ell=0}^{m-1}\sum_{b,b'=0}^{m-1}\frac{1}{m}\left(\frac{1-Q}{2}\right)^{n}\delta_{k,\ell}e^{-\frac{2\pi ibk}{m}}e^{\frac{2\pi ib'\ell}{m}}\,|\Phi_{0,b}\rangle\,\langle\Phi_{0,b'}|}_{①}\\
&\qquad+\underbrace{\sum_{k,\ell=0}^{m-1}\sum_{b,b'=0}^{m-1}\frac{1}{m}\left(\frac{1-Q}{2}\right)^{n-d}\left(\frac{1-2Q}{2}\right)^{d}(1-\delta_{k,\ell})e^{-\frac{2\pi ibk}{m}}e^{\frac{2\pi ib'\ell}{m}}\,|\Phi_{0,b}\rangle\,\langle\Phi_{0,b'}|}_{②}.
\end{aligned}$$

Now,

$$①=\sum_{b,b'=0}^{m-1}\frac{1}{m}\left(\frac{1-Q}{2}\right)^{n}\underbrace{\left(\sum_{k=0}^{m-1}e^{\frac{2\pi i}{m}(b-b')k}\right)}_{m\delta_{b,b'}}|\Phi_{0,b}\rangle\,\langle\Phi_{0,b'}|=\sum_{b=0}^{m-1}\left(\frac{1-Q}{2}\right)^{n}|\Phi_{0,b}\rangle\,\langle\Phi_{0,b}|,$$

and

$$\begin{aligned}
②&=\sum_{k,\ell=0}^{m-1}\sum_{b,b'=0}^{m-1}\Bigg[\frac{1}{m}\left(\frac{1-Q}{2}\right)^{n-d}\left(\frac{1-2Q}{2}\right)^{d}e^{-\frac{2\pi ibk}{m}}e^{\frac{2\pi ib'\ell}{m}}\\
&\qquad-\frac{1}{m}\left(\frac{1-Q}{2}\right)^{n-d}\left(\frac{1-2Q}{2}\right)^{d}\delta_{k,\ell}e^{-\frac{2\pi ibk}{m}}e^{\frac{2\pi ib'\ell}{m}}\Bigg]\,|\Phi_{0,b}\rangle\,\langle\Phi_{0,b'}|\\
&=\left(\frac{1-Q}{2}\right)^{n-d}\left(\frac{1-2Q}{2}\right)^{d}|\Phi_{0,0}\rangle\,\langle\Phi_{0,0}|-\sum_{b=0}^{m-1}\left(\frac{1+p}{4}\right)^{n-d}\left(\frac{1-2Q}{2}\right)^{d}|\Phi_{0,b}\rangle\,\langle\Phi_{0,b}|
\end{aligned}$$

Therefore, the first term of (D.1) is equal to

$$\sum_{b=0}^{m-1}\left[\left(\frac{1-Q}{2}\right)^{n}+(\delta_{b,0}m-1)\left(\frac{1-2Q}{2}\right)^{d}\left(\frac{1-Q}{2}\right)^{n-d}\right]|\Phi_{0,b}\rangle\,\langle\Phi_{0,b}|.$$

The second term of (D.1) can be written as

$$\sum_{c\neq\underline{0}^{n}}\sum_{(k,\ell)\in\mathcal{I}_{c}}\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k,\ell}}|k,\ell\rangle\,\langle k,\ell|=\sum_{\substack{k,\ell=0\\k\neq\ell}}^{m-1}\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k,\ell}}|k,\ell\rangle\,\langle k,\ell|.$$

Writing this in the Bell basis, and using $\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k,\ell}} = \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d}$, gives

$$\begin{aligned}
\sum_{\substack{k,\ell=0\\k\neq\ell}}^{m-1} \left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k,\ell}} |k,\ell\rangle\langle k,\ell| &= \sum_{\substack{k,\ell=0\\k\neq\ell}}^{m-1} \sum_{\substack{a,b\\a',b'=0}}^{m-1} \left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k,\ell}} |\Phi_{a,b}\rangle \underbrace{\langle\Phi_{a,b}|k,\ell\rangle}_{\frac{1}{\sqrt{m}}e^{-\frac{2\pi i b k}{m}}\delta_{\ell,k+a}} \underbrace{\langle k,\ell|\Phi_{a',b'}\rangle}_{\frac{1}{\sqrt{m}}e^{\frac{2\pi i b' k}{m}}\delta_{\ell,k+a'}} \langle\Phi_{a',b'}| \\
&= \sum_{\substack{k,\ell=0\\k\neq\ell}}^{m-1} \sum_{b,b'=0}^{m-1} \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \frac{1}{m} e^{\frac{2\pi i}{m}(b'-b)k} |\Phi_{\ell-k,b}\rangle\langle\Phi_{\ell-k,b'}| \\
&= \sum_{\ell'=1}^{m-1} \sum_{k=0}^{m-1} \sum_{b,b'=0}^{m-1} \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \frac{1}{m} e^{\frac{2\pi i}{m}(b'-b)k} |\Phi_{\ell',b}\rangle\langle\Phi_{\ell',b'}| \\
&= \sum_{\ell'=1}^{m-1} \sum_{b,b'=0}^{m-1} \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \delta_{b,b'} |\Phi_{\ell',b}\rangle\langle\Phi_{\ell',b'}| \\
&= \sum_{\ell'=1}^{m-1} \sum_{b=0}^{m-1} \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} |\Phi_{\ell',b}\rangle\langle\Phi_{\ell',b}| .
\end{aligned}$$

Therefore,

$$\begin{aligned}
\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}} = \sum_{b=0}^{m-1} \left[\left(\frac{1-Q}{2}\right)^n + (\delta_{b,0}m - 1) \left(\frac{1-2Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} \right] |\Phi_{0,b}\rangle\langle\Phi_{0,b}| \\
+ \sum_{a=1}^{m-1} \sum_{b=0}^{m-1} \left(\frac{Q}{2}\right)^d \left(\frac{1-Q}{2}\right)^{n-d} |\Phi_{a,b}\rangle\langle\Phi_{a,b}| ,
\end{aligned} \tag{D.2}$$

that is, $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is diagonal in the Bell basis, as required. ■

Proposition D.2

For any simplex code $\mathcal{S}(n,d,m)$, the state $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is separable for all $Q \geq \frac{1}{3}$.

PROOF: We first observe from (D.1) that the block $M_{Q,\mathcal{S}}^{(\underline{0}^n)}$ becomes diagonal after taking the partial transpose, while the matrix elements previously corresponding to off-diagonal elements of $M_{Q,\mathcal{S}}^{(\underline{0}^n)}$ now become off-diagonal elements of the blocks $M_{Q,\mathcal{S}}^{(c)}$ with $c \neq \underline{0}^n$. All such blocks contain 2×2 sub-blocks supported on orthogonal subspaces that can be diagonalized by the Hadamard matrix H defined in (6.1). In fact, all such sub-blocks are the same. This means that the distinct eigenvalues of $\left(\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}\right)^{\mathsf{T}_{\tilde{B}}}$ are

$$\begin{gathered}
\left(\frac{1-Q}{2}\right)^n, \\
\left(\frac{1-Q}{2}\right)^{n-d} \left(\left(\frac{Q}{2}\right)^d + \left(\frac{1-2Q}{2}\right)^d \right), \\
\left(\frac{1-Q}{2}\right)^{n-d} \left(\left(\frac{Q}{2}\right)^d - \left(\frac{1-2Q}{2}\right)^d \right).
\end{gathered}$$

The first and second eigenvalues are never negative, while negativity of the third eigenvalue easily leads to the condition $Q < \frac{1}{3}$, which is the range of values for which $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is *entangled*. $\rho_{Q,\mathcal{S}}^{\tilde{A}\tilde{B}}$ is therefore separable for all $Q \geq \frac{1}{3}$. Since the simplex code $\mathcal{S}$ was arbitrary, the proof is complete. ■

Lemma D.3

For all simplex codes, the roots of $\Lambda_{0,1}$ and $\Lambda_{1,0}$ are equal in the interval $0 \leq Q \leq \frac{1}{2}$.

PROOF: Let $\lambda^*_{0,0}$, $\lambda^*_{0,1}$ and $\lambda^*_{1,0}$ be the eigenvalues of $\rho^{\tilde{A}\tilde{B}}_{Q,S}$ at the value of Q for which $\Lambda_{1,0} = 0$. Let $\Lambda^*_{0,1}$ be the eigenvalue $\Lambda_{0,1}$ evaluated at that same value. From the expression of $\Lambda_{1,0}$ in (6.19), $\Lambda_{1,0} = 0$ gives us

$$\frac{1}{m} + \frac{-\frac{1}{m}\lambda^*_{0,0} - \frac{m-1}{m}\lambda^*_{0,1} + \lambda^*_{1,0}}{2\sqrt{\lambda^*_{0,1}\lambda^*_{0,0}} + (m-2)\lambda^*_{0,1} + m(m-1)\lambda^*_{1,0}} = 0.$$

This leads to

$$\begin{aligned}
&\lambda^*_{0,0} + (m-1)\lambda^*_{0,1} - m\lambda^*_{1,0} = 2\sqrt{\lambda^*_{0,1}\lambda^*_{0,0}} + (m-2)\lambda^*_{0,1} + m(m-1)\lambda^*_{1,0} \\
\Rightarrow\ &\lambda^*_{0,0} - 2\sqrt{\lambda^*_{0,1}\lambda^*_{0,0}} + \lambda^*_{0,1} = m^2\lambda^*_{1,0} \\
\Rightarrow\ &\left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)^2 = m^2\lambda^*_{1,0} \\
\Rightarrow\ &\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}} = \pm m\sqrt{\lambda^*_{1,0}}.
\end{aligned}$$

Since $\lambda_{0,0} \geq \lambda_{0,1}$ for all simplex codes for all $0 \leq Q \leq \frac{1}{2}$, we have that $\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}} = m\sqrt{\lambda^*_{1,0}}$. Now,

$$\Lambda^*_{0,1} = 1 - \frac{\lambda^*_{0,0} - \lambda^*_{0,1}}{2\sqrt{\lambda^*_{1,0}\lambda^*_{0,0}} + 2(m-1)\sqrt{\lambda^*_{1,0}\lambda^*_{0,1}} + m(m-2)\lambda^*_{1,0}},$$

and using $\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}} = m\sqrt{\lambda^*_{1,0}}$, we obtain

$$\begin{aligned}
2\sqrt{\lambda^*_{1,0}\lambda^*_{0,0}} + 2(m-1)\sqrt{\lambda^*_{1,0}\lambda^*_{0,1}} + m(m-2)\lambda^*_{1,0} &= 2\sqrt{\lambda^*_{1,0}}\left(\sqrt{\lambda^*_{0,0}} + (m-1)\sqrt{\lambda^*_{0,1}} + \frac{1}{2}m(m-2)\sqrt{\lambda^*_{1,0}}\right) \\
&= \frac{2}{m}\left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)\left(\sqrt{\lambda^*_{0,0}} + (m-1)\sqrt{\lambda^*_{0,1}} + \frac{1}{2}(m-2)\left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)\right) \\
&= \frac{2}{m}\left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)\left(\sqrt{\lambda^*_{0,0}} + m\sqrt{\lambda^*_{0,1}} - \sqrt{\lambda^*_{0,1}} + \frac{m}{2}\sqrt{\lambda^*_{0,0}} - \frac{m}{2}\sqrt{\lambda^*_{0,1}} - \sqrt{\lambda^*_{0,0}} + \sqrt{\lambda^*_{0,1}}\right) \\
&= \frac{2}{m}\left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)\frac{m}{2}\left(\sqrt{\lambda^*_{0,0}} + \sqrt{\lambda^*_{0,1}}\right) \\
&= \left(\sqrt{\lambda^*_{0,0}} - \sqrt{\lambda^*_{0,1}}\right)\left(\sqrt{\lambda^*_{0,0}} + \sqrt{\lambda^*_{0,1}}\right) \\
&= \lambda^*_{0,0} - \lambda^*_{0,1}.
\end{aligned}$$

Therefore,

$$\Lambda^*_{0,1} = 1 - \frac{\lambda^*_{0,0} - \lambda^*_{0,1}}{\lambda^*_{0,0} - \lambda^*_{0,1}} = 0,$$

as required. ■

Appendix E

Linear Codes

We consider here general linear codes, which we recall from §4.1 form a (linear) subspace of the vector space of the n-bit strings, that is, they are closed under the bitwise-XOR addition $\oplus$. We will let $\mathcal{P}$ denote an arbitrary linear code of size 2^m for some $m < n$, and we will consider the two cases of Alice and Bob both post-selecting on $\mathcal{P}$ and of only Bob post-selecting on $\mathcal{P}$. The corresponding filtered states have a much more general structure than the states from Chapters 5 and 6, and there are no known analytical results about their symmetric extendability. In particular, there is no analytical approach to determining the thresholds $Q^*_{\mathcal{P}}$, and the channel Tr_{E_2} alone might not construct a symmetric extension of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}$ at those thresholds. Therefore, the special map $\mathcal{N} \circ \mathrm{Tr}_{E_2}$ might not construct a symmetric extension of the filtered states throughout the gap. Nevertheless, we will determine the structure of the filtered states and determine the eigenvalues of $J(\mathcal{N})$ so that it is possible to determine whether or not the special map will work for a given linear code.

Throughout this chapter, we will let $\mathrm{Bin}_n(k)$ stand for the n-bit binary representation of the decimal number k. For example, $\mathrm{Bin}_3(5) = 101$. Also, for non-negative integers x and y, we will let $x \oplus y$ denote the unique non-negative integer satisfying $\mathrm{Bin}_n(x \oplus y) = \mathrm{Bin}_n(x) \oplus \mathrm{Bin}_n(y)$, where n is the smallest block size such that both x and y can be represented as n-bit binary strings.

E.1 Post-Selection by Alice and Bob

When Alice and Bob post-select on the same linear code $\mathcal{P}$ of size 2^m for $m < n$, it holds due the closure of linear codes that the sets $\mathcal{C}$ and $\mathcal{I}_c$ defined in (4.13) and (4.16), respectively, satisfy:

1. $\mathcal{C} = \mathcal{P}$;
2. $|\mathcal{I}_c| = 2^m$ for all $c \in \mathcal{C}$.

In other words, each block $M^{(c)}_{Q,\mathcal{P}}$ can be labelled by a codeword in $\mathcal{P}$, and the size of each such block is $2^m \times 2^m$. Furthermore, since $d_{\tilde{A}} = d_{\tilde{B}} = 2^m$, we can think of the filtered state $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}} \in \mathrm{D}(\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^m})$ as residing in the space $\mathrm{D}\Big(\underbrace{(\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2)}_{m \text{ times}} \otimes \underbrace{(\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2)}_{m \text{ times}}\Big)$ of a pair of m qubits through the isomorphism $|a, b\rangle \leftrightarrow |\mathrm{Bin}_m(a), \mathrm{Bin}_m(b)\rangle$ for all $0 \leq a, b \leq 2^m - 1$. In other words, after post-selection, Alice and Bob effectively hold m qubits instead of n that they had initially.

For convenience, we will always assume that the codewords in $\mathcal{P}$ are ordered such that

$$P_i \oplus P_j = P_{i\oplus j} \quad \forall\, 0 \leq i,j \leq 2^m - 1. \tag{E.1}$$

With this ordering, the set $\mathcal{I}_{P_k} = \{(i,j) | P_i \oplus P_j = P_k\}$ can be written as $\mathcal{I}_{P_k} = \{(\ell, \ell\oplus k) : 0 \leq \ell \leq 2^m - 1\}$ for all $0 \leq k \leq 2^m - 1$. This ordering of $\mathcal{P}$ can be achieved in the following way: pick any (ordered) basis $\{B_1, B_2, \ldots, B_m\}$ of $\mathcal{P}$. We then let

$$P_k = (\mathrm{Bin}_m(k))_1 B_1 \oplus (\mathrm{Bin}_m(k))_2 B_2 \oplus \cdots \oplus (\mathrm{Bin}_m(k))_m B_m \quad \forall\, 0 \leq k \leq 2^m - 1.$$

Then, it holds that

$$\begin{aligned} P_{k\oplus\ell} &= (\mathrm{Bin}_m(k\oplus\ell))_1 B_1 \oplus (\mathrm{Bin}_m(k\oplus\ell))_2 B_2 \oplus \cdots \oplus (\mathrm{Bin}_m(k\oplus\ell))_m B_m \\ &= ((\mathrm{Bin}_m(k))_1 \oplus (\mathrm{Bin}_m(\ell))_1)\, B_1 \oplus ((\mathrm{Bin}_m(k))_2 \oplus (\mathrm{Bin}_m(\ell))_2)\, B_2 \oplus \cdots \oplus ((\mathrm{Bin}_m(k))_m \oplus (\mathrm{Bin}_m(\ell))_m)\, B_m \\ &= (\mathrm{Bin}_m(k))_1 B_1 \oplus (\mathrm{Bin}_m(k))_2 B_2 \oplus \cdots \oplus (\mathrm{Bin}_m(k))_m B_m \\ &\quad \oplus (\mathrm{Bin}_m(\ell))_1 B_1 \oplus (\mathrm{Bin}_m(\ell))_2 B_2 \oplus \cdots \oplus (\mathrm{Bin}_m(\ell))_m B_m \\ &= P_k \oplus P_\ell, \end{aligned}$$

as required.

Proposition E.1

For any linear code $\mathcal{P}$, the resulting filtered state $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}$ satisfies

$$\left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k\oplus j,\ell\oplus j \\ k'\oplus j,\ell'\oplus j}} = \left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k,\ell \\ k',\ell'}} \quad \forall\, 0 \leq k,\ell,k',\ell',j \leq 2^m - 1. \tag{E.2}$$

In particular, the state can be written as

$$\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}} = \sum_{j=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k,k\oplus j \\ \ell,\ell\oplus j}} |k, k\oplus j\rangle \langle \ell, \ell\oplus j|\,.$$

Additionally, the matrix V such that $V\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}V^\dagger = \bigoplus_{k=0}^{2^m-1} M^{(P_k)}_{Q,\mathcal{P}} = \sum_{k=0}^{2^m-1} |k\rangle\langle k| \otimes M^{(P_k)}_{Q,\mathcal{P}}$ can be written as

$$V = \sum_{k,\ell=0}^{2^m-1} |k,\ell\rangle \langle \ell, \ell\oplus k|\,.$$

PROOF: The fact that $\left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k\oplus j,\ell\oplus j \\ k'\oplus j,\ell'\oplus j}} = \left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k,\ell \\ k',\ell'}}$ follows from the definition of the matrix elements of $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}$ as written in (4.12) and from the fact that $P_{k\oplus\ell} = P_k \oplus P_\ell$.

Next, as described above, by identifying the blocks $M^{(c)}_{Q,\mathcal{P}}$ with the codewords of $\mathcal{P}$, and using the fact that $\mathcal{I}_{P_j}$ can be written as $\mathcal{I}_{P_j} = \{(\ell, \ell\oplus j) : 0 \leq \ell \leq 2^m - 1\}$ for all $0 \leq j \leq 2^m - 1$, we have by (4.15)

$$\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}} = \sum_{j=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{P}}\right)_{\substack{k,k\oplus j \\ \ell,\ell\oplus j}} |k, k\oplus j\rangle \langle \ell, \ell\oplus j|\,,$$

as required.

Finally, letting $V = \sum_{k,\ell=0}^{2^m-1} |k, \ell\rangle \langle \ell, \ell \oplus k|$, we get

$$\begin{aligned}
V\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}V^\dagger &= \sum_{\substack{i,j\\ i',j'=0}}^{2^m-1} \sum_{\ell'=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\oplus\ell'\\ \ell,\ell\oplus\ell'}} |i,j\rangle \langle j, j\oplus i|k, k\oplus\ell'\rangle \langle \ell, \ell\oplus\ell'|j', j'\oplus i'\rangle \langle i', j'| \\
&= \sum_{\substack{i,j\\ i',j'=0}}^{2^m-1} \sum_{\ell'=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\oplus\ell'\\ \ell,\ell\oplus\ell'}} \delta_{j,k}\delta_{j\oplus i,k\oplus\ell'}\delta_{\ell,j'}\delta_{\ell\oplus\ell',j'\oplus i'} |i,j\rangle \langle i', j'| \\
&= \sum_{i,i'=0}^{2^m-1} \sum_{\ell'=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\oplus\ell'\\ \ell,\ell\oplus\ell'}} \underbrace{\delta_{k\oplus i,k\oplus\ell'}}_{\delta_{i,\ell'}\ \forall k} \underbrace{\delta_{\ell\oplus\ell',\ell\oplus i'}}_{\delta_{i',\ell'}\ \forall \ell} |i,k\rangle \langle i', \ell| \\
&= \sum_{i,i'=0}^{2^m-1} \sum_{k,\ell=0}^{2^m-1} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\oplus i\\ \ell,\ell\oplus i}} \delta_{i,i'} |i,k\rangle \langle i', \ell| \\
&= \sum_{i=0}^{2^m-1} |i\rangle \langle i| \otimes \underbrace{\sum_{k,\ell=0}^{2^m-1} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,k\oplus i\\ \ell,\ell\oplus i}} |k\rangle \langle \ell|}_{M_{Q,\mathcal{P}}^{(P_i)}} \\
&= \sum_{i=0}^{2^m-1} |i\rangle \langle i| \otimes M_{Q,\mathcal{P}}^{(P_i)},
\end{aligned}$$

as required. ■

The matrix elements of the blocks $M_{Q,\mathcal{P}}^{(P_k)}$ from the previous proposition are equal to

$$\left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{\ell\\ \ell'}} = \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{\ell,\ell\oplus k\\ \ell',\ell'\oplus k}} \quad \forall\, 0 \le \ell, \ell', k \le 2^m - 1. \tag{E.3}$$

Proposition E.2

For all $0 \le k \le 2^m - 1$, the blocks $M_{Q,\mathcal{P}}^{(P_k)}$ satisfy

$$\left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{\ell\\ \ell'}} = \left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{\ell\oplus j\\ \ell'\oplus j}} \quad \forall\, 0 \le \ell, \ell', j \le 2^m - 1. \tag{E.4}$$

PROOF: Follows from (E.2) and (E.3). ■

The proposition above states that the blocks $M_{Q,\mathcal{P}}^{(P_k)}$ are essentially "translation-invariant" with respect to the addition $\oplus$. They are fully specified by their first row, since

$$\left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{\ell\\ \ell'}} = \left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{\ell\oplus\ell\\ \ell'\oplus\ell}} = \left(M_{Q,\mathcal{P}}^{(P_k)}\right)_{\substack{0\\ \ell\oplus\ell'}} \quad \forall\, 0 \le \ell, \ell' \le 2^m - 1.$$

The following useful lemma tells us how to diagonalize any matrix A with such a translation-invariance property.

Lemma E.3

Let A be a $2^m \times 2^m$ matrix for some $m \geq 1$ satisfying

$$A_{\ell\ \ell'} = A_{\substack{\ell\oplus j \\ \ell'\oplus j}} \quad \forall\, 0 \leq \ell, \ell', j \leq 2^m - 1. \tag{E.5}$$

It holds that

$$H^{\otimes m} A H^{\otimes m} = D,$$

where H is the normalized Hadamard matrix $\tilde{H}$ from (6.1),

$$H = \frac{1}{\sqrt{2}}\tilde{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{E.6}$$

and D is the diagonal matrix of eigenvalues $\{\lambda_k\}_{k=0}^{2^m-1}$,

$$\lambda_k \equiv D_{k\ k} = \sum_{\ell'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(\ell')\cdot\mathrm{Bin}_m(k)} A_{0\ \ell'} \quad \forall\, 0 \leq k \leq 2^m - 1. \tag{E.7}$$

PROOF: Writing H as

$$H = \frac{1}{\sqrt{2}} \sum_{i,j=0}^{1} (-1)^{ij} |i\rangle \langle j| ,$$

we have that

$$H^{\otimes m} = \frac{1}{(\sqrt{2})^m} \sum_{\ell,\ell'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(\ell')} |\ell\rangle \langle \ell'| , \tag{E.8}$$

where we recall the dot product $\cdot$ on binary strings defined in §4.1. Since $A_{\ell\ \ell'} = A_{\substack{\ell\oplus j \\ \ell'\oplus j}}$ for all $0 \leq j \leq 2^m - 1$, we can write $A_{\ell\ \ell'} = A_{\substack{0 \\ \ell\oplus\ell'}}$ for all $0 \leq \ell, \ell' \leq 2^m - 1$, so that

$$A = \sum_{\ell,\ell'=0}^{2^m-1} A_{\substack{0 \\ \ell\oplus\ell'}} |\ell\rangle \langle \ell'| .$$

Now, the rows $\{|v_k\rangle\}_{k=0}^{2^m-1}$ of $H^{\otimes m}$, defined by

$$|v_k\rangle = H^{\otimes m} |k\rangle = \frac{1}{(\sqrt{2})^m} \sum_{\ell=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(k)} |\ell\rangle ,$$

satisfy

$$\begin{aligned} A|v_k\rangle &= \sum_{j,j',\ell=0}^{2^m-1} A_{\substack{0 \\ j\oplus j'}} \frac{1}{(\sqrt{2})^m} (-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(k)} |j\rangle \underbrace{\langle j'|\ell\rangle}_{\delta_{j',\ell}} \\ &= \sum_{j=0}^{2^m-1} \left(\sum_{\ell=0}^{2^m-1} A_{\substack{0 \\ j\oplus\ell}} \frac{1}{(\sqrt{2})^m} (-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(k)} \right) |j\rangle \\ &= \sum_{j=0}^{2^m-1} \left(\sum_{\ell'=0}^{2^m-1} \frac{1}{(\sqrt{2})^m} A_{0\ \ell'} (-1)^{\mathrm{Bin}_m(\ell'\oplus j)\cdot\mathrm{Bin}_m(k)} \right) |j\rangle . \end{aligned}$$

Then, since

$$\mathrm{Bin}_m(\ell' \oplus j) \cdot \mathrm{Bin}_m(k) = (\mathrm{Bin}_m(\ell') \oplus \mathrm{Bin}_m(j)) \cdot \mathrm{Bin}_m(k) = \mathrm{Bin}_m(\ell') \cdot \mathrm{Bin}_m(k) + \mathrm{Bin}_m(j) \cdot \mathrm{Bin}_m(k),$$

where the addition $+$ in the above equation is modulo 2, we get that

$$\begin{aligned} A\,|v_k\rangle &= \sum_{j=0}^{2^m-1} \left(\sum_{\ell'=0}^{2^m-1} A_{\substack{0\\ \ell'}} (-1)^{\mathrm{Bin}_m(\ell')\cdot\mathrm{Bin}_m(k)} \right) \frac{1}{(\sqrt{2})^m} (-1)^{\mathrm{Bin}_m(j)\cdot\mathrm{Bin}_m(k)}\,|j\rangle \\ &= \underbrace{\left(\sum_{\ell'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(\ell')\cdot\mathrm{Bin}_m(k)} A_{\substack{0\\ \ell'}} \right)}_{\lambda_k} \underbrace{\left(\sum_{j=0}^{2^m-1} \frac{1}{(\sqrt{2})^m} (-1)^{\mathrm{Bin}_m(j)\cdot\mathrm{Bin}_m(k)}\,|j\rangle \right)}_{|v_k\rangle} \\ &= \lambda_k\,|v_k\rangle\,, \end{aligned}$$

which means that $H^{\otimes m} A H^{\otimes m} = D$, as required. ■

By using from (E.8) the fact that

$$(-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(\ell')} = \left(\tilde{H}^{\otimes m}\right)_{\substack{\ell\\ \ell'}} \quad \forall\, 0 \le \ell, \ell' \le 2^m - 1,$$

observe that the eigenvalues (E.7) can be written as

$$\vec{\lambda} = \tilde{H}^{\otimes m} \vec{A}, \quad \vec{\lambda} := \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{2^m-1} \end{pmatrix}, \; \vec{A} := \begin{pmatrix} A_{\substack{0\\ 0}} \\ A_{\substack{0\\ 1}} \\ \vdots \\ A_{\substack{0\\ 2^m-1}} \end{pmatrix}.$$

An expression of this type is called a *Hadamard transform*. Therefore, the eigenvalues of any matrix A with the translation-invariance property (E.5) are simply given by the Hadamard transform of the first row of the matrix.

Using the fact that the blocks of $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ have this translation-invariance property, and the previous lemma, we obtain the following.

Theorem E.4

For any linear code $\mathcal{P}$, the resulting filtered state $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ is diagonalized by WV, where

$$V = \sum_{k,\ell=0}^{2^m-1} |k,\ell\rangle\langle\ell,\ell\oplus k|, \quad W = \bigoplus_{k=0}^{2^m-1} H^{\otimes m}.$$

The eigenvectors $\{|v_{a,b}\rangle\}_{a,b=0}^{2^m-1}$ of $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ are

$$|v_{a,b}\rangle = \frac{1}{(\sqrt{2})^m} \sum_{\ell'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell')} \left|\ell', \ell'\oplus a\right\rangle \quad \forall\, 0 \le a,b \le 2^m-1, \tag{E.9}$$

and the corresponding eigenvalues are

$$\lambda_{a,b} = \sum_{\ell'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell')} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{0,a\\ \ell',\ell'\oplus a}} \quad \forall\, 0 \le a,b \le 2^m-1. \tag{E.10}$$

Proposition E.5

The eigenvectors $\{|v_{k,\ell}\rangle\}_{k,\ell=0}^{2^m-1}$ of $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ in (E.9) have the following properties:

1. $|v_{0,0}\rangle = |\Phi_{0,0}\rangle$, where $|\Phi_{0,0}\rangle$ was defined in (6.6).
2. For all $0 \le a,b \le 2^m-1$,

   $$|v_{a,b}\rangle = \left(\mathbb{1}_{\mathbb{C}^{2^m}} \otimes U(a)V(b)\right)|v_{0,0}\rangle,$$

   where $U(a) \in \mathrm{U}(\mathbb{C}^{2^m})$ and $V(b) \in \mathrm{U}(\mathbb{C}^{2^m})$ are unitary operators defined by

   $$U(a)|\ell\rangle = |\ell\oplus a\rangle \quad \forall\, 0 \le \ell,a \le 2^m-1 \tag{E.11}$$

   and

   $$V(b)|\ell\rangle = (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell)}|\ell\rangle \quad \forall\, 0 \le \ell,b \le 2^m-1. \tag{E.12}$$

3. $\mathrm{Tr}_{\tilde{B}}\left[|v_{k,\ell}\rangle\langle v_{k,\ell}|\right] = \frac{1}{2^m}\mathbb{1}_{\tilde{A}}$ for all $0 \le k,\ell \le 2^m-1$;
4. Viewed as vectors in the space of a pair of m qubits,

   $$|v_{k,\ell}\rangle = W(\left|\beta_{x_1,y_1}\right\rangle \otimes \left|\beta_{x_2,y_2}\right\rangle \otimes \cdots \otimes \left|\beta_{x_m,y_m}\right\rangle),$$

   where $x = x_1x_2\cdots x_m := \mathrm{Bin}_m(k)$, $y = y_1y_2\cdots y_m := \mathrm{Bin}_m(\ell)$,

   $$|\beta_{0,0}\rangle := \left|\Phi^+\right\rangle, \quad |\beta_{0,1}\rangle := \left|\Phi^-\right\rangle, \quad |\beta_{1,0}\rangle = \left|\Psi^+\right\rangle, \quad |\beta_{1,1}\rangle := \left|\Psi^-\right\rangle \tag{E.13}$$

   are the two-qubit Bell states from (2.22), and W is the operator on m pairs of qubits from (4.4). Furthermore, viewed as operators on the space of a pair of m qubits,

   $$U(k) = (\sigma_x)^x \quad \text{and} \quad V(\ell) = (\sigma_z)^y \quad \forall\, 0 \le k,\ell \le 2^m-1.$$

PROOF:

1. Follows from substitution.

2. Follows from substitution.

3. We have for all $0 \leq k, \ell \leq 2^m - 1$

$$|v_{k,\ell}\rangle\langle v_{k,\ell}| = \sum_{j,j'=0}^{2^m-1} \frac{1}{2^m}(-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j)+\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j')} |j, j\oplus k\rangle\langle j', j'\oplus k|,$$

   so that

$$\begin{aligned}
\mathrm{Tr}_{\tilde{B}}\left[|v_{k,\ell}\rangle\langle v_{k,\ell}|\right] &= \sum_{j,j'=0}^{2^m-1} \frac{1}{2^m}(-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j)+\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j')}\delta_{j\oplus k,j'\oplus k}\,|j\rangle\langle j'| \\
&= \frac{1}{2^m}\sum_{j=0}^{2^m-1} \underbrace{(-1)^{\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j)+\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(j)}}_{1\ \forall j} |j\rangle\langle j| \\
&= \frac{1}{2^m}\sum_{j=0}^{2^m-1} |j\rangle\langle j| \\
&= \frac{1}{2^m}\mathbb{1}_{\tilde{A}},
\end{aligned}$$

   as required.

4. This follows from the isomorphism $|k, \ell\rangle \leftrightarrow |x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m\rangle$ and the fact that

$$|\beta_{x,y}\rangle = \frac{1}{\sqrt{2}}\sum_{\ell=0}^{1}(-1)^{\ell y}|\ell, \ell\oplus x\rangle \quad \forall\, 0 \leq x, y \leq 1. \quad \blacksquare$$

The last part of the proposition above tells us that the states $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ are unitarily-equivalent to *multi-qubit Bell-diagonal states*. The symmetric extendability of such states was examined extensively in [Myh10] using the symmetries of the states but without reaching a full resolution in terms of some necessary and sufficient criteria except in the case $m = 1$, which is covered by (3.2).

Proposition E.6

The states $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ are invariant under $U(a)V(b) \otimes U(a)V(b)$ for all $0 \leq a, b \leq 2^m - 1$, that is,

$$(U(a)V(b) \otimes U(a)V(b))\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}(U(a)V(b) \otimes U(a)V(b))^\dagger = \rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}} \quad \forall\, 0 \leq a, b \leq 2^m - 1.$$

PROOF: First, for any $0 \le a, a', b, b', k, \ell \le 2^m - 1$, it holds that

$$\begin{aligned}
&(U(a)V(a') \otimes U(b)V(b')) \left|v_{k,\ell}\right\rangle \\
&= \frac{1}{(\sqrt{2})^m} \sum_{j=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(j)\cdot\mathrm{Bin}_m(\ell)} (-1)^{\mathrm{Bin}_m(a')\cdot\mathrm{Bin}_m(j)} (-1)^{\mathrm{Bin}_m(b')\cdot\mathrm{Bin}_m(j\oplus k)} \left|j\oplus a, j\oplus k\oplus b\right\rangle \\
&= \frac{1}{(\sqrt{2})^m} \sum_{j=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(j)\cdot\mathrm{Bin}_m(\ell\oplus a'\oplus b')} (-1)^{\mathrm{Bin}_m(b')\cdot\mathrm{Bin}_m(k)} \left|j\oplus a, j\oplus k\oplus b\right\rangle \\
&= (-1)^{\mathrm{Bin}_m(b')\cdot\mathrm{Bin}_m(k)} (-1)^{\mathrm{Bin}_m(a)\cdot\mathrm{Bin}_m(\ell\oplus a'\oplus b')} \underbrace{\frac{1}{(\sqrt{2})^m} \sum_{j'=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(j')\cdot\mathrm{Bin}_m(\ell\oplus a'\oplus b')} \left|j', j'\oplus k\oplus b\right\rangle}_{\left|v_{k\oplus a\oplus b,\ell\oplus a'\oplus b'}\right\rangle} \\
&= (-1)^{\mathrm{Bin}_m(b')\cdot\mathrm{Bin}_m(k)} (-1)^{\mathrm{Bin}_m(a)\cdot\mathrm{Bin}_m(\ell\oplus a'\oplus b')} \left|v_{k\oplus a\oplus b,\ell\oplus a'\oplus b'}\right\rangle .
\end{aligned}$$

Therefore,

$$\begin{aligned}
&(U(a)V(b) \otimes U(a)V(b)) \left|v_{k,\ell}\right\rangle \\
&\qquad = (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(k)} (-1)^{\mathrm{Bin}_m(a)\cdot\mathrm{Bin}_m(\ell)} \left|v_{k,\ell}\right\rangle \quad \forall\, 0 \le a, b, k, \ell \le 2^m - 1.
\end{aligned} \tag{E.14}$$

Writing $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ in its spectral decomposition therefore gives us

$$\begin{aligned}
&(U(a)V(b) \otimes U(a)V(b)) \rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}} (U(a)V(b) \otimes U(a)V(b))^\dagger \\
&= \sum_{k,\ell=0}^{2^m-1} \lambda_{k,\ell} (U(a)V(b) \otimes U(a)V(b)) \left|v_{k,\ell}\right\rangle \left\langle v_{k,\ell}\right| (U(a)V(b) \otimes U(a)V(b))^\dagger \\
&= \sum_{k,\ell=0}^{2^m-1} \lambda_{k,\ell} \left|v_{k,\ell}\right\rangle \left\langle v_{k,\ell}\right| \\
&= \rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}},
\end{aligned}$$

as required. ■

Both the block structure and the property (E.2) of $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ are implied by the proposition above since for all $0 \le k, \ell, k', \ell' \le 2^m - 1$

$$\begin{aligned}
\left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} &= \left\langle k,\ell\right| \rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}} \left|k',\ell'\right\rangle \\
&= \left\langle k,\ell\right| (U(a)V(b) \otimes U(a)V(b)) \rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}} (U(a)V(b) \otimes U(a)V(b))^\dagger \left|k',\ell'\right\rangle \\
&= (-1)^{\mathrm{Bin}_m(k\oplus\ell\oplus k'\oplus\ell')\cdot\mathrm{Bin}_m(b)} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k\oplus a,\ell\oplus a\\k'\oplus a,\ell'\oplus a}} \quad \forall\, 0 \le a, b \le 2^m - 1.
\end{aligned}$$

Taking $b = 0$ gives (E.2), while taking $a = 0$ gives

$$\left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} = (-1)^{\mathrm{Bin}_m(k\oplus\ell\oplus k'\oplus\ell')\cdot\mathrm{Bin}_m(b)} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} \quad \forall\, 0 \le b \le 2^m - 1.$$

This implies that

$$\left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} = \frac{1}{2^m} \underbrace{\sum_{b=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(k\oplus\ell\oplus k'\oplus\ell')\cdot\mathrm{Bin}_m(b)}}_{2^m\delta_{k\oplus\ell\oplus k'\oplus\ell',0} = 2^m\delta_{k\oplus\ell,k'\oplus\ell'}} \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} = \left(\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}\right)_{\substack{k,\ell\\k',\ell'}} \delta_{k\oplus\ell,k'\oplus\ell'},$$

which is precisely the statement of the block structure of the state from (4.12).

Now, by using (3.11), it holds that the Choi representation of $\mathcal{N}$ corresponding to the special map is

$$J(\mathcal{N}) = \sum_{k',\ell'=0}^{2^m-1} \left[\sum_{k,\ell=0}^{2^m-1} \left(\frac{\sum_{a,b=0}^{2^m-1} \frac{1}{2^m} \lambda_{a,b} (-1)^{\mathrm{Bin}_m(b\oplus\ell')\cdot\mathrm{Bin}_m(k)+\mathrm{Bin}_m(\ell)\cdot\mathrm{Bin}_m(a\oplus k')}}{\sum_{a',b'=0}^{2^m-1} \sqrt{\lambda_{a',b'}\lambda_{a'\oplus k,b'\oplus\ell}}} \right) \right] |v_{k',\ell'}\rangle \langle v_{k',\ell'}| , \tag{E.15}$$

where $\{\lambda_{a,b}\}_{a,b=0}^{2^m-1}$ and $\{|v_{k',\ell'}\rangle\}_{k',\ell'=0}^{2^m-1}$ are the eigenvalues and eigenvectors defined in (E.10) and (E.9), respectively. It is straightforward to show from this that $\mathcal{N}$ is trace-preserving.

As with the eigenvalues of $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$, we have that the eigenvalues $\{\Lambda_{u,v}\}_{u,v=0}^{2^m-1}$ of $J(\mathcal{N})$ can be written as the following Hadamard transform:

$$\vec{\Lambda} = H^{\otimes 2m} \vec{D},$$

where

$$\vec{\Lambda} = \begin{bmatrix} \Lambda_{0,0} \\ \Lambda_{0,1} \\ \vdots \\ \Lambda_{2^m-1,2^m-1} \end{bmatrix}, \quad \vec{D} = \begin{bmatrix} D_{0,0} \\ D_{0,1} \\ \vdots \\ D_{2^m-1,2^m-1} \end{bmatrix}, \quad D_{k,\ell} = \frac{(H^{\otimes 2m}\vec{\lambda})_{k,\ell}}{\left(H^{\otimes 2m}(H^{\otimes 2m}\sqrt{\vec{\lambda}} \circ H^{\otimes 2m}\sqrt{\vec{\lambda}})\right)_{\ell,k}}$$

and

$$\vec{\lambda} = \begin{bmatrix} \lambda_{0,0} \\ \lambda_{0,1} \\ \vdots \\ \lambda_{2^m-1,2^m-1} \end{bmatrix}, \quad \sqrt{\vec{\lambda}} = \begin{bmatrix} \sqrt{\lambda_{0,0}} \\ \sqrt{\lambda_{0,1}} \\ \vdots \\ \sqrt{\lambda_{2^m-1,2^m-1}} \end{bmatrix},$$

and $\circ$ is the Hadamard product defined in (4.25). The form of the denominator of the elements of $\vec{D}$ follows from the fact that

$$\sum_{a,b=0}^{2^m-1} \sqrt{\lambda_{a,b}\lambda_{a\oplus k,b\oplus\ell}} = 2^m \left(H^{\otimes 2m}(H^{\otimes 2m}\sqrt{\vec{\lambda}} \circ H^{\otimes 2m}\sqrt{\vec{\lambda}})\right)_{k,\ell},$$

which is straightforward to verify.

E.1.1 The Corresponding Channels

By using from Proposition E.5 the fact that

$$\mathrm{Tr}_{\tilde{B}}[|v_{k,\ell}\rangle \langle v_{k,\ell}|] = \frac{1}{2^m}\mathbb{1}_{\tilde{A}} \quad \forall\, 0 \le k,\ell \le 2^m - 1,$$

it holds that after normalization, $\mathrm{Tr}_{\tilde{B}}[\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}] = \frac{1}{2^m}\mathbb{1}_{\tilde{A}}$, so that the CP map $\Phi_{Q,\mathcal{P}} \in \mathrm{T}(\mathfrak{H}_{\tilde{A}}, \mathfrak{H}_{\tilde{B}})$ corresponding to $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ is (after normalization) in fact a channel. Its Kraus representation can be obtained from the following general fact.

Proposition E.7

Any map $\Phi : \mathrm{L}(\mathfrak{H}_A) \to \mathrm{L}(\mathfrak{H}_B)$ with $d_A = d_B = 2^m$ for some $m > 1$ such that its Choi representation is of the form

$$J(\Phi) = \sum_{a,b=0}^{2^m-1} p_{a,b} \left|v_{a,b}\right\rangle \left\langle v_{a,b}\right|$$

(that is, $J(\Phi)$ is diagonal in the basis $\{|v_{a,b}\rangle\}_{a,b=0}^{2^m-1}$) has Kraus representation

$$\Phi(X) = \frac{1}{2^m} \sum_{a,b=0}^{2^m-1} p_{a,b} (U(a)V(b))(X)(U(a)V(b))^\dagger$$

for all $X \in \mathrm{L}(\mathfrak{H}_A)$.

PROOF: Using the fact that

$$|v_{a,b}\rangle = (\mathbb{1}_A \otimes U(a)V(b)) |\Phi_{0,0}\rangle \quad \forall\, 0 \leq a, b \leq 2^m - 1$$

and that

$$|\Phi_{0,0}\rangle \langle\Phi_{0,0}| = \frac{1}{2^m} J(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)}) \Rightarrow (\mathbb{1}_A \otimes U(a)V(b)) J(\mathbb{1}_{\mathrm{L}(\mathfrak{H}_A)}) (\mathbb{1}_A \otimes U(a)V(b))^\dagger = J((U(a)V(b))(\cdot)(U(a)V(b))^\dagger),$$

we get that

$$J(\Phi) = \frac{1}{2^m} \sum_{a,b=0}^{2^m-1} p_{a,b} J((U(a)V(b))(\cdot)(U(a)V(b))^\dagger),$$

so that

$$\begin{aligned}
\Phi(X) &= \mathrm{Tr}_A \left[(X^\mathsf{T} \otimes \mathbb{1}_B) J(\Phi)\right] \\
&= \frac{1}{2^m} \sum_{a,b=0}^{2^m-1} p_{a,b} \underbrace{\mathrm{Tr}_A \left[(X^\mathsf{T} \otimes \mathbb{1}_B) J((U(a)V(b))(\cdot)(U(a)V(b))^\dagger)\right]}_{(U(a)V(b))(X)(U(a)V(b))^\dagger} \\
&= \frac{1}{2^m} \sum_{a,b=0}^{2^m-1} p_{a,b} (U(a)V(b))(X)(U(a)V(b))^\dagger,
\end{aligned}$$

as required. ■

By the proposition above, the filtered states $\rho_{Q,\mathcal{P}}^{\tilde{A}\tilde{B}}$ formed from a linear code $\mathcal{P}$ correspond to the following set of CP maps,

$$\Phi_{Q,\mathcal{P}}(X) = \sum_{k,\ell=0}^{2^m-1} \lambda_{k,\ell} \left(U(k)V(\ell)\right) X \left(U(k)V(\ell)\right)^\dagger \quad \forall\, X \in \mathrm{L}(\mathfrak{H}_{\tilde{A}}), \tag{E.16}$$

where the eigenvalues $\{\lambda_{k,\ell} : 0 \leq k, \ell \leq 2^m - 1\}$ were defined in (E.10). They are covariant under the operators $\{U(a)V(b) : 0 \leq a, b \leq 2^m - 1\}$, which is to say that for all $X \in \mathrm{L}(\mathfrak{H}_{\tilde{A}})$

$$U(a)V(b)\Phi_{Q,\mathcal{P}}(X)(U(a)V(b))^\dagger = \Phi_{Q,\mathcal{P}}\left(U(a)V(b)X(U(a)V(b))^\dagger\right) \quad \forall\, 0 \leq a, b \leq 2^m - 1.$$

Proposition E.8

The set of operators $\{U(a) : 0 \leq a \leq 2^m - 1\}$ and $\{V(b) : 0 \leq b \leq 2^m - 1\}$ defined in (E.11) and (E.12), respectively, have the following properties:

1. $U(a)$ and $V(b)$ are Hermitian, satisfying $U(a)^2 = V(b)^2 = \mathbb{1}_{\mathbb{C}^{2^m}}$, for all $0 \leq a, b \leq 2^m - 1$;
2. $U(a)V(b) = (-1)^{\mathrm{Bin}_m(a)\cdot\mathrm{Bin}_m(b)} V(b)U(a)$ for all $0 \leq a, b \leq 2^m - 1$.
3. $U(a)U(a') = U(a \oplus a')$ for all $0 \leq a, a' \leq 2^m - 1$ and $V(b)V(b') = V(b \oplus b')$ for all $0 \leq b, b' \leq 2^m - 1$.
4. The set $\{U(a)V(b) : 0 \leq a, b \leq 2^m - 1\}$ is an orthogonal basis for $\mathrm{L}(\mathbb{C}^{2^m})$.

PROOF:

1. This is clear by writing $U(a)$ and $V(b)$ as

$$U(a) = \sum_{\ell=0}^{2^m-1} |\ell \oplus a\rangle \langle \ell| \quad \text{and} \quad V(b) = \sum_{\ell=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell)} |\ell\rangle \langle \ell| \quad \forall\, 0 \leq a, b \leq 2^m - 1.$$

2. Holds by straightforward computation using the forms of $U(a)$ and $V(b)$ above.

3. Follows by straightforward computation.

4. Firstly, there are $(2^m)^2$ operators in the set $\{U(a)V(b) : 0 \leq a, b \leq 2^m - 1\}$, which is also equal to the dimension of $\mathrm{L}(\mathbb{C}^{2^m})$. Now, let $X_{a,b} \coloneqq U(a)V(b)$. Then,

$$\begin{aligned}
\mathrm{Tr}[X_{a,b}] = \mathrm{Tr}\left[U(a)V(b)\right] &= \mathrm{Tr}\left[\sum_{j=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(j)} |j \oplus a\rangle \langle j|\right] = \sum_{j=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(j)} \delta_{j,j\oplus a} \\
&= \delta_{a,0} \sum_{j=0}^{2^m-1} (-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(j)} \\
&= 2^m \delta_{a,0}\delta_{b,0}.
\end{aligned}$$

   This means that

$$\begin{aligned}
\mathrm{Tr}[X_{a,b}^\dagger X_{c,d}] &= \mathrm{Tr}[V(b)U(a)U(c)V(d)] \\
&= \mathrm{Tr}\left[U(a \oplus c)V(b \oplus d)\right] \\
&= 2^m \delta_{a,c}\delta_{b,d} \quad \forall\, 0 \leq a, b, c, d \leq 2^m - 1.
\end{aligned}$$

   which means that $\{X_{a,b} : 0 \leq a, b \leq 2^m - 1\}$ is an orthogonal set[1]. Consequently, it is linearly independent. Since it also contains $(2^m)^2$ elements, it necessarily spans the space $\mathrm{L}(\mathbb{C}^{2^m})$. ■

The last part of the proposition above implies that any operator $X \in \mathrm{L}(\mathbb{C}^{2^m})$ can be written in the basis $\{U(a)V(b) : 0 \leq a, b \leq 2^m - 1\}$ as

$$X = \frac{1}{2^m} \sum_{a,b=0}^{2^m-1} \alpha_{\substack{a \\ b}}(X) U(a)V(b), \quad \alpha_{\substack{a \\ b}}(X) \coloneqq \mathrm{Tr}\left[X^\dagger \left(U(a)V(b)\right)\right].$$

[1]For any complex Euclidean space $\mathfrak{H}$, the inner product on $\mathrm{L}(\mathfrak{H})$ being used here is the *Hilbert-Schmidt inner product* defined as $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$ for all $A, B \in \mathrm{L}(\mathfrak{H})$.

As well, any operator $X \in \mathrm{L}(\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^m})$ can be written as

$$X = \frac{1}{(2^m)^2} \sum_{\substack{a,b \\ a',b'=0}}^{2^m-1} \alpha_{\substack{a,a' \\ b,b'}}(X) U(a)V(b) \otimes U(a')V(b'), \quad \alpha_{\substack{a,a' \\ b,b'}}(X) = \mathrm{Tr}\left[X^\dagger \left(U(a)V(b) \otimes U(a')V(b')\right)\right].$$

E.2 No Post-Selection by Alice

We now let $\mathcal{Q}$ be a linear code and let $\mathcal{P} = \mathcal{B}_n$ be the set corresponding to no post-selection by Alice. The following facts then hold about the corresponding filtered states $\rho^{A^n\tilde{B}}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}$:

1. $\mathcal{C} = \mathcal{P}$, which follows from the fact that $\{P_k \oplus Q_\ell\}_{k=0}^{2^n-1} = \mathcal{P}$ for all $0 \leq \ell \leq 2^m - 1$. So the blocks $M^{(c)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}$ can be labelled by the elements of $\mathcal{B}_n$.

2. $|\mathcal{I}_c| = 2^m$ for all $c \in \mathcal{C}$; in particular, without loss of generality, we make take

$$\mathcal{I}_{P_k} = \{(\mathrm{Dec}(Q_\ell) \oplus k, \ell)\}_{\ell=0}^{2^m-1} \quad \forall\, 0 \leq k \leq 2^n - 1,$$

   where $\mathrm{Dec}(Q_\ell)$ is the decimal representation of Q_ℓ, which follows from the fact that for all $0 \leq \ell \leq 2^m - 1$ $Q_\ell = P_{\mathrm{Dec}(Q_\ell)}$.

3. The matrix V such that $V\rho^{A^n\tilde{B}}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}V^\dagger = \bigoplus_{k=0}^{2^n-1} M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}$ is given by

$$V = \sum_{k=0}^{2^n-1} \sum_{\ell=0}^{2^m-1} |k,\ell\rangle \langle \mathrm{Dec}(Q_\ell) \oplus k, \ell|,$$

   with

$$M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})} = \sum_{\ell,\ell'=0}^{2^m-1} \left(M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{\ell \\ \ell'}} |\ell\rangle \langle \ell'|, \quad \left(M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{\ell \\ \ell'}} = \left(\rho^{\tilde{A}\tilde{B}}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{\mathrm{Dec}(Q_\ell)\oplus k,\ell \\ \mathrm{Dec}(Q_{\ell'})\oplus k,\ell'}}.$$

   As in the previous section, it holds that

$$\left(M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{\ell\oplus j \\ \ell'\oplus j}} = \left(M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{\ell \\ \ell'}} \quad \forall\, 0 \leq \ell, \ell', j \leq 2^m - 1,\ \forall\, 0 \leq k \leq 2^n - 1,$$

which means that $M^{(P_k)}_{\mathcal{Q},(\mathcal{B}_n,\mathcal{Q})}$ is diagonalized by $H^{\otimes m}$ for all $0 \leq k \leq 2^n - 1$. Consequently, the following holds.

Theorem E.9

The state $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$ is diagonalized by WV, where

$$V = \sum_{k=0}^{2^n-1}\sum_{\ell=0}^{2^m-1} |k,\ell\rangle\langle \mathrm{Dec}(Q_\ell)\oplus k,\ell|, \quad W = \bigoplus_{k=0}^{2^n-1} H^{\otimes m}.$$

The eigenvectors $\{|v_{a,b}\rangle : 0 \le a \le 2^n-1,\ 0 \le b \le 2^m-1\}$ are

$$|v_{a,b}\rangle = \frac{1}{(\sqrt{2})^m}\sum_{\ell=0}^{2^m-1}(-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell)}|\mathrm{Dec}(Q_\ell)\oplus a,\ell\rangle, \tag{E.17}$$

and the corresponding eigenvalues $\{\lambda_{a,b} : 0 \le a \le 2^n-1,\ 0 \le b \le 2^m-1\}$ are

$$\lambda_{a,b} = \sum_{\ell=0}^{2^m-1}(-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(\ell)}\left(\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}\right)_{\substack{a,0\\ \mathrm{Dec}(Q_\ell)\oplus a,\ell}}. \tag{E.18}$$

By using (3.11), it holds that the Choi representation of $\mathcal{N}$ corresponding to the special map is

$$J(\mathcal{N}) = \sum_{u=0}^{2^n-1}\sum_{v=0}^{2^m-1}\left[\frac{1}{2^{2m}}\sum_{s,s',\ell'=0}^{2^m-1}\begin{pmatrix}\frac{\sum_{b=0}^{2^m-1}\lambda_{\mathrm{Dec}(Q_{\ell'})\oplus u,b}(-1)^{\mathrm{Bin}_m(b)\cdot\mathrm{Bin}_m(s\oplus s')}}{\sigma_{\mathrm{Dec}(Q_s)\oplus u,\mathrm{Dec}(Q_{s'})\oplus u}}\end{pmatrix}\begin{matrix}(-1)^{\mathrm{Bin}_n(\ell')\cdot\mathrm{Bin}_n(\mathrm{Dec}(Q_{s'})\oplus u)}\\ \times(-1)^{\mathrm{Bin}_m(v)\cdot\mathrm{Bin}_m(s\oplus s')}\end{matrix}\right]|v_{u,v}\rangle\langle v_{u,v}|, \tag{E.19}$$

where

$$\sigma_{a,a'} := \sum_{\ell',s=0}^{2^m-1}\left(A(\mathrm{Dec}(Q_s)\oplus a',\mathrm{Dec}(Q_s)\oplus a)\right)_{\substack{s\\ \ell'}}(-1)^{\mathrm{Bin}_n(s\oplus\ell')\cdot\mathrm{Bin}_n(a')} \quad \forall\ 0 \le a,a' \le 2^n-1, \tag{E.20}$$

where

$$\left(A(k,k')\right)_{\substack{\ell\\ \ell'}} = \frac{1}{2^{2m}}\sum_{b,b'=0}^{2^m-1}\sqrt{\lambda_{k,b}\lambda_{k',b'}}(-1)^{\mathrm{Bin}_m(b\oplus b')\cdot\mathrm{Bin}_m(\ell\oplus\ell')} \quad \begin{matrix}\forall\ 0 \le k,k' \le 2^n-1,\\ \forall\ 0 \le \ell,\ell' \le 2^m-1\end{matrix} \tag{E.21}$$

and $\{\lambda_{a,b} : 0 \le a \le 2^n-1\ 0 \le b \le 2^m-1\}$ are the eigenvalues of $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{Q})}$. It is straightforward to show from this that $\mathcal{N}$ is trace-preserving.

E.2.1 Repetition Codes

Using the formula in Theorem E.9, the eigenvalues of $\rho^{A^n\tilde{B}}_{Q,(\mathcal{B}_n,\mathcal{R}_n)}$ are

$$\begin{aligned}\lambda_{a,0} &= \left(\frac{Q}{2}\right)^{|P_a|}\left(\frac{1-Q}{2}\right)^{n-|P_a|} + \left(\frac{1-2Q}{2}\right)^{n-|P_a|}\delta_{P_a,\underline{0}^n},\\ \lambda_{a,1} &= \left(\frac{Q}{2}\right)^{|P_a|}\left(\frac{1-Q}{2}\right)^{n-|P_a|} - \left(\frac{1-2Q}{2}\right)^{n-|P_a|}\delta_{P_a,\underline{0}^n}\end{aligned} \quad \forall\ 0 \le a \le 2^n-1. \tag{E.22}$$

Note that the eigenvalues $\lambda_{0,0}$, $\lambda_{0,1}$, $\lambda_{2^n-1,0}$ and $\lambda_{2^n-1,1}$ coincide with the eigenvalues (5.1) of the state $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$ obtained from post-selection by both Alice and Bob on $\mathcal{R}_n$.

Using the formula (E.19), then, the eigenvalues of the Choi representation of $\mathcal{N}$ are

$$\begin{aligned}
\Lambda_{u,v} &= \frac{1}{4}\sum_{s,s'=0}^{1}\left(\frac{\sum_{\ell',b=0}^{1}\lambda_{\mathrm{Dec}(Q_{\ell'})\oplus u,b}(-1)^{b\cdot(s\oplus s')}(-1)^{\mathrm{Bin}_n(\ell')\cdot\mathrm{Bin}_n(\mathrm{Dec}(Q_{\ell'})\oplus u)}}{\sigma_{\mathrm{Dec}(Q_s)\oplus u,\mathrm{Dec}(Q_{s'})\oplus u}}\right)(-1)^{v\cdot(s\oplus s')} \\
&= \frac{1}{4}\Bigg[\left(\frac{\lambda_{u,0}+\lambda_{u,1}+(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}(\lambda_{2^n-1\oplus u,0}+\lambda_{2^n-1\oplus u,1})}{\sigma_{u,u}}\right) \\
&\quad+(-1)^{v}\left(\frac{\lambda_{u,0}-\lambda_{u,1}-(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}(\lambda_{2^n-1\oplus u,0}-\lambda_{2^n-1\oplus u,1})}{\sigma_{u,2^n-1\oplus u}}\right) \\
&\quad+(-1)^{v}\left(\frac{\lambda_{u,0}-\lambda_{u,1}+(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}(\lambda_{2^n-1\oplus u,0}-\lambda_{2^n-1\oplus u,1})}{\sigma_{2^n-1\oplus u,u}}\right) \\
&\quad+\left(\frac{\lambda_{u,0}+\lambda_{u,1}-(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}(\lambda_{2^n-1\oplus u,0}+\lambda_{2^n-1\oplus u,1})}{\sigma_{2^n-1\oplus u,2^n-1\oplus u}}\right)\Bigg]
\end{aligned}$$

for all $0 \le u \le 2^n-1$ and for all $0 \le v \le 1$, where

$$\begin{aligned}
\sigma_{a,a'} &= \big(A(a',a)\big)_{0}^{0} + (-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(a')}\big(A(a',a)\big)_{1}^{0} \\
&\quad+(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(a')}\big(A(2^n-1\oplus a',2^n-1\oplus a)\big)_{0}^{1}+\big(A(2^n-1\oplus a',2^n-1\oplus a)\big)_{1}^{1}
\end{aligned}$$

for all $0 \le a, a' \le 2^n-1$, where

$$\begin{aligned}
\big(A(k,k')\big)_{0}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{k,0}\lambda_{k',0}}+\sqrt{\lambda_{k,0}\lambda_{k',1}}+\sqrt{\lambda_{k,1}\lambda_{k',0}}+\sqrt{\lambda_{k,1}\lambda_{k',1}}\right), \\
\big(A(k,k')\big)_{1}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{k,0}\lambda_{k',0}}-\sqrt{\lambda_{k,0}\lambda_{k',1}}-\sqrt{\lambda_{k,1}\lambda_{k',0}}+\sqrt{\lambda_{k,1}\lambda_{k',1}}\right), \\
\big(A(k,k')\big)_{0}^{1} &= \big(A(k,k')\big)_{1}^{0}, \\
\big(A(k,k')\big)_{1}^{1} &= \big(A(k,k')\big)_{0}^{0}
\end{aligned}$$

for all $0 \le k, k' \le 2^n-1$.

Straightforward calculations using (E.21) show that

$$\begin{aligned}
(A(0,0))_{0}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{0,0}}+\sqrt{\lambda_{0,1}}\right)^2, \\
(A(0,0))_{1}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{0,0}}-\sqrt{\lambda_{0,1}}\right)^2, \\
(A(2^n-1,2^n-1))_{0}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{2^n-1,0}}+\sqrt{\lambda_{2^n-1,1}}\right)^2, \\
(A(2^n-1,2^n-1))_{1}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{2^n-1}}-\sqrt{\lambda_{2^n-1,1}}\right)^2, \\
(A(0,2^n-1))_{0}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{0,0}}+\sqrt{\lambda_{0,1}}\right)\left(\sqrt{\lambda_{2^n-1,0}}+\sqrt{\lambda_{2^n-1,1}}\right), \\
(A(0,2^n-1))_{1}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{0,0}}-\sqrt{\lambda_{0,1}}\right)\left(\sqrt{\lambda_{2^n-1,0}}-\sqrt{\lambda_{2^n-1,1}}\right), \\
(A(2^n-1,0))_{0}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{2^n-1,0}}+\sqrt{\lambda_{2^n-1,1}}\right)\left(\sqrt{\lambda_{0,0}}+\sqrt{\lambda_{0,1}}\right), \\
(A(2^n-1,0))_{1}^{0} &= \frac{1}{4}\left(\sqrt{\lambda_{2^n-1,0}}-\sqrt{\lambda_{2^n-1,1}}\right)\left(\sqrt{\lambda_{0,0}}-\sqrt{\lambda_{0,1}}\right),
\end{aligned}$$

which leads to

$$\begin{aligned}
\sigma_{0,0} &= \frac{1}{2}\left(\lambda_{0,0}+\lambda_{0,1}+\lambda_{2^n-1,0}+\lambda_{2^n-1,1}\right),\\
\sigma_{0,2^n-1} &= \sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,1}\lambda_{0,0}},\\
\sigma_{2^n-1,0} &= \sqrt{\lambda_{0,0}\lambda_{2^n-1,0}}+\sqrt{\lambda_{0,1}\lambda_{2^n-1,1}},\\
\sigma_{2^n-1,2^n-1} &= \sqrt{\lambda_{2^n-1,0}\lambda_{2^n-1,1}}+\sqrt{\lambda_{0,0}\lambda_{0,1}}.
\end{aligned}$$

Therefore, the eigenvalues $\{\Lambda_{0,0},\Lambda_{0,1},\Lambda_{2^n-1,0},\Lambda_{2^n-1,1}\}$ are equal to

$$\begin{aligned}
\Lambda_{0,0} &= \frac{1}{4}\Bigg(2+\frac{\lambda_{0,0}-\lambda_{0,1}-\lambda_{2^n-1,0}+\lambda_{2^n-1,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,1}\lambda_{0,0}}}+\frac{\lambda_{0,0}-\lambda_{0,1}+\lambda_{2^n-1,0}-\lambda_{2^n-1,1}}{\sqrt{\lambda_{0,0}\lambda_{2^n-1,0}}+\sqrt{\lambda_{0,1}\lambda_{2^n-1,1}}}\\
&\quad+\frac{\lambda_{0,0}+\lambda_{0,1}-\lambda_{2^n-1,0}-\lambda_{2^n-1,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{2^n-1,1}}+\sqrt{\lambda_{0,0}\lambda_{0,1}}}\Bigg),\\
\Lambda_{0,1} &= \frac{1}{4}\Bigg(2-\frac{\lambda_{0,0}-\lambda_{0,1}-\lambda_{2^n-1,0}+\lambda_{2^n-1,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,1}\lambda_{0,0}}}-\frac{\lambda_{0,0}-\lambda_{0,1}+\lambda_{2^n-1,0}-\lambda_{2^n-1,1}}{\sqrt{\lambda_{0,0}\lambda_{2^n-1,0}}+\sqrt{\lambda_{0,1}\lambda_{2^n-1,1}}}\\
&\quad+\frac{\lambda_{0,0}+\lambda_{0,1}-\lambda_{2^n-1,0}-\lambda_{2^n-1,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{2^n-1,1}}+\sqrt{\lambda_{0,0}\lambda_{0,1}}}\Bigg),
\end{aligned}\tag{E.23}$$

$$\begin{aligned}
\Lambda_{2^n-1,0} &= \frac{1}{4}\Bigg(\frac{\lambda_{2^n-1,0}-\lambda_{0,0}+\lambda_{2^n-1,1}-\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{2^n-1,1}}+\sqrt{\lambda_{0,0}\lambda_{0,1}}}+\frac{\lambda_{2^n-1,0}+\lambda_{0,0}-\lambda_{2^n-1,1}-\lambda_{0,1}}{\sqrt{\lambda_{0,0}\lambda_{2^n-1,0}}+\sqrt{\lambda_{0,1}\lambda_{2^n-1,1}}}\\
&\quad+\frac{\lambda_{2^n-1,0}-\lambda_{0,0}-\lambda_{2^n-1,1}+\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,1}\lambda_{0,0}}}+2\Bigg),\\
\Lambda_{2^n-1,1} &= \frac{1}{4}\Bigg(\frac{\lambda_{2^n-1,0}-\lambda_{0,0}+\lambda_{2^n-1,1}-\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{2^n-1}}+\sqrt{\lambda_{0,0}\lambda_{0,1}}}-\frac{\lambda_{2^n-1,0}+\lambda_{0,0}-\lambda_{2^n-1,1}-\lambda_{0,1}}{\sqrt{\lambda_{0,0}\lambda_{2^n-1,0}}+\sqrt{\lambda_{0,1}\lambda_{2^n-1,1}}}\\
&\quad-\frac{\lambda_{2^n-1,0}-\lambda_{0,0}-\lambda_{2^n-1,1}+\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,1}\lambda_{0,0}}}+2\Bigg).
\end{aligned}\tag{E.24}$$

Using from (E.22) the fact that $\lambda_{2^n-1,0}=\lambda_{2^n-1,1}$, the eigenvalues written above simplify to

$$\begin{aligned}
\Lambda_{0,0} &= \frac{1}{2}+\frac{1}{2}\frac{\lambda_{0,0}-\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,0}\lambda_{0,0}}}+\frac{1}{4}\frac{\lambda_{0,0}+\lambda_{0,1}-2\lambda_{2^n-1,0}}{\lambda_{2^n-1,0}+\sqrt{\lambda_{0,0}\lambda_{0,1}}},\\
\Lambda_{0,1} &= \frac{1}{2}-\frac{1}{2}\frac{\lambda_{0,0}-\lambda_{0,1}}{\sqrt{\lambda_{2^n-1,0}\lambda_{0,1}}+\sqrt{\lambda_{2^n-1,0}\lambda_{0,0}}}+\frac{1}{4}\frac{\lambda_{0,0}+\lambda_{0,1}-2\lambda_{2^n-1,0}}{\lambda_{2^n-1,0}+\sqrt{\lambda_{0,0}\lambda_{0,1}}},\\
\Lambda_{2^n-1,0} &= \frac{1}{2}+\frac{1}{4}\frac{2\lambda_{2^n-1,0}-\lambda_{0,0}-\lambda_{0,1}}{\lambda_{2^n-1,0}+\sqrt{\lambda_{0,0}\lambda_{0,1}}}=\Lambda_{2^n-1,1}.
\end{aligned}\tag{E.25}$$

These are exactly the same as the eigenvalues (6.17), (6.18), (6.19) (with $m=2$) of $J(\mathcal{N})$ (equivalently, $\Lambda_1,\Lambda_2,\Lambda_3,\Lambda_4$ from (5.8)) obtained for $\rho^{\tilde{A}\tilde{B}}_{Q,\mathcal{R}_n}$.

The remaining eigenvalues $\Lambda_{u,v}$, for $1\leq u\leq 2^n-2$ and $0\leq v\leq 1$, have a relatively simple form.

Lemma E.10

For all $1 \leq u \leq 2^n - 2$, it holds that

$$\Lambda_{u,0} = \Lambda_{u,1} = \frac{Q^{|P_u|}(1-Q)^{n-|P_u|}}{Q^{|P_u|}(1-Q)^{n-|P_u|} + Q^{n-|P_u|}(1-Q)^{|P_u|}}. \tag{E.26}$$

PROOF: We start by observing from (E.22) that

$$\lambda_{u,0} = \lambda_{u,1} = \left(\frac{Q}{2}\right)^{|P_u|} \left(\frac{1-Q}{2}\right)^{n-|P_u|}, \quad \forall\, 1 \leq u \leq 2^n - 2.$$

Then, the general expression for the eigenvalue $\Lambda_{u,v}$ can be simplified to

$$\Lambda_{u,v} = \frac{1}{4}\left(\frac{2\lambda_{u,0} + 2(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}\lambda_{2^n-1\oplus u,0}}{\sigma_{u,u}} + \frac{2\lambda_{u,0} - 2(-1)^{\mathrm{Bin}_n(1)\cdot\mathrm{Bin}_n(u)}\lambda_{2^n-1\oplus u,0}}{\sigma_{2^n-1\oplus u,2^n-1\oplus u}}\right).$$

Since for all $1 \leq u \leq 2^n - 2$ it holds that

$$(A(u,u))_{\substack{\ell \\ \ell'}} = \frac{1}{2}\left(\lambda_{u,0} + (-1)^{\ell\oplus\ell'}\lambda_{u,0}\right) = \lambda_{u,0}\delta_{\ell,\ell'},$$

we have that

$$\sigma_{u,u} = \lambda_{u,0} + \lambda_{2^n-1\oplus u,0} = \sigma_{2^n-1\oplus u,2^n-1\oplus u} \quad \forall\, 1 \leq u \leq 2^n - 2.$$

Therefore, $\Lambda_{u,v}$ simplifies to

$$\Lambda_{u,v} = \frac{\lambda_{u,0}}{\lambda_{u,0} + \lambda_{2^n-1\oplus u,0}} \quad \forall\, 1 \leq u \leq 2^n - 2,\ \forall\, 0 \leq v \leq 1,$$

which further simplifies to the required form. ■