Université de Montréal

From Classical to Quantum Secret Sharing

par
Paul-Robert Chouha

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

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

Avril, 2012

Université de Montréal
Faculté des arts et des sciences

Ce mémoire intitulé:

From Classical to Quantum Secret Sharing

présenté par:

Paul-Robert Chouha

a été évalué par un jury composé des personnes suivantes:

Louis Salvail,	président-rapporteur
Alain Tapp,	directeur de recherche
Gilles Brassard,	codirecteur
Neil Stewart,	membre du jury

Mémoire accepté le: . . . .

RÉSUMÉ

Dans ce mémoire, nous nous pencherons tout particulièrement sur une primitive cryptographique connue sous le nom de partage de secret. Nous explorerons autant le domaine classique que le domaine quantique de ces primitives, couronnant notre étude par la présentation d'un nouveau protocole de partage de secret quantique nécessitant un nombre minimal de parts quantiques c.-à-d. une seule part quantique par participant. L'ouverture de notre étude se fera par la présentation dans le chapitre préliminaire d'un survol des notions mathématiques sous-jacentes à la théorie de l'information quantique ayant pour but primaire d'établir la notation utilisée dans ce manuscrit, ainsi que la présentation d'un précis des propriétés mathématique de l'état de Greenberger-Horne-Zeilinger (GHZ) fréquemment utilisé dans les domaines quantiques de la cryptographie et des jeux de la communication. Mais, comme nous l'avons mentionné plus haut, c'est le domaine cryptographique qui restera le point focal de cette étude. Dans le second chapitre, nous nous intéresserons à la théorie des codes correcteurs d'erreurs classiques et quantiques qui seront à leur tour d'extrême importances lors de l'introduction de la théorie quantique du partage de secret dans le chapitre suivant.

Dans la première partie du troisième chapitre, nous nous concentrerons sur le domaine classique du partage de secret en présentant un cadre théorique général portant sur la construction de ces primitives illustrant tout au long les concepts introduits par des exemples présentés pour leurs intérêts autant historiques que pédagogiques. Ceci préparera le chemin pour notre exposé sur la théorie quantique du partage de secret qui sera le focus de la seconde partie de ce même chapitre. Nous présenterons alors les théorèmes et définitions les plus généraux connus à date portant sur la construction de ces primitives en portant un intérêt particulier au partage quantique à seuil. Nous montrerons le lien étroit entre la théorie quantique des codes correcteurs d'erreurs et celle du partage de secret. Ce lien est si étroit que l'on considère les codes correcteurs d'erreurs quantiques étaient de plus proches analogues aux partages de secrets quantiques que ne leur étaient les codes de partage de secrets classiques. Finalement, nous présenterons un de nos trois résultats parus dans [13]; un protocole sécuritaire et minimal de partage de secret quantique a seuil (les deux autres résultats dont nous traiterons pas ici portent sur la complexité de la communication et sur la simulation classique de l’état de GHZ).

Mots clefs: Cryptographie, théorie de l’information quantique, codes correcteurs d’erreurs, corrections d’erreurs quantiques, partage de secret classique, partage de secrets quantiques à seuil.

ABSTRACT

In this thesis, we will focus on a cryptographic primitive known as secret sharing. We will explore both the classical and quantum domains of such schemes culminating our study by presenting a new protocol for sharing a quantum secret using the minimal number of possible quantum shares i.e. one single quantum share per participant. We will start our study by presenting in the preliminary chapter, a brief mathematical survey of quantum information theory (*QIT*) which has for goal primarily to establish the notation used throughout the manuscript as well as presenting a *précis* of the mathematical properties of the Greenberger-Horne-Zeilinger (GHZ)-state, which is used thoroughly in cryptography and in communication games. But as we mentioned above, our main focus will be on cryptography. In chapter two, we will pay a close attention to classical and quantum error corrections codes (*QECC*) since they will become of extreme importance when we introduce quantum secret sharing schemes in the following chapter. In the first part of chapter three, we will focus on classical secret shearing, presenting a general framework for such a primitive all the while illustrating the abstract concepts with examples presented both for their historical and analytical relevance. This first part (chapters one and two) will pave the way for our exposition of the theory of Quantum Secret Sharing (QSS), which will be the focus of the second part of chapter three. We will present then the most general theorems and definitions known to date for the construction of such primitives putting emphasis on the special case of quantum *threshold* schemes. We will show how quantum error correction codes are related to *QSS* schemes and show how this relation leads to a very solid correspondence to the point that *QECC*'s are closer analogues to *QSS* schemes than are the classical secret sharing primitives. Finally, we will present one of the three results we have in [13] in particular, a secure minimal quantum threshold protocol (the other two results deal with communication complexity and the classical simulation of the GHZ-state).

Keywords: Cryptography, quantum information theory, error correction codes, quantum error correction, classical secret sharing, quantum secret sharing, quantum threshold schemes.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

CSS	Claderbank-Shor-Stean.
EPR	Einstein-Podolsky-Rosen.
GHZ	Greenberger-Horne-Zeilinger.
GR	General Relativity.
LOCC	Local Operation and Classical Communication.
MSP	Monotone Spam Program.
$\mathscr{N}.\mathscr{B}.$	Nota bene.
qubit	Quantum Bit.
qshare	Quantum Share.
QEC	Quantum Error Correction.
QECC	Quantum Error Correcting Codes.
QIT	Quantum Information Theory.
QM	Quantum mechanics.
QSS	Quantum Secret Sharing.
QTS	Quantum Threshold Schemes.
SR	Special Relativity.
SSS	Secret Sharing Schemes.

NOTATION

$\mathbb{C}$	Field of complex numbers.
$\|\alpha\|$	Modulus of the complex number $\alpha \in \mathbb{C}$.
$\mathbb{F}_q$	Finite field of q-elements.
$\mathbb{F}_q^n$	n-dimensional vector space with entries in the finite field $\mathbb{F}_q$.
$\mathbb{Z}_2$	Ring of integers modulo 2.
$\equiv_2$	Congruence equivalence modulo 2.
$\mathscr{H}$	Hilbert space.
$\mathscr{H}_*$	Dual Hilbert space.
$\mathscr{H}_2$	Two dimensional Hilbert space.
$\mathscr{H}_A$	Hilbert space associated with system A.
$\mathbf{C}$	Code space.
$\mathbf{C}^\perp$	Code space perpendicular to $\mathbf{C}$.
$\hat{O}$	Quantum-mechanical operator as designated in the physics literature.
$E^\dagger$	Hermitian conjugate of E.
E^T	Transpose of E.
$[A,B]$	Commutator of two operators (matrices) A and B.
$\{A,B\}$	Anti-commutator of two operators (matrices) A and B.
$\|\psi\rangle$	Ket vector.
$\langle\psi\|$	Bra vector dual to the ket vector.
$\langle\psi\|\varphi\rangle$	Inner product between the vectors $\|\psi\rangle$ and $\|\varphi\rangle$.
$\|\psi\rangle \otimes \|\varphi\rangle$	Tensor product of the vectors $\|\psi\rangle$ and $\|\varphi\rangle$.
$\|\psi\rangle\langle\varphi\|$	Outer product of the vectors $\|\psi\rangle$ and $\|\varphi\rangle$.
ρ_A	Density matrix associated with system A.
Tr	Trace function.

Tr_A	Partial trace on subsystem A.
$[n,k,d]$	Classical error correcting code with parameters n, k, and d.
$[[n,k,d]]$	Quantum error correcting code with parameters n, k, and d.
$\mathscr{G}_n$	Pauli group of n-qubits.
(k,n)	Classical threshold secret sharing scheme.
$((k,n))$	Quantum threshold secret sharing scheme.
$\mathscr{D}$	The dealer or the person of authority in a given protocol.
$\mathscr{S}$	Set of all possible shares.
$\mathscr{K}$	Set of all possible keys.
$\mathscr{P}_n$	Set of n players.
P_i	The i $^{\text{th}}$-player.
Γ	Access structure of a given secret sharing scheme.
Γ_0	Minimal access structure associated with Γ.
$\Pi(x)$	Parity of the integer x.
$\in_R$	Picked uniformly at random in $\ldots$.

To the memory of my father Robert Chouha,

to my mother Bernadette,
to my sister Fabiola,
to my supervisors Alain Tapp and Gilles Brassard and…

to Stéphanie and Ariadna who were, are and always will be the most precious gems of my life.

ACKNOWLEDGMENTS

First of all, I would like to thank my supervisors and directors Gilles Brassard and Alain Tapp for all their help, support and teaching without which this thesis would not have seen the day. It was a privilege to learn from them and to work side by side with them through all the fluctuations[1] that I encountered along the road.

I would like to thank as well Louis Salvail from whom I learned modern cryptography and the care he took to explain the intricate unending reductions throughout the course of our study.

A big thank you to my mother and sister who continuously supported me in so many ways.

A big thank you to Stéphanie who continued to believe in my capabilities and to Ariadna who with her shining smile gave me the strength to carry on with this task.

Finally, but not least a big thank You to God the creator of the Universe with all its marvels and laws without Whom we would not be here to ponder the beauty of it all and as scientists be privileged to have a direct glimpse at the secrets of His handy work.

[1] only classical fluctuations are considered here since they were macroscopic.

PREFACE

When the Greek words $\kappa\rho\upsilon\pi\tau\acute{o}\sigma$ "***Kryptós***" (hidden) and $\gamma\rho\acute{\alpha}\varphi\varepsilon\iota\nu$ "***gráphein***" (to write) are put together appropriately they give us the new word *cryptography*, which in the old days was seen as the *art* of writing down important information in a secret or hidden way. When the subject was put on a firm mathematical foundation by Shannon [60], it passed from an art to a science. The subject now rests on important axioms or mathematical assumptions like the existence of one-way functions[2] to formally prove or disprove the security of cryptographic protocols.

Quantum cryptography, on the other hand, is the study of cryptography when the laws of quantum mechanics are taken into account. At first glance, one would wonder what does the world of microscopic physics have to do with computer science or any of its branches? In science (at least the way theoretical physics has evolved in the twentieth century), when one is looking for a link between apparently different subjects, one has to pay close attention to the most fundamental objects in the theory. In our case, the fundamental entity in computer science and in cryptography in particular is *information*. It is the key to unlock the mysterious connection between the physical world and the world of computer science. Once information is viewed as a physical system, we are ready to go beyond classical computer science and apply the framework of quantum mechanics to information theory. One then passes from a *bit* of information to a qubit (i.e. to a quantum bit). So quantum cryptography is not the quantization of the classical theory of cryptography, but is the application of quantum principles to cryptography. As we will see in the preliminary chapter, the quantum world differs drastically in its philosophy from our "everyday" classical concepts and constitutes in itself a new paradigm *à la* Thomas Kuhn (c.f. [40]).

Quantum secret sharing, as we will explore in Chapter 3, is the quantum generalization of classical secret sharing. Briefly speaking, those are cryptographic primitives that involve a certain number of participants who try to reconstruct a given classical or

[2] Those are functions that can easily be computed but very hard (in the sense of complexity theory) to invert.

quantum secret in such a way that individually they cannot learn any useful (or in the most interesting case any) information (at all) about that secret, but need the coalition of *authorized sets* of players to be able to do so. The everyday example would be the simultaneous usage of two keys to open a safe in a bank by the client and a sub-manager or by two high-profile generals wanting to launch a missile when they are issued the order. It is our task in the next few chapters to put on a firm mathematical ground the theory of quantum secret sharing starting from its classical counterpart and the theories of classical and quantum error correcting codes.

CHAPTER 1

THE QUANTUM EXPRESS

We begin our exposition with an express overview of Quantum Information Theory with two objectives in mind, the first is to establish notation and the second to introduce the reader to the major core results and mathematical machinery that will be extensively used in the text.

In the classical world of information theory, the unit of information is said to be the *bit*, coined for binary digit. For example, we express the length of a number by how many bits it contains (for example: 3 has two bits corresponding to its binary expansion 11 while 17 has five bits corresponding to 10001 in its binary notation). Very often, we will be interested in the number of bits required to achieve a certain task; for example the number of bits that need to be communicated between two or more parties in the computation of a given function; this is a simple example of communication complexity (c.f. [41] for a survey of classical communication complexity and [16, 17] and [9] for good surveys of the quantum aspects of the subject).

In the quantum world of information theory, in analogy with the classical notion of bits, we coin the word quantum bits or *qubits* to describe the quantum unit of information. To distinguish the quantum world from the classical one we use a special notation. For example[1] the "quantum" digit 3 is represented as $|11\rangle$ in its binary expansion and we thus say that it is represented by two qubits and write $|3\rangle \equiv |11\rangle$. While $|17\rangle$ would be represented by $|10001\rangle$ and thus by five qubits.

Very briefly, after the 1920's quantum revolution [8, 58] in our understanding of the microcosm, it became clear that we were being exposed to new ideas that were totally alien to our classical way of thinking. Just a few years earlier, Einstein's 1905 special theory of relativity (*SR*) [27] and his 1915 general theory of relativity (*GR*) [28] revolutionized the way we think about space and time. In particular we had to give up the notion that time is absolute and accept that space and time are weaved together in

[1] This notation is known as the Dirac notation and will be explained in the text shortly.

an eternal or finite fabric (depending on whether the Universe is open or closed, respectively) called *spacetime*, which in turn is itself a dynamical entity ever evolving. Einstein taught us in *SR* as well that an observer may measure two different lengths, times, and speeds depending on whether he is still or in motion; that twins who travel in space may age differently if one of them was accelerating through spacetime, while in *GR* we were taught that matter tells spacetime how to curve and in return spacetime tells matter how to move. Thus, we see that depending on one's reference frame, measurements are indeed relative.

Although those notions came as a shock to the scientific community, nothing prepared them for the *Quantum Mechanical* (*QM*) revolution. Just the fact of "observing" the system under study becomes crucial in its future dynamical evolution as well as crucial to what we measure. Although in small steps, we see the beginning of a pattern, observers start to enter science in different but crucial ways. From a passive observer who (observes) "measures" with a stick a length, with a clock a time and with a speedometer a speed, to an active observer who (in the Copenhagen interpretation of QM) collapses the wavefunction of the system just by observing (measuring) it, and therefore the system settles down in one of its eigenstates. What we observe (the physical trait) is the eigenvalue of that eigenstate.

We will shortly discuss the postulates of quantum mechanics that explain those notions, but in order to do so we first need to introduce the mathematical machinery (i.e. the language before the poetry).

1.1 The Mathematical Machinery of Quantum Information Theory

A *qubit* lives in $\mathscr{H}_2$ where by $\mathscr{H}_2$ we mean the two-dimensional Hilbert space and in using Paul Dirac's *bra* $\langle .|$ *ket* $|.\rangle$ notation we may write a general qubit as:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{with } |\alpha|^2 + |\beta|^2 = 1, \tag{1.1}$$

where the set $\{|0\rangle, |1\rangle\}$ is called the *computational basis* and $\alpha,\ \beta \in \mathbb{C}$ are called the *amplitudes*.

Notation 1.1. $|\alpha|^2 = \alpha\alpha^* = \alpha^*\alpha$ *is the modulus of the complex number* α*, where* α^* *denotes its complex conjugate.*

In matrix form the qubit is a (2×1)-matrix i.e. a column vector. The basis therefore are written as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The general qubit in Eq.(1.1) is then given by :

$$|\Psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Let $\mathscr{H}$ be a Hilbert space and $\mathscr{H}_*$ be the dual space endowed with a multiplication law of the form

$$(c,\xi) = c^*\ \xi$$

A very useful operation on vector spaces (where the Hilbert space is just an example) is the *inner product*, which we define next.

Definition 1.2. *The* inner product *is a bilinear form (duality)*

$$\langle\ \cdot|\cdot\rangle\ : \mathscr{H}_* \otimes \mathscr{H} \to \mathbb{C}.$$

The symbol $\otimes$ *is called the Cartesian product and is studied in more detail in Notation1.10 bellow.*

Definition 1.3. The dual *(or complex conjugate) of the vector* $|\psi\rangle \in \mathscr{H}$ *is denoted by* $\langle\psi| \in \mathscr{H}_*$ *and in forming the* ***inner product*** *between them we get the square of the length of the vector. If it is properly* ***normalized*** *we call it a unit vector.*
Let $|\psi\rangle$ *be as in Eq.(1.1) with* α, $\beta \in \mathbb{C}$*, the* ***inner product*** *known also as the* ***dot product*** *is given by:*

$$\langle\psi|\psi\rangle = (\alpha^*\langle 0| + \beta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = |\alpha|^2 + |\beta|^2 = 1,$$

which is the requirement that the vector be normalized to unity and $|\alpha|^2 + |\beta|^2 = 1$ *expresses this normalization condition. To arrive at the above condition, we have used the distributive law of the inner product as well as the fact that* $|0\rangle$ *and* $|1\rangle$ *are mutually* ***orthonormal*** *(i.e are orthogonal and of unit norm).*

Definition 1.4. *A* ***quantum register*** *(of n qubits) lives in* $\mathscr{H}_2 \otimes \mathscr{H}_2 \otimes \cdots \mathscr{H}_2 = \mathscr{H}_2^{\otimes n}$ *(we write* $\mathscr{H}_{2^n}$ *for* $\mathscr{H}_2^{\otimes n}$*) and is of the form*

$$|\Theta\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \quad \textit{with} \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

We now present some important notions borrowed from linear algebra concerning special kinds of matrices that are needed to describe the allowed operations used to manipulate qubits. A more detailed exposition on linear transformations and their relation to matrices and more subtle properties are presented in Appendix I.
We start with the notion of a *Hermitian matrix*:

Definition 1.5. *A matrix* $M : \mathbb{C}^n \to \mathbb{C}^n$ *is said to be* ***Hermitian*** *if it satisfies:*

$$M^\dagger = M,$$

where the ***Hermitian conjugate*** $M^\dagger$ *of* $M : \mathbb{C}^n \to \mathbb{C}^n$ *is defined by*

$$\langle x|M|y\rangle = \langle M^\dagger x|\, y\rangle = \langle y|M^\dagger|x\rangle^*,$$

with $|x\rangle$, $|y\rangle$ *arbitrary vectors in* $\mathbb{C}^n$.

In other words, $M^\dagger$ is the conjugate transpose of M.

Definition 1.6. *Any* ***quantum operation*** *is reversible, linear and preserves the norm. Thus a quantum operation is valid if and only if it is* ***unitary*** *i.e. an operator* $\widehat{V}$ *satisfying* $\widehat{V}\,\widehat{V}^\dagger = \widehat{I} = \widehat{V}^\dagger \widehat{V}$.

Definition 1.7. *The set of* $(n \times n)$-unitary *matrices is a group called the* ***unitary group*** *denoted by* $U(n)$. *If in addition the matrices are* **unimodular** *i.e. of unit determinant, then the group is called the* ***special unitary group*** *and is denoted by* $SU(n)$.

Notation 1.8. *From now on we will adopt the notation widely spread in the computer science literature and omit writing a* $''\widehat{hat}''$ *on the quantum operator as is usually the custom in physics.*

Examples of unitary operators are:

- **Negation**

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.2}$$

- **Control-NOT gate**

$$C_{NOT} = \begin{pmatrix} I_{2\times 2} & 0 \\ 0 & N_{2\times 2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{1.3}$$

  where $I_{2\times 2}$ denotes the two by two identity matrix and $N_{2\times 2}$ the two by two negation operator introduced above.

- **Hadamard Transform**

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1.4}$$

  and we explicitly display the action of the Hadamard transform on the *computa-*

tional basis $|0\rangle$ and $|1\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \tag{1.5}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle, \tag{1.6}$$

where $\{|\pm\rangle\}$ is known as the *Hadamard basis*.

The action of the n-fold Hadamard transform on an n-dimensional qubit living in a 2^n-dimensional Hilbert space is given by:

$$\boxed{H_n|x\rangle = \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle,}$$

where $x \cdot y$ denotes the dot product between the two vectors $x \cdot y \equiv (x_1y_1 + x_2y_2 + \cdots + x_ny_n) \mod 2$.

- **Phase-Shift**

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{1.7}$$

with action on the computational basis given by:

$$S_\theta|0\rangle = |0\rangle$$

$$S_\theta|1\rangle = e^{i\theta}|1\rangle.$$

We denote by T the operator with $\theta = \frac{\pi}{2}$ i.e. $T = S_{\theta=\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

- **The Pauli Matrices**

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1.8}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.9}$$

We include the identity operator among the Pauli operators for completeness.

An important property that those matrices have is seen through their *commutation and anticommutation relations*, respectively:

$$[X,Y] = iZ, \quad [Y,Z] = iX, \quad [Z,X] = iY \text{ where } [A,B] = AB - BA,$$

$$\{X,Y\} = \{Y,Z\} = \{Z,X\} = 0 \text{ where } \{A,B\} = AB + BA.$$

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle.$$

Remark 1.9. *We note that in the theory of* Quantum Error Corrections *(QEC) (about which we will have more to say later) the Identity operator represents the "occurrence" of no error, the X operator is known as a* bit flip *(we can see that it takes a $|0\rangle$ to $|1\rangle$ and vise versa), the Z operator is known as a* phase-flip *(it flips the phase of the qubit if it is in the* 1 *state), and given that $Y = iXZ$ it is a combination of both, a phase flip followed by a bit flip.*

We see as well that the Hadamard transform (in the single qubit case) is given by:

$$H = \frac{1}{\sqrt{2}}(X + Z) \tag{1.10}$$

with $HXH = Z, HYH = -Y, HZH = X$.

Notation 1.10. ***Tensor Product***

*A useful operation is known as the **Kronecker product** or the **tensor product** denoted by $\otimes$, which acts as follows on the general qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ when* *tensored with another qubit $|\Lambda\rangle = \gamma|0\rangle + \delta|1\rangle$:*

$$|\Psi\rangle \otimes |\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \beta \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}.$$

We note that its action is to enlarge the space. What this means physically is that it describes the coupling of two qubits into one 2-qubit state.

This process could be extended to d-dimensions and we then talk about a qudit.

When $\alpha = 1$ and $\beta = 0$, hence $|\Psi\rangle = |0\rangle$, we have

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

When we expand the space of the system by appending (i.e. tensoring) $|0\cdots 0\rangle$ to the right of a quantum state $|\Psi\rangle$, we call those extra dimensional $|0\rangle$'s ancillary qubits *and they represent working space.*

ℹ $\mathscr{N}.\mathscr{B}$. We will usually write $|\varphi\rangle|\psi\rangle$ as a shorthand for $|\varphi\rangle \otimes |\psi\rangle$ and even $|\underbrace{00\cdots 0}_{n\ times}\rangle$ for $\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n\ times} \equiv |0^n\rangle$ omitting the $\otimes$-symbol.

Remark 1.11. *The* Kronecker *or tensor product has some important properties that facilitates complex calculations.*

Let A be an $(m \times n)$ matrix, B a $(p \times q)$ matrix, C an $(n \times r)$ matrix and D a $(q \times s)$ matrix:

1. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

2. $A \otimes (B + C) = A \otimes B + A \otimes C$.

3. $(A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger}$.

4. $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

Now let A be an $(m \times m)$ *matrix and B an* $(n \times n)$ *matrix:*

1. $\mathrm{Tr}(A \otimes B) = (\mathrm{Tr}\, A)(\mathrm{Tr}\, B)$.

2. $\det(A \otimes B) = (\det\, A)^{n}(\det\, B)^{m}$.

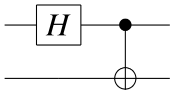
Where Tr *and* det *denote respectively the* trace *and the* determinant *of the given matrix.*

We mentioned above the computational basis $|0\rangle$ and $|1\rangle$. We now introduce the *EPR-basis* named after Einstein, Podolsky and Rosen [29]:

Definition 1.12. ***EPR Basis or Bell Basis***

Consider the circuit

$$E = C_{NOT}(H \otimes I) = \tag{1.11}$$



We have:
$E|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\varphi^{+}\rangle,\ \ E|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\varphi^{-}\rangle,$
$E|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\psi^{+}\rangle,\ \ E|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\psi^{-}\rangle.$
The set $\{|\varphi^{+}\rangle, |\varphi^{-}\rangle, |\psi^{+}\rangle, |\psi^{-}\rangle\}$ *constitutes the* ***Bell basis****.*

The circuit above thus serves to create entanglement; a property we now define.

Definition 1.13. *Let* $\{|i\rangle_A\}$ *and* $\{|j\rangle_B\}$ *be fixed bases for the Hilbert spaces* $\mathscr{H}_A$ *and* $\mathscr{H}_B$*, respectively. Consider the most general state on* $\mathscr{H}_A \otimes \mathscr{H}_B$

$$|\psi_{AB}\rangle = \sum_{i,j} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B.$$

If one can write the coefficients $\alpha_{ij} = \alpha_i^A \alpha_j^B$*, then the quantum state is termed* separable *and we can thus write* $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = \sum_i \alpha_i^A |i\rangle_A \otimes \sum_j \alpha_j^B |j\rangle_B$*. Otherwise, the state is called an* ***entangled state*** *of which the Bell-states (bases) represent a perfect example.*

ℹ $\mathscr{N}.\mathscr{B}.$ Any Bell state can be transformed into another by applying the appropriate unitary transformation to the first qubit.

$$|\varphi^+\rangle = I_2|\varphi^+\rangle,\ |\psi^+\rangle = (N \otimes I)|\varphi^+\rangle,\ |\varphi^-\rangle = (Z \otimes I)|\varphi^+\rangle,\ |\psi^-\rangle = (ZN \otimes I)|\varphi^+\rangle,$$

where by I_n or $I^{\otimes n}$ we mean the n-times tensor product of the identity operator (i.e. $I_n \equiv \underbrace{I \otimes I \otimes \cdots \otimes I}_{n-times} \equiv I^n$); this notation applies equally well to any operator.

Before delving into some of the important results and theorems of Quantum Information Theory (*QIT*) let us step back and take a brief look at the underlying physical theory. We give an overview of the postulates of quantum mechanics *à la* Nielsen and Chuang [50]. We present the so-called *Copenhagen interpretation* of quantum mechanics [8].

1.1.1 The Postulates of Quantum Mechanics

- (**Postulate I**) At a fixed time t_0, the state of an isolated physical system is completely described by a normalized wave vector $|\Psi(t_0)\rangle$ living in the *Hilbert* space $\mathscr{H}$.

  That is to say that in quantum mechanics every physically realizable state of a system is described by a state function Ψ that contains all the *accessible* physical information.

  Now suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are two orthogonal physical states of the system. Then, their linear superposition $c_1|\psi_1\rangle + c_2|\psi_2\rangle$ with $c_i \in \mathbb{C}$ (and proper normalization) is also an allowed state of the system. This property is known as the *superposition principle*. It is at the core of quantum mechanics (*QM*) and has no classical counterpart. In the classical world, a bit could be either 0 or 1 but in *QM* the qubit can be in a superposition of those, i.e. in a new state that is both of them at the same time without being neither of them individually until a measurement is made.

- (**Postulate II**) To any given physical *observable* (i.e. a trait or property) "$\mathfrak{a}$" is associated a *Hermitian operator* A that acts on the Hilbert space $\mathscr{H}$ such that when a measurement of "$\mathfrak{a}$" is made on the physical system, we obtain one of the *eigenvalues* λ_i of A. Mathematically we write an eigenvalue equation

$$A\,|\lambda_i\rangle = \lambda_i\,|\lambda_i\rangle. \tag{1.12}$$

Let λ_1 and λ_2 be two eigenvalues of A and suppose the system is in a superposition $c_1|\lambda_1\rangle + c_2|\lambda_2\rangle$. If a measurement of the trait "$\mathfrak{a}$" is made, the system undergoes an *instantaneous* reduction to one of the two eigenstates $|\lambda_1\rangle$ or $|\lambda_2\rangle$ with probability of occurrence

$$p_1 = \frac{|c_1|^2}{\sqrt{|c_1|^2+|c_2|^2}} \text{ and } p_2 = \frac{|c_2|^2}{\sqrt{|c_1|^2+|c_2|^2}} \text{ respectively.}$$

This is known in the literature as the *collapse of the wavefunction*, and the complex coefficients c_i are called the probability amplitudes.

Definition 1.14. *Let "$\mathfrak{a}$" be a given physical observable with its unitary representation A and a given state $|\psi_i\rangle \in \mathscr{H}$ with probability of occurrence p_i, the* ***expectation value*** *of "$\mathfrak{a}$" is defined as*

$$\langle A\rangle = \sum_{i=1}^{N} p_i \langle\psi_i|A|\psi_i\rangle, \tag{1.13}$$

where N is the number of available states (to the observer) which are assumed to be properly normalized.

- (**Postulate II$'$**) We may reformulate *Postulate II* above in the language of pro-

jective measurements. We denote by $\{P_i\}_{i=0}^{n-1}$, where each $P_i = |i\rangle\langle i|$, the set of quantum measurements satisfying the following properties:
If the state of the system is $|\psi\rangle$ before the act of observation, which we equivocate with measurement, then the probability that outcome i occurs is given by the *expectation value* of P_i:

$$\langle\psi|P_i^{\dagger}P_i|\psi\rangle = \langle\psi|i\rangle\langle i|\psi\rangle = |\langle\psi|i\rangle|^2 = p_i,$$

and the sate of the system immediately after the measurement is

$$\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i^{\dagger}P_i|\psi\rangle}}.$$

The projection operators P_i satisfy the ***completeness relation***

$$\sum_i P_i^{\dagger}P_i = I. \tag{1.14}$$

In the case of qubits (i.e. when $n = 2$), the set of possible measurements in the computational basis is given by $\{P_0, P_1\}$ where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$.
For example, if the system was in the state $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, then the probability p_0 of the system to be found in the state $|0\rangle$ (i.e. to measure the outcome zero) is given by:

$$\langle\psi|P_0^{\dagger}P_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = |c_1|^2.$$

Immediately after the measurement the system is collapsed onto

$$\frac{P_0|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}} = \frac{c_1|0\rangle}{\sqrt{|c_1|^2}} = e^{i\theta}|0\rangle,$$

where we have written the complex number c_1 as $r_a e^{i\theta}$.
In quantum mechanics, we cannot distinguish between $e^{i\theta}|0\rangle$ and $e^{i\gamma}|0\rangle$. Global phase factors are irrelevant. This is because in the Hilbert space the entities we are dealing with are not exactly vectors but rather objects called *rays* (these are

equivalence classes of vectors that differ by multiplication by a nonzero complex number). On the other hand, an expression like $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is clearly different from $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (i.e. relative phase factors in state superpositions are physically relevant).

- (**Postulate III**) In non relativistic quantum mechanics, the time evolution of a given closed physical system is governed by the *Schrödinger* equation [58]

  $$i\hbar\frac{\partial|\psi\rangle}{\partial t} = \mathscr{H}|\psi\rangle, \tag{1.15}$$

  where $|\psi\rangle = |\psi(\vec{x},t)\rangle$ i.e. the wavefunction is both a function of position $\vec{x}$ and time parameter t. $\mathscr{H}$ is the *Hamiltonian* of the system, a Hermitian operator whose eigenvalues (in the matrix representation of quantum mechanics) are the possible energy levels of the system.

  In the ***Heisenberg picture*** [35] the states are time independent and evolve under the action of unitary operators $U(t)$ such that if the state of the system was $|\psi\rangle$ just before the evolution it is $U(t)|\psi\rangle$ immediately after. In *Quantum Information Theory* there is no explicit notion of time evolution (unless we consider physical realizations of quantum computers and we are back in the *Hamiltonian* formalism) so we mimic time evolution by comparing a state before the action of a given quantum gate and after. We read the *time evolution* by looking at a quantum circuit evolving from left to right i.e. from an *input* state to an *output* state.

1.1.2 The Density Matrix

We have described above in *postulate I* the state of a physical system by a normalized state vector $|\Psi\rangle \in \mathscr{H}$, but what if the state of the quantum system is not completely known? This is the general situation, and more often than not, we do not know what $|\Psi\rangle$ is. Only in very restricted scenarios do we know the entire wave function. So we describe our ignorance of the entire state by the *density matrix* formalism.

Definition 1.15. *Let $\{\psi_j\}$ form a normalized but not necessarily an orthogonal basis in $\mathscr{H}_N$ (i.e $\langle\psi_j|\psi_j\rangle = 1$) and let $\Omega_j = \{p_j\}_{j=1}^{N}$ be a probability distribution with $p_j \geq 0$ for every j such that $\sum_j p_j = 1$, and suppose a quantum system is in state $|\psi_j\rangle$ with probability of occurrence p_j, then the* density matrix *for the system can be expressed as*

$$\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j| \tag{1.16}$$

and is equivalent to the following conditions

1. *$tr(\rho) = 1$ (i.e. ρ is of unit trace)*
   For assume $\{e_k\}$ to be an orthonormal basis of $\mathscr{H}$ then

$$\begin{aligned} tr(\rho) = \sum_k \langle e_k|\rho|e_k\rangle &= \sum_j\sum_k \langle e_k|p_j|\psi_j\rangle \underbrace{\langle\psi_j|e_k\rangle}_{\delta_{jk}} \\ &= \sum_j p_j \underbrace{\sum_k \delta_{jk}^2}_{=1} = \sum_k p_k = 1. \end{aligned}$$

   where δ_{jk} is the Kronecker operator defined as:

$$\delta_{jk} = \begin{cases} 1 & \textit{if } j = k \\ 0 & \textit{if } j \neq k. \end{cases}$$

2. *ρ is a positive semi-definite operator.*
   That is

$$\langle\varphi|\rho|\varphi\rangle = \sum_j p_j\langle\varphi|\psi_j\rangle\langle\psi_j|\varphi\rangle = \sum_j p_j|\langle\psi_j|\varphi\rangle|^2 \geq 0$$

for all states $\varphi\rangle$.

A few remarks are in order about the density matrix formalism.

Remark 1.16. ***(Pure and Mixed States)***

① *A physical system given by the density matrix ρ as in Equation 1.16 is known as a **mixed state** while if all the p_j's except one are zero we call this a **pure state** i.e. the density matrix reduces to $\rho = |\psi\rangle\langle\psi|$.*

- *A state ρ is pure if and only if $\rho^2 = \rho$.*
- *A state ρ is pure if and only if $\mathrm{Tr}\rho^2 = 1$.*

Given a mixed state ρ and a bipartite system $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$:

- *A state ρ is called **uncorrelated** if it can be written as $\rho = \rho_A \otimes \rho_B$.*
- *It is called **separable** if it can be written as $\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$, where $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$ and it is called **entangled** if ρ does not admit such a decomposition (c.f. definition 1.13 as well).*

② *In view of the above, we note that the* mean value *or expectation value of an observable A (c.f. Equation 1.13) can be written in terms of the density matrix ρ as*

$$\langle A \rangle = \mathrm{Tr}(\rho A). \tag{1.17}$$

③ *The temporal evolution of the density matrix is given by the **Liouville-Von Neumann equation***

$$i\hbar \frac{d}{dt}\rho = [\mathscr{H}, \rho],$$

*where $\mathscr{H}$ is the Hamiltonian of the system and $[.\ ,\ .]$ denotes the **commutator** i.e. $[\mathscr{H}, \rho] = \mathscr{H}\rho - \rho\mathscr{H}$.*

Two important concepts in dealing with density matrices and composite systems are the *partial trace* and the *state purification* that we define respectively:

Definition 1.17. *Let $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ be a Hilbert space of a bipartite system (A and B) and let ρ be a density operator acting on the total Hilbert space $\mathscr{H}$.*
*We define the **partial trace** of ρ over $\mathscr{H}_B$ as an operator that acts on $\mathscr{H}_A$ as follows*

$$\rho_A = \mathrm{Tr}_B \rho \equiv \sum_j (I \otimes \langle j|)\rho(I \otimes |j\rangle), \tag{1.18}$$

where $\{|j\rangle\}$ is an orthonormal basis. This defines ρ_A uniquely, regardless of the choice of the orthogonal basis.

Thus ρ_A describes Alice's[2] partial knowledge of the full system. For example imagine we do not have access to system B (the natural situation in physics is the inside of a black hole) so we trace out that system (i.e. in the black hole context, we get ride of its unaccessible degrees of freedom).

More often than not, the physical system will be described by a mixed state density matrix. The following procedure defines what we call *state purification*, which is a procedure to transform a given general mixed state into a pure state.

Definition 1.18. *Let $\rho_A = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ be a general density matrix on Hilbert space $\mathscr{H}_A$. We introduce a second Hilbert space $\mathscr{H}_B$ such that[3] $|\mathscr{H}_A| = |\mathscr{H}_B|$ and a normalized state vector*

$$|\Psi\rangle = \sum_j \sqrt{p_j} |\psi_j\rangle \otimes |\varphi_j\rangle, \tag{1.19}$$

*where $\{|\varphi_j\rangle\}$ is an orthonormal basis for $\mathscr{H}_B$. This state vector $|\Psi\rangle$ is the **purification** of ρ_A.*

It is easy to verify that Equation (1.19) leads to the desired result. Consider the pure density matrix $\rho = |\Psi\rangle\langle\Psi|$.
We look at the partial trace (c.f. Def. 1.18) of ρ over system B

$$\begin{aligned} \mathrm{Tr}_B\rho = \mathrm{Tr}_B|\Psi\rangle\langle\Psi| &= \sum_{i,j,k} (\ I \otimes \langle\varphi_i|\ )\ \sqrt{p_j p_k}\ |\psi_j\rangle\ |\varphi_j\rangle\langle\psi_k|\langle\varphi_k|\ (\ I \otimes |\varphi_i\rangle\ ) \\ &= \sum_j p_j |\psi_j\rangle\langle\psi_j| = \rho_A. \end{aligned} \tag{1.20}$$

One of the driving theorems in QIT is the *no-cloning theorem* [66] which is a pure consequence of the linearity of quantum mechanics[4].

[2] Alice will be properly introduced shortly.

[3] In general there is no direct connection between the number of pure states that enter a mixture and the dimension of the Hilbert space.

[4] This would not be totally true if we consider measurements as well.

Theorem 1.19. *(**Quantum No-Cloning Theorem**) There does not exist any unitary operator U such that*
$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \quad \forall\, |\psi\rangle \in \mathscr{H}.$

Proof. Assume such an operator U exists, and that $|\psi\rangle$ and $|\varphi\rangle$ are two distinct and non-orthogonal states the operator U is to copy. Then, we must have that

$$\begin{aligned}
U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle, \\
U|\varphi\rangle|0\rangle &= |\varphi\rangle|\varphi\rangle \;\text{ and we get:} \\
\langle\psi|\varphi\rangle &= (\langle\psi|\otimes\langle 0|)I(|\varphi\rangle\otimes|0\rangle) \\
&= (\langle\psi|\otimes\langle 0|)\underbrace{U^{\dagger}U}_{I}(|\varphi\rangle\otimes|0\rangle) = (\langle\psi|\otimes\langle\psi|)(|\varphi\rangle\otimes|\varphi\rangle) = |\langle\psi|\varphi\rangle|^{2}.
\end{aligned}$$

Therefore, we reach a contradiction and such a copying operator does not exist.
In the last line of the proof, we used the fact that U was a unitary operator. Another way to prove the theorem is to use the linearity of quantum mechanics in the following way: Let $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be an arbitrary quantum state that we wish to clone so that $\alpha \neq 0$ and $\beta \neq 0$.

$$\begin{aligned}
U|\Psi\rangle|0\rangle = U\left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle &= \left(\alpha|0\rangle + \beta|1\rangle\right)\left(\alpha|0\rangle + \beta|1\rangle\right) \\
&= \alpha^{2}|00\rangle + \beta^{2}|11\rangle + \underbrace{\alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle}_{\text{cross terms}} \qquad (1.21)
\end{aligned}$$

But, from the linearity of quantum mechanics we also have that:

$$U|\Psi\rangle|0\rangle = \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle = \alpha|00\rangle + \beta|11\rangle. \qquad (1.22)$$

Comparing the two Equations (1.21) and (1.22) we see that we arrive at a contradiction due to the extra *cross term* in Equ.(1.21) because $\alpha \neq 0$ and $\beta \neq 0$.
Hence, such a U does not exist, and therefore an unknown arbitrary quantum state can not be cloned. □

ℹ $\mathscr{N}.\mathscr{B}.$ It is important to understand that the no cloning theorem applies to **un-**

known arbitrary states like the one in Eq.(1.1). While sets of entangled states (like those forming the Bell basis), although arbitrary in the sense that one can pick any of the four Bell basis with equal probability, can nevertheless be cloned on account of them being mutually orthogonal. The loophole is that the theorem does not apply if the states to be cloned are limited to $|0\rangle$ and $|1\rangle$ (or any set of mutually orthogonal states).

We present briefly some of the most important quantum protocols that will be used later in the text and are by now standard tools in QIT, and in doing so we introduce our first two famous cryptographic characters, Alice and Bob, who usually want to accomplish some given task.

- **Teleportation:** [6] This is the most important quantum protocol and the most famous of them all not only for its science fictional appeal but also for its power as to demonstrate what quantum protocols can achieve.
  - Alice wants to send Bob who is far away (even on astronomical distances) an *unknown* quantum state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ by just sharing an EPR pair and Local Operations and Classical Communication (LOCC).
  - Say they share the state $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
  - A calculation shows that their joint state is:

    $$|\Psi\rangle|\varphi^+\rangle = \frac{1}{2}(\ |\varphi^+\rangle|\Psi\rangle + |\psi^+\rangle(N|\Psi\rangle) + |\varphi^-\rangle(Z|\Psi\rangle) + |\psi^-\rangle(NZ|\Psi\rangle)\ ),$$

    where N is the negation operator Eq.(1.2), and Z the phase-flip operator Eq.(1.9) introduced above.
  - Alice applies $E^\dagger$ to her shares (where $E^\dagger$ is the reverse operator of E defined in Eq.(1.11) on page 9):

    $$(E^\dagger \otimes I)|\Psi\rangle|\varphi^+\rangle = \frac{1}{2}(\ |00\rangle|\Psi\rangle + |01\rangle(N|\Psi\rangle) + |10\rangle(Z|\Psi\rangle) + |11\rangle(NZ|\Psi\rangle)\ ).$$

  - Alice measures her qubits (and thus gets 2 classical bits of information) and sends her result to Bob who knows now what operator to apply to his share of the former EPR-pair so as to reconstruct the unknown state $|\Psi\rangle$.

Conclusion: $1ebit + 2bits \geq 1qubit$.

where by *ebit* which stands for an *e*ntangled qubit, we mean an EPR-pair.

- **Dense Coding:** This serves to transmit 2 bits of information using only 1 qubit and 1 ebit.
  - Alice and Bob share a Bell state say $|\varphi^{-}\rangle$.
  - Alice chooses one of the Bell states.
  - Alice acts on her qubit with an appropriate unitary transformation to transform it into her desired Bell state.
  - Alice sends Bob her qubit.
  - Bob applies $E^{\dagger}$ learning thus which Bell state he has, where E was defined in Eq.(1.11) above.

Conclusion: $1ebit + 1qubit \geq 2bits$.

1.1.3 The mathematics of the GHZ state

In this section we describe some of the important mathematical properties of the GHZ state, as it is one of the pillars of our main result on quantum secret sharing and is used extensively in the protocol we introduce in Section 3.3.2 of Chapter III.

Daniel M. Greenberger, Michael A. Horne and Anton Zeilinger introcuded the *GHZ state* in [33] as a way of proving that quantum mechanics was not local realistic (c.f. as well Bell's Theorem [4]). The n-party version of the GHZ state is given by

$$|\Phi^n_+\rangle = \frac{1}{\sqrt{2}}\overbrace{|00\ldots0\rangle}^{n}+\frac{1}{\sqrt{2}}\overbrace{|11\ldots1\rangle}^{n} = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\,. \qquad (1.23)$$

As the most frequently used multi-party entangled state, the GHZ state has appeared in applications such as nonlocality [46], communication complexity [18] and multi-party cryptography [10] (as we will see in chapter 3 when we discuss quantum secret sharing). Besides $|\Phi^n_+\rangle$ in Eq.(1.23) we define

$$|\Phi^n_-\rangle \equiv \frac{1}{\sqrt{2}}\overbrace{|00\ldots0\rangle}^{n}-\frac{1}{\sqrt{2}}\overbrace{|11\ldots1\rangle}^{n} = \frac{1}{\sqrt{2}}|0^n\rangle - \frac{1}{\sqrt{2}}|1^n\rangle\,. \qquad (1.24)$$

We mentioned above how the Hadamard transform acts on an arbitrary vector state

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle. \qquad (1.25)$$

Now, define ***the parity*** $P(x)$ to be

$$P(x) \equiv x\cdot y|_{y=(1,1,\cdots,1)} = (x_1\ 1+x_2\ 1+\cdots+x_n\ 1) \mod 2 = x_1+x_2+\cdots+x_n \mod 2.$$

$$\begin{aligned}
H^{\otimes n}|\Phi^n_+\rangle &= \frac{1}{\sqrt{2}}H^{\otimes n}(|00\ldots0\rangle+|11\ldots1\rangle)\\
&= \frac{1}{\sqrt{2}}(H^{\otimes n}|00\ldots0\rangle+H^{\otimes n}|11\ldots1\rangle)\\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{0^n\cdot y}|y\rangle+\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{1^n\cdot y}|y\rangle\right)\\
&= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{y=0}^{2^n-1}|y\rangle+\sum_{y=0}^{2^n-1}(-1)^{P(y)}|y\rangle\right)\\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y=0}^{2^n-1}\left(1+(-1)^{P(y)})|y\rangle\right) = \frac{1}{\sqrt{2^{n-1}}}\sum_{\substack{y=0\ s.t.\\ P(y)=0}}^{2^n-1}|y\rangle. \qquad (1.26)
\end{aligned}$$

Similarly, the action of the n-Hadamard transform on $|\Phi_-^n\rangle$ is given by:

$$H^{\otimes n}|\Phi_-^n\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{y=0 \ s.t. \\ P(y)=1}}^{2^n-1} |y\rangle. \tag{1.27}$$

For completeness, we give the effect of the phase-shift operator introduced in Eq (1.7) above on $|\Phi_+^n\rangle$ and $|\Phi_-^n\rangle$:

$$(I_{2^{k-1}} \otimes S_\theta \otimes I_{2^{n-k}})\,|\Phi_+^n\rangle = \frac{1}{\sqrt{2}}\Big(|00\ldots0\rangle + e^{i\theta}|11\ldots1\rangle\Big), \tag{1.28}$$

$$(S_{\theta_1} \otimes \cdots \otimes S_{\theta_n})|\Phi_+^n\rangle = (S_{\theta_1+\cdots+\theta_n} \otimes I_{2^{n-1}})|\Phi_+^n\rangle = \frac{1}{\sqrt{2}}\Big(|00\ldots0\rangle + e^{i(\theta_1+\cdots+\theta_n)}|11\ldots1\rangle\Big).$$

In particular we see that for $\theta = \pi$

$$(S_\pi \otimes I_{2^{n-1}})|\Phi_+^n\rangle = |\Phi_-^n\rangle. \tag{1.29}$$

Combining the last few results

$$\begin{aligned} H^{\otimes n}(S_{\theta_1} \otimes \cdots \otimes S_{\theta_n})|\Phi_+^n\rangle &= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} \Big(1 + e^{i\sum\theta_j}(-1)^{P(y)}\Big)|y\rangle \\ &= \begin{cases} \frac{1}{\sqrt{2^{n-1}}} \sum_{P(y)=0} |y\rangle & \text{if } \sum\theta_j = k\pi \text{ with } k \text{ even} \\ \\ \frac{1}{\sqrt{2^{n-1}}} \sum_{P(y)=1} |y\rangle & \text{if } \sum\theta_j = k\pi \text{ with } k \text{ odd.} \end{cases} \end{aligned} \tag{1.30}$$

This concludes our exposé of the preliminary chapter in which we have presented briefly the machinery of quantum information theory and the underlying postulates of quantum mechanics together with an express overview of the mathematics of the *GHZ* state.

CHAPTER 2

QUANTUM ERROR CORRECTION CODES

In this chapter, we explore the classical and quantum domains of coding theory, and various constructions pertinent to classical and quantum error correcting codes. The need for those topics will become apparent when we discuss quantum secret sharing schemes, where we will see how they are closely related to quantum error corrections[1]. For completeness, we have included an appendix on *Linear Algebra* (c.f. appendix I), which reviews some of the nomenclature and basic facts met in chapter one and in the subsequent sections.

2.1 From Classical Linear Codes to Quantum Error Correction

In discussing classical error correction which as we will see has a direct generalization in the quantum world, we will need a quick review of coding theory in its simplest form. That is in what follows unless explicitly stated we will concentrate on classical linear codes following J. Preskill's lecture notes on *QIT* [56].

Definition 2.1. *A* code $\mathbf{C}$ *of length n is a set of q-nary vectors of length n, called* codewords. *When* $q = 2$ *we talk about binary vectors and* $\mathbf{C}$ *becomes a* ***binary code***.

In the special case in which k bits are encoded in a binary string of length n, we designate from among the 2^n strings, a subset containing 2^k strings (i.e. a k-bit message is encoded by selecting one of those 2^k-words).

Let $\mathbb{F}_2$ denote the field of two elements $\{0,1\}$ defined by the operations in Table 2.1. $\mathbb{F}_2$ is also the ring of integers modulo 2, that is $\mathbb{Z}_2$.

Definition 2.2. *In a* binary linear code *the* codewords *form a k-dimensional closed linear subspace* $\mathbf{C}$ *of the binary vector space* $\mathbb{F}_2^n$, *where* $\mathbb{F}^n$ *is the n-dimensional vector space with entries in the field* $\mathbb{F}$.

[1] Mainly we will see that all quantum secret sharing schemes are quantum error correcting codes while the converse is not true.

Table 2.I: Addition and Multiplication Tables of the Binary Field $\mathbb{F}_2$.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

That is, in a binary linear code, we have that the *XOR* function[2] of two codewords is another codeword in the subspace and therefore we say that the code is additive. In addition we have that the code $\mathbf{C}$ satisfies that for any $\alpha \in \mathbb{F}_2$ and $c \in \mathbf{C}$, $\alpha c \in \mathbf{C}$.
The space $\mathbf{C}$ of the code is *spanned* by a basis of k vectors $\{c_1, c_2, ..., c_k\}$ so that an arbitrary codeword may be expressed as a linear combination of those basis vectors

$$c(\alpha_1, \cdots, \alpha_k) = \sum_i \alpha_i \, c_i,$$

where each $\alpha_i \in \{0,1\}$ and addition is modulo two.
Thus we say that the vector $\vec{c}$ of length n encodes the k-bit message $\alpha = (\alpha_1, \cdots, \alpha_k)$ via the k basis vectors $c_1, \cdots, c_k$, which may be assembled in a $(k \times n)$-matrix G.

Definition 2.3. *The matrix G formed by the basis vectors c_i is called the* generator matrix *of the code* $\mathbf{C}$ *and is of dimension* $(k \times n)$

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}, \tag{2.1}$$

and in matrix notation:

$$c(\alpha) = \alpha \; G \quad \textit{(we say that the matrix G acts on the left to encode } \alpha\textit{).} \tag{2.2}$$

Alternatively, the k-dimensional code subspace of $\mathbb{F}_2^n$ can be characterized by speci-

[2] Recall that the XOR function is just addition of vectors over the field $\mathbb{F}_2$ so in this context, we use the XOR-function, addition modulo 2 and the $\oplus$ operator interchangeably.

fying $(n-k)$ linear constraints.

Definition 2.4. *Thus we can define an* $(n-k)\times n$*-matrix* H *such that*[3]

$$H\ c^T = 0, \quad \forall\, \vec{c} \in \mathbf{C}. \tag{2.3}$$

H *is called* the parity check matrix *of the code* $\mathbf{C}$.

From this definition and Eq.(I.6) of Appendix I we see that the rows of H are $(n-k)$ linearly independent vectors and therefore $\mathbf{C}$ is the code space of vectors orthogonal to all those $(n-k)$ vectors.

Definition 2.5. *In this context,* Orthogonality *in* $\mathbb{Z}_2$ *is defined as follows:* $\forall\ \vec{x}, \vec{y} \in \mathbf{C}$ *where* $\vec{x} = (x_1, x_2, \cdots, x_n)$ *and* $\vec{y} = (y_1, y_2, \cdots, y_n)$ *we have that:*

$$\vec{x}\cdot\vec{y} = \sum_{i=1}^{n} x_i y_i \mod 2 = 0. \tag{2.4}$$

Example 2.6. *Let* $\vec{c}_1 = (0,1,1,0,1,0,1)$ *and* $\vec{c}_2 = (1,1,1,0,0,1,0)$. *Their inner product is*

$$\vec{c}_1\cdot\vec{c}_2 = (0\cdot 1 \oplus 1\cdot 1 \oplus 1\cdot 1 \oplus 0\cdot 0 \oplus 1\cdot 0 \oplus 0\cdot 1 \oplus 1\cdot 0) = 2 \equiv 0 \mod 2,$$

and therefore c_1 *and* c_2 *are orthogonal in* $\mathbb{Z}_2$.

Remark 2.7. *We also have that the rows of G are orthogonal to those of H*

$$H\ G^T = 0 \tag{2.5}$$

Let $\vec{e}$ be the n-component vector that characterizes the occurrence of an error in a given n-bit string.

The 1's in $\vec{e}$ mark the locations where errors occur.

Therefore when afflicted with $\vec{e}$, the n-bit string $\vec{c}$ becomes $\vec{c} \to \vec{c} + \vec{e}$.

[3] When we show explicitly $\vec{c}$ as the vector notation of the codeword c we really want to think of it as a vector in the code space; while if we write it as simply c, we think of it in terms of matrices (in that case a raw matrix in the code $\mathbf{C}$ i.e. $\vec{c} = c^T$).

Definition 2.8. *Some errors can be detected by applying the parity check matrix H to the corrupted vector*

$$H(c+e)^T = He^T \quad \textit{(where we have used Eq.(2.3)).}$$

He^T *is known as the* error syndrome.

We not in passing that when we do not explicitly show the vector arrow on a mathematical quantity, we have passed from the vector notation to the matrix form of the equation.

A few remarks are in order. Let $\mathscr{E}$ denote the set of errors $\{e_i\}$ that we wish to correct. Error recovery is possible in principal if and only if all the errors e_i have distinct error syndromes.
Only then can we flip back the bit via

$$c+e \to (c+e)+e = c+(e+e) = c.$$

(Recall that the arithmetic is done modulo two.)
We run into trouble when $He_1 = He_2$ for $e_1 \neq e_2$, since there is no way to distinguish between those errors. We can mistake e_1 for e_2 and vice versa

$$c+e_1 \to (c+e_1)+e_2 = \underbrace{c+(e_1+e_2)}_{\in \mathbf{C}} \neq c.$$

What really happens is that the information contents of the original codeword is altered. We start with the codeword c and end up with another *valid* codeword c' (i.e. in the code subspace $\mathbf{C}$) but different from c.

Definition 2.9. *The* ***distance*** $d(\mathbf{C})$ *of a code* $\mathbf{C}$ *is defined as the minimum distance between two distinct codewords.*

In a *linear code* $\mathbf{C}$, the *Hamming weight* is the number of non-zero entries of a given codeword $c \in \mathbf{C}$ denoted by $wt(c)$. While the *Hamming distance* d_H is the number of

1's present in the codeword c which is equal to the Hamming weight of the difference. In the case of a binary code, the hamming distance is equal to the Hamming weight of the sum.

More formally, the distance is the minimum weight of $\vec{y}$ such that

$$\exists\, \vec{x}, \vec{x}' \in \ \mathbf{C} \text{ and } \vec{x}+\vec{y}=\vec{x}'.$$

That is for a binary vector c with p 1's we say that it has a *Hamming weight* $wt(c) = p$ and that the *Hamming distance* between two codewords c_1 and c_2 is $d_H(c_1, c_2) = wt(c_1 + c_2)$.

In example 2.6 above the $wt(c_1) = wt(c_2) = 4$ we have that the Hamming distance between the two codewords c_1 and c_2 is

$$d_H(c_1, c_2) = wt(c_1 + c_2) = wt(1,0,0,0,1,1,1) = 4.$$

ℹ $\mathcal{N}.\mathcal{B}.$ A single bit-flip error generates a bit string whose Hamming distance differs by 1 from the original codeword. Furthermore, if we are dealing with binary vectors, for a code **C** with minimum distance d, any of those vectors is within Hamming distance $t = \lfloor \frac{d-1}{2} \rfloor$ of at most one codeword.

Definition 2.10. *The **support** of a vector c, denoted by $supp(c)$, is the set of coordinates of c where the corresponding entry is not* 0*, i.e.*

$$supp(v) = \{i : c_i \neq 0\}.$$

Back to our example 2.6 above, for the given codewords c_1 and c_2 we have that $supp(c_1) = \{2,3,5,7\}$ while $supp(c_2) = \{1,2,3,6\}$.

Finally, we are in a position to introduce the notion of classical error correcting codes.

Definition 2.11. *A linear code with length n, dimension k, and minimum distance $d =$*

$2t+1$ *is called an* $[n,k,d]$ *code and can correct t errors or detect (without correcting)* $2t$ *errors.*

Notation 2.12. *The general notation convention for a classical error correcting code is* (n,K,d) *where n is the number of physical bits,* $K=2^k$ *is the number of encoded bits and d is the distance. In definition 2.11 we used the notation* $[n,k,d]$*, which is usually reserved for a* Linear Error Correcting Code *(**LECC**).*

From now on, we will only consider binary codes unless explicitly stated.
We will also need the notion of the dual of a code $\mathbf{C}$ which is imperative for most constructions of classical and quantum codes.

Definition 2.13. *The **dual code*** $\mathbf{C}^\perp$ *of a code* $\mathbf{C}$ *is the set of vectors orthogonal to all codewords, that is*

$$C^\perp = \{v \in \mathbb{F}_2^n : v \cdot c = 0, \forall\, c \in \mathbf{C}.\}$$

The best way to understand the dual code $\mathbf{C}^\perp$ is by looking at the relationship between the check matrix H and the generator matrix G of the code $\mathbf{C}$.
Recall that the $(k \times n)$ generator matrix G and the $(n-k)\times n$ parity check matrix H satisfy

$$H\,G^T = 0 \quad \text{for the code } \mathbf{C}. \tag{2.6}$$

Taking the transpose of the above equation we get

$$(H\,G^T)^T = G\,H^T = 0.$$

So now H^T can be seen as the generator matrix, while G as the parity check matrix of an $(n-k)$-dimensional code which we denoted by $\mathbf{C}^\perp$ and called the *dual code* of $\mathbf{C}$.
Thus $\mathbf{C}^\perp$ is the orthogonal complement of $\mathbf{C}$ in $\mathbb{F}_2^n$.

Definition 2.14. *A vector is **self-orthogonal** if it has* even weight.

So it is possible for $\mathbf{C} \cap \mathbf{C}^\perp \neq \emptyset$.

Definition 2.15. ***Self-dual codes****: A code contains its dual if all its codewords have even weight and are mutually orthogonal. If $n = 2k$, it is possible to have $\mathbf{C} = \mathbf{C}^{\perp}$, in which case $\mathbf{C}$ is said to be* self-dual.

We also have the following important lemma relating a code and its dual.

Lemma 2.16. $\mathbf{C}$ *and* $\mathbf{C}^{\perp}$ *are related in the following useful way:*

$$\sum_{c\in\mathbf{C}}(-1)^{v\cdot c} = \begin{cases} 2^k & \text{if } c \in \mathbf{C}^{\perp} \\ \\ 0 & \text{if } c \notin \mathbf{C}^{\perp}. \end{cases} \tag{2.7}$$

The zero part of the above relation follows from the fact that given two strings c and w of length k

$$\sum_{c\in\{0,1\}^k}(-1)^{c\cdot w} = 0,\ w \neq 0.$$

If the vector $\vec{c}$ is an encoding of α (c.f. Eq.(2.2)), we have that $c = \alpha G$ and we get:

$$\sum_{c\in\mathbf{C}}(-1)^{v\cdot c} = \sum_{c\in\mathbf{C}}(-1)^{v\cdot\alpha G} = \sum_{\alpha\in\{0,1\}^k}(-1)^{\alpha\cdot vG} = 0, \forall\ vG \neq 0.$$

Since G, the generator matrix of $\mathbf{C}$ is the parity check matrix for $\mathbf{C}^{\perp}$ the sum vanishes whenever $c \notin \mathbf{C}^{\perp}$.

Several classical bounds are known for the given n, k, d parameters forming an $[n,k,d]$-error correcting code, but here we only give the *Singleton bound* and the *Hamming bound* [43]:

Theorem 2.17. *A classical $[n,k,d]$ linear error correcting code satisfies the* Singleton bound*, given by*

$$d - 1 \leq n - k. \tag{2.8}$$

Codes that satisfy the *Singleton bound* with equality are called *Maximum Distance Separable* or *MDS* codes for short. Those codes have special properties among the most

important ones is that if $\mathbf{C}$ is an *MDS*-code so is its dual $\mathbf{C}^{\perp}$.
We also give the *classical Hamming bound*, which has a direct quantum analog:

Theorem 2.18. *The* ***Hamming bound*** *for a classical linear q-nary code* $[n,k,d]_q$ *of distance d satisfies the following inequality*

$$k \leq n - \log_q \left(\sum_{i=0}^{t} \begin{pmatrix} n \\ i \end{pmatrix} (q-1)^i \right), \tag{2.9}$$

where $t = \lfloor \frac{d-1}{2} \rfloor$ *is the maximum number of errors that can be corrected by the given code.*

In particular for a binary error correcting code of distance $d = 3$, $[n,k,3]_2$ the Hamming bound simplifies to

$$k \leq n - \lg(n+1), \tag{2.10}$$

where lg is the base-two logarithm function.

2.1.1 Notions in *Q*uantum *E*rror *C*orrection *C*odes

In what follows, we will introduce enough nomenclature and tools to be able to connect *QECC* to *QSS* schemes.
Classically, in the case of a binary code, the only possible type of error that can occur is a bit flip, i.e. a $0 \to 1$ and vise versa. The simplest classical error correcting code that can handle this problem is the repetition code:

$$\begin{aligned} 0 \quad &\longrightarrow \quad 000 \overset{majority}{\longleftarrow} 010 \\ 1 \quad &\longrightarrow \quad 111 \overset{majority}{\longleftarrow} 101 \end{aligned}$$

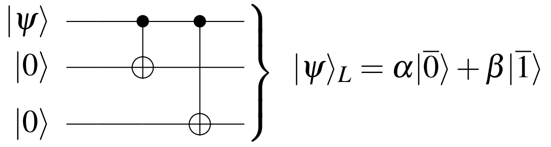
where we use the majority function i.e. if two of the bits are 0 then we flip the non-zero 1 back to 0 (since it is more probable that one bit was erroneously flipped rather than two). The same goes for the value 1 bit as well.

Now, a natural question to ask is: can we use the same technique quantum mechanically? Unfortunately, due to the No-Cloning theorem, we cannot do so; for we cannot copy non-orthogonal states (i.e. completely unknown states). Furthermore, how can we look at the quantum state in order to compute the majority (or parity)? For we know that any measurement or information gain about a quantum system disturbs the state in a non reversible way.

The first thing to note is that quantum mechanically, besides a bit flip, which is the same as applying the X Pauli operator to the qubit, we can have a phase flip as well. The latter is the same as applying the Z operator to the qubit. Furthermore, we can have both a phase flip and bit flip happening at the same time, which is the same as applying the Y operator to the qubit (c.f. remark 1.9 above). So, apart from taking into account the No-Cloning theorem and the measurement problem, we have to be able to correct for X, Z and Y-errors. Theorem 2.19 and remark 2.20 bellow illustrate the most general single-qubit error that can occur.

As we will see subsequently, the main idea in quantum error correction is to determine which bit is different without knowing its value.

Let $|\bar{0}\rangle = \overbrace{|00\cdots0\rangle}^{n}$ and $|\bar{1}\rangle = \overbrace{|11\cdots1\rangle}^{n}$ denote the *encoded* states or *logical* states. For simplicity, we will focus on the three-qubit error correcting code with $n=3$, which is the quantum analogue of the repetition code. We note in passing that the quantum circuit in



$|\psi\rangle$
$|0\rangle$
$|0\rangle$
$|\psi\rangle_L = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$

(2.11)

Figure 2.1: Encoding of the Quantum State Into the Logical State .

Fig. 2.1 allows us to prepare a 3-*GHZ* state[4] as well. But in the context of *QEC*-codes, the state$|\psi\rangle_L$ is called the *logical qubit*, while each individual qubit constituting it is known as the *physical qubit*. Furthermore, using the same terminology as in classical

[4] Actually, it prepares a generalized version of the GHZ-state, unless $\alpha = \beta = \frac{1}{\sqrt{2}}$.

coding theory, we will call the set:

$$\mathbf{C} = \{\alpha|000\rangle + \beta|111\rangle \; |\alpha, \beta \in \mathbb{C}, \; |\alpha|^2 + |\beta|^2 = 1\}$$

the *code* and each member of **C** a *codeword*.

ℹ$\mathscr{N}.\mathscr{B}$. It is important to note that the state $|\psi\rangle$ itself is not triplicated, only the basis states are triplicated. Hence, we are in no way violating the no-cloning theorem

$$|\psi\rangle_L \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3},$$

unless $\alpha = 0$ or $\beta = 0$. Now the protocol goes as follows:

(**Transmission**) Say Alice encodes the state $|\psi\rangle$ as shown above into $|\psi\rangle_L$ and sends the logical state to Bob through a quantum channel susceptible to noise. Let p denote the probability that a bit flip occurs due to that noisy quantum channel. We assume that p is sufficiently small so that not many such errors occur during the transmission. Clearly the state $|\psi\rangle_L$ will thus be transmitted with no error with a probability $p_{no\ error} = (1-p)^3$ while the probability of having only one error (say on the 1st, 2nd or 3rd qubit) is $p_{1\ error} = 3p(1-p)^2$. On the other hand, the probabilities of having two and three errors occurring (all bits are flipped) is given by $p_{2\ errors} = 3p^2(1-p)$ and $p_{all\ flip} = p^3$, respectively.

(**Error Syndrome Detection and Correction**) In order to detect any bit flip error, we need to look but not see, i.e. we need to locate the error without measuring the value of the qubit. To do so, we use the following quantum circuit (Fig. 2.12 on page 32) which is the quantum analogue of the classical error syndrome introduced in definition 2.8.

In order to correct for errors, Bob needs to prepare ancillary qubits in the state $|00\rangle$ as seen in Fig. 2.1.1. He then applies four CNOT gates (c.f. Eq.(1.3)) with the control bits being the encoded qubits and the target bits being his ancillary qubits.

Assuming that only bit-flip errors have occurred, let $|x_1x_2x_3\rangle$ be a basis vector Bob has received and let $|.\rangle_A$ and $|.\rangle_B$ be the final states of the first and second ancillary qubits

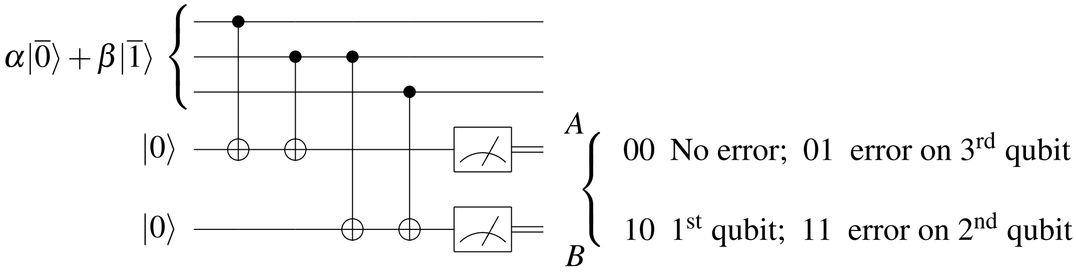

$\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$
$|0\rangle$
$|0\rangle$
A
B
00 No error; 01 error on 3rd qubit
10 1st qubit; 11 error on 2nd qubit

Figure 2.2: Error Syndrome Measurement.

respectively. Then the effect of the Error Syndrome circuit is to leave the final ancillary qubits in the respective states:

$$|x_1 \oplus x_2\rangle_A \ \text{ and } \ |x_2 \oplus x_3\rangle_B.$$

So we see that depending on which qubit was flipped (if any), the outcome of the error syndrome when measured will be as displayed in Table 2.II bellow.

Just to illustrate the above discussion, let's say Bob received the following state

$$|\psi\rangle_{e_1} = \alpha|010\rangle + \beta|101\rangle.$$

He applies the Error syndrome circuit (Fig.2.1.1) and thus is left with the following global state

$$|\psi\rangle_{Bob} = \alpha|01011\rangle + \beta|10111\rangle = |\psi\rangle_{e_1} \otimes |11\rangle.$$

Table 2.II: Error Syndrome Measurement and Bit Flip Correction.

Error syndrome	Operator needed for Correction
(00)	I No errors occurred
(01)	X_3 Error on 3rd qubit
(10)	X_1 Error on 1st qubit
(11)	X_2 Error on 2nd qubit

Now, Bob measures the ancillary qubits and finds the classical bits $\{11\}$ and thus he knows that an error occurred on the 2^{nd} qubit, so he applies:

$$X_2 = (I \otimes X \otimes I)\,(\alpha|010\rangle + \beta|101\rangle) = \alpha|000\rangle + \beta|111\rangle = |\psi\rangle_L. \ \surd$$

What if instead Bob receives the following state

$$|\psi\rangle_{e_2} = \alpha|101\rangle + \beta|010\rangle \ ?$$

If he applies the error syndrome circuit, he now has the global state:

$$|\psi\rangle_{Bob} = \alpha|10111\rangle + \beta|01011\rangle = |\psi\rangle_{e_2} \otimes |11\rangle.$$

And thus if Bob measures the ancillary qubits he ends up again with the classical bits $\{11\}$. He will erroneously conclude that the error occurred on the 2^{nd}-qubit and when he applies X_2 as above he ends up instead with

$$\alpha|111\rangle + \beta|000\rangle = N|\psi\rangle_L \neq |\psi\rangle_L.$$

Thus Bob ends up with the *negation* of the state instead of the desired state itself.

The way out of this is to look at the probabilities of occurrence of the above states so as to be able to recognize which state is which. For the state $|\psi\rangle_{e_1}$ the probability is given by $p_{e1} = p(1-p)^2$ since only one bit flip occurred; while that of $|\psi\rangle_{e_2}$ is given by $p_{e_2} = p^2(1-p)$.

To put numbers in, if the probability of an error to occur is $p = 0.1$ then $p_{e_1} = 0.081$ while $p_{e_2} = 0.009$ i.e. $p_{e_1} = 9p_{e_2}$. Furthermore, the probability that one or two errors to occur equals 0.972 while that of two or three errors to occur is 0.28. Therefore the probability of $N|\psi\rangle_L$ to occur is about 35 times less likely than that of $|\psi\rangle_L$.

What about phase flip errors?

We noted above, in discussing the Hadamard transform in Eq.(1.4) and Eq.(1.10), that the X and Z operators are related via:

$$HXH = Z \text{ and } HZH = X.$$

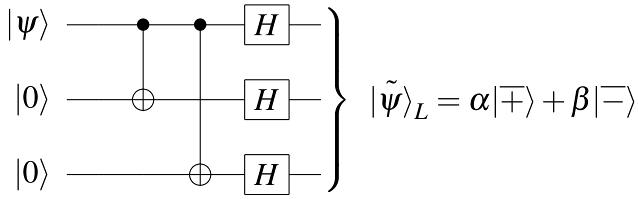
Furthermore, let $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ (the Hadamard basis introduced in Eq.(1.5) above). We have that the action of the Z and X operators on the Hadamard basis is given by

$$Z|+\rangle = |-\rangle \quad \text{and} \quad Z|-\rangle = |+\rangle, \tag{2.12}$$

$$X|+\rangle = |+\rangle \quad \text{and} \quad X|-\rangle = -|-\rangle. \tag{2.13}$$

This suggests that the Z operator is to the Hadamard basis what the X operator is to the computational basis. This means that the two errors, bit flip and phase flip, are related via the Hadamard transform and thus their correction is also related. This gives us grounds to suggest the encoding of

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{\tilde{E}} |\tilde{\psi}\rangle_L = \alpha|+++\rangle + \beta|---\rangle = \alpha|\overline{+}\rangle + \beta|\overline{-}\rangle.$$


$|\psi\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
$|\tilde{\psi}\rangle_L = \alpha|\overline{+}\rangle + \beta|\overline{-}\rangle$

(2.14)

Figure 2.3: $\tilde{E}$: The Encoding Circuit for the Phase Shift Error.

The error syndrome quantum circuit gets a slight modification as well with the introduction of single Hadamard gates on the first three quantum wires. The procedure for error detection and correction remains identical as in the bit-flip case, with the Z operator replacing the X operator in the previous discussion. For completness we show the circuit

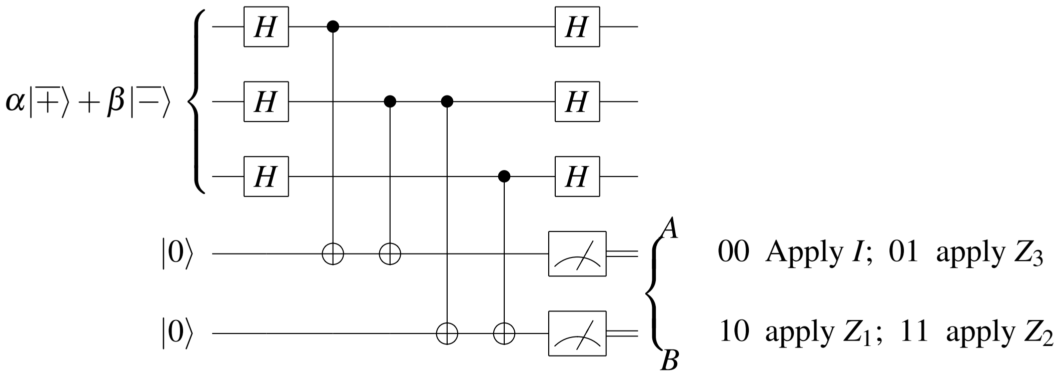

$\alpha|\overline{+}\rangle + \beta|\overline{-}\rangle$
H
H
H
H
H
H
$|0\rangle$
$|0\rangle$
A
B
00 Apply I; 01 apply Z_3
10 apply Z_1; 11 apply Z_2

Figure 2.4: Error Syndrome Measurement and Correction for Z-Errors.

The previous discussion applies to either a bit flip or a phase flip. To be able to correct for both errors at once, the nine-qubit code introduced by Peter Shor [61] comes to the rescue by using both codes at once.[5] We do not explain it here because it is not the most efficient single-error correcting code, nonetheless, it still achieves its goal. Since X and Z error corrections are independent the code can correct one of each such as $Y = iXZ$. What about correcting all single qubit errors?

Theorem 2.19. *If a quantum error correcting code corrects errors A and B, it also corrects $\alpha A + \beta B$.*

Remark 2.20. *We note that the most general* one qubit-*error that can occur can be written as a linear combination of the Pauli matrices i.e.*

$$\alpha I + \beta X + \gamma Y + \delta Z. \tag{2.15}$$

ℹ *Any* QECC *correcting single qubit errors X, Y and Z (plus the Identity) corrects every single-qubit error; and therefore correcting all t-qubit X, Y and Z-errors on t-qubits (+I) corrects all t-qubits errors.*

The last remark becomes more transparent if recast in the language of the *the Pauli group $\mathscr{G}_n$* which we now define:

[5] We give in example 2.24 bellow the list of all the Pauli operators that enables us to determine the error syndrome. For a detailed description of the original nine qubit code that does not employ the language of Pauli operators c.f. [61].

Definition 2.21. *(***The Pauli Group** $\mathscr{G}_n$*) We define the* ***Pauli group*** $\mathscr{G}_n$ *on n qubits to be generated by I, X, Y and Z on individual qubits. Then* $\mathscr{G}_n$ *consists of all tensor products of up to n operators I, X, Y and Z including the overall phases* $\{\pm i, \pm 1\}$*. (The phases are included to respect the closure property of the group, otherwise we would have tensor products that would not be in the group.)*

Properties:

- *Any* $M \in \mathscr{G}_n$ *satisfies* $M^2 = \pm M$.
- *If* $M, N \in \mathscr{G}_n$*, either* $MN = NM$ *or* $MN = -NM$*. That is, for every pair M and N of the Pauli group, either they commute or anticommute.*

Definition 2.22. *The* weight *of a Pauli operator* $M \in \mathscr{G}_n$ *is the number of non identity tensor factors in M or, equivalently, the number of qubits on which M acts as the non-identity operator.*

For example, $M = Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$ has weight equal to 2, while $N = I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X$ has weight equal to 6.

ℹ$\mathcal{N}.\mathcal{B}$. The weight-t Pauli errors form a basis for all t-qubit errors.

A few remarks are in order before we delve deeper into the machinery of *QECC*.

Remark 2.23. *We will work in the Hadamard basis defined in Eq.(1.5) and therefore the X operators and Z operators exchange roles, i.e. now X will correct a phase-flip error while Z will correct a bit-flip error.*

- *In the classical repetition code, a correctly encoded state* 000 *or* 111 *has the property that the first two bits have even parity as well as the second and the third. A state with an error on the first and second bits (or second and third) will show an odd parity. Thus, we say that a codeword (i.e. one without error) is a* $(+1)$*-eigenvector of* $Z \otimes Z \otimes I$ *and a state with an error on the first and second qubits is a* (-1)*-eigenstate of* $Z \otimes Z \otimes I$.

- *Similarly, for the* 3*-qubit phase error correcting code, a codeword has eigenvalue of* $(+1)$ *for* $X \otimes X \otimes I$ *whereas an eigenvalue of* (-1) *for* $X \otimes X \otimes I$ *if a phase error occurred on the first two qubits.*
  - *Thus measuring* $Z \otimes Z$ *detects bit flip (i.e.* X*) errors, while measuring* $X \otimes X$ *detects phase flip (i.e.* (Z)*) errors.*
  - *The error syndrome is formed by measuring enough operators to determine the location of the errors.*

Example 2.24. *We mentioned above Shor's nine-qubit code [61] we give here the list of all Pauli's operators that enable us to determine the error syndrome.*

$$\begin{aligned}
M_1 =&\ Z\otimes Z\otimes I\otimes I\otimes I\otimes I\otimes I\otimes I\otimes I; & M_5 =&\ I\otimes I\otimes I\otimes I\otimes I\otimes I\otimes Z\otimes Z\otimes I\\
M_2 =&\ I\otimes Z\otimes Z\otimes I\otimes I\otimes I\otimes I\otimes I\otimes I; & M_6 =&\ I\otimes I\otimes I\otimes I\otimes I\otimes I\otimes I\otimes Z\otimes Z\\
M_3 =&\ I\otimes I\otimes Z\otimes Z\otimes I\otimes I\otimes I\otimes I\otimes I; & M_7 =&\ X\otimes X\otimes X\otimes X\otimes X\otimes X\otimes I\otimes I\otimes I\\
M_4 =&\ I\otimes I\otimes I\otimes I\otimes Z\otimes Z\otimes I\otimes I\otimes I; & M_8 =&\ I\otimes I\otimes I\otimes X\otimes X\otimes X\otimes X\otimes X\otimes X.
\end{aligned}$$

The $\{M_1, \cdots M_8\}$ *form a group called the* ***Stabilizer*** *of the code. The group here consists of all the* M_i *Pauli operators with special properties that we give in the following definition. This deserves a section of its own.*

2.1.2 The Stabilizer Code Formalism

Definition 2.25. *Let* T *be a subspace of an n-qubit Hilbert space.*
Define a set:

$$S(T) = \{M \in \mathcal{G}_n :\ M|\psi\rangle = |\psi\rangle, \forall |\psi\rangle \in T\}. \tag{2.16}$$

$S(T)$ *is called the* ***stabilizer*** *of* T *with the following properties:*

Properties of The Stabilizer Code

1. *$S(T)$ is a group: M, $N \in S(T) \Rightarrow MN|\psi\rangle = M|\psi\rangle = |\psi\rangle$, (i.e. if M and N are in the group so is M group operator N where the group operator here is matrix multiplication).*

2. *$S(T)$ is an* Abelian *group*[6]*:*
$M,N \in S(T) \Rightarrow MN|\psi\rangle = |\psi\rangle = NM|\psi\rangle \Rightarrow [M,N]|\psi\rangle = 0, \forall\ |\psi\rangle \in T$.
ℹ*Recall that in quantum mechanics, operators that do not commute can not be measured simultaneously.*

3. *$-I \notin S(T)$, since $-I|\psi\rangle = -|\psi\rangle \neq |\psi\rangle$ (i.e. has (-1) as eigenvalue).*

4. *From $(1)+(2)+(3)$ above $\Rightarrow |S(T)| = 2^r$ where r is the number of generators*[7] *$M_1, \cdots, M_r$ and thus a general element can be written as $M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r}$ where $a_i \in \{0,1\}$.*

Definition 2.26. *Given an Abelian group S of Pauli operators, define a code space $T(S) = \{|\psi\rangle :\ M|\psi\rangle = |\psi\rangle, \forall\ M \in S\}$. Then, $T(S)$ encodes k-logical qubits in n-physical qubits when S has $n-k$ generators and has dimension $|T(S)| = 2^{n-k}$.*

Remark 2.27. *We note in passing that we refer to either S or $T(S)$ as the stabilizer code, where S is an Abelian subgroup of $\mathscr{G}_n$. Other names for the stabilizer code are:* symplectic code*, or* additive *or* additive $GF(4)$.

Definition 2.28. *Let S be a stabilizer and $T(S)$ the corresponding quantum error correcting code. We define the* Normalizer

$$N(S) = \{P \in \mathscr{G}_n : MP = PM, \forall\ M \in S\}. \tag{2.17}$$

The following theorem relates the *normalizer* to the *stabilizer* and to error correcting criteria.

Theorem 2.29. *Let S be a stabilizer code with r-generators on n-qubits. Then:*

[6] Recall that the M's and N's are tensor products of Pauli matrices.
[7] C.f. definition 2.26.

1. *dim $T(S) = |T(S)| = 2^{n-r}$ (where the number of encoded qubits $= k = n-r$).*
2. *Let $N(S) = S^{\perp} = \{P \in \mathscr{G}_n : PM = MP, \forall\, M \in S\}$, then S can detect errors outside $N(S)\backslash S$.*

Remark 2.30. *We make some important remarks on the previous theorem 2.29.*

- *(Remark on (1) in the theorem): Every time we add a Pauli operator, we divide the space by two (since we have (± 1)-eigenvalues). We continue on doing so till we have exhausted all the r generators i.e. we have divided the space by 2^r (c.f. item (4) in definition (2.25) above) and therefore the dimension of the stabilizer $|T(S)| = \frac{2^n}{2^r} = 2^{n-r}$.*
- *(Remark on (2) in the theorem): Informally, $N(S)$ is the set of all Pauli operators that commute with everything in the stabilizer. We sketch a proof of (2) since it will illustrate how the entire machinery is related to formal quantum error correction.*

  Proof. Suppose $M \in S$ and $P \in \mathscr{G}_n$ where P is an error that occurred. Therefore, P anticommutes with all elements of S i.e. $\{P, M\} = 0$ for all $M \in S$.

  We thus have that $M(P|\psi\rangle) = -PM|\psi\rangle = -P|\psi\rangle$.

  $\Rightarrow\ P|\psi\rangle$ is an eigenvector of M with eigenvalue $\{-1\}$.

  Suppose $P \in \mathscr{G}_n$, $[P, M] = 0$, $\forall\, M \in S \ \Leftrightarrow P \in N(S)$ (by definition of $N(S)$).

  Then for all $M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle \Rightarrow P|\psi\rangle$ is an eigenvector of M with eigenvalue $\{+1\}$.

  Therefore $P|\psi\rangle \in S(T)$ (i.e. $P|\psi\rangle$ is a valid codeword).

  We conclude that P is an undetectable error *except* if $P|\psi\rangle = |\psi\rangle$, $\forall\, |\psi\rangle \in T(S) \Leftrightarrow P \in S$.

  Therefore we need to mod $N(S)$ by those P's in S that are undetectable errors or are even valid codewords. □

(Conclusion:)

ℹ *Given the eigenvalue of an operator $M \in S$ (the stabilizer), one can detect errors E that anticommute with $M \in S$ and therefore, the code $T(S)$ detects errors that are not in*

$N(S)\backslash S$.

ℹℹ *Just as classical codewords vanish under the action of the parity check matrix (c.f. definition 2.4 and Eq.(2.3)), elements of the quantum code are fixed (or stabilized) by each stabilizer.*

Definition 2.31. *Let S be the stabilizer and $T(S)$ the corresponding quantum error correcting code. The* distance *d of $T(S)$ is defined to be the weight (c.f. definition 2.22) of the smallest Pauli operator M in $N(S)\backslash S$.*

Remark 2.32. *A stabilizer code of distance d, corrects $\lfloor (d-1)/2 \rfloor$-errors. Thus to correct t-errors, we need the distance $d = 2t+1$.*

In this context, we have the following definition of *error syndrome*.

Definition 2.33. *The* error syndrome (E.S.) *of the stabilizer code, is the list of eigenvalues of the generators of S. In general, for a stabilizer code the error syndrome of $F \in \mathscr{G}_n$ is given by an r-bit binary vector $\vec{e}$ such that:*

$$e_i = \begin{cases} 0, & \text{if } [E,F] = 0 \\ \\ 1, & \text{if } \{E,F\} = 0. \end{cases} \tag{2.18}$$

The Syndrome(EF)=Syndrome(E)+Syndrome(F) (in binary).
If however, the Syndrome(E) =Syndrome(F) $\Leftrightarrow$ Syndrome(EF) $=_{\oplus_2} 0 \Leftrightarrow EF \in N(S)$ (i.e. we cannot distinguish between E and F.) More precisely, E and F have the same E.S. *if and only if $E^\dagger F$ is in $N(S)$ and thus, E and F commute with the same set of generators of S.*
ℹ *If $E^\dagger F \notin N(S)$, the* E.S. *can distinguish between them.*

☞ The code corrects errors for which $E^\dagger F \notin N(S)\backslash S$ for all possible pairs of error (E,F).

ℹ $\mathscr{N}.\mathscr{B}$. If there exist some errors in S that keep the codewords fixed, then we say that the *QECC* is *degenerate*.

We are finally in a position to state the most general conditions for quantum error correction, which are given by the following theorem:

Theorem 2.34. *Suppose $\mathscr{E}$ is a linear space of errors acting on the Hilbert space$\mathscr{H}$ and let* $\mathbf{C}$ *be a subspace of $\mathscr{H}$. Denote the encoded basis states by $\{|\overline{\psi_i}\rangle\} \in \mathbf{C}$, and the basis errors by $\{E_a\}$ (with all the $\{E_a|\overline{\psi_i}\rangle\}$ mutually orthogonal). Let $S_a = \{E_a|\overline{\psi_1}\rangle, E_a|\overline{\psi_2}\rangle, \cdots\}$ denote the measure subspaces.*
Given a map $S_a \longrightarrow \mathscr{H}_L$ that takes $E_a|\overline{\psi_i}\rangle \longmapsto |\overline{\psi_i}\rangle$, the following are equivalent:

1. *$\{|\overline{\psi_i}\rangle\}$ forms a basis for a* QECC *correcting $\mathscr{E}$ (or the Span$(\mathscr{E})$).*
2. *$\langle\overline{\psi_i}|E_a^\dagger E_b|\overline{\psi_j}\rangle = \Lambda_{ab}\delta_{ij}$,*
   where Λ_{ab} is a Hermitian matrix independent of both i and j.
3. *The subspace* $\mathbf{C}$ *of $\mathscr{H}$ forms a quantum error-correcting code correcting errors $\mathscr{E}$ if and only if*

$$\langle\overline{\psi}|E^\dagger E|\overline{\psi}\rangle = \Lambda(E). \tag{2.19}$$

for all $E \in \mathscr{E}$. The function $\Lambda(E)$ is independent of the state $|\overline{\psi}\rangle$.

Proof. We sketch the idea behind the proof.

- (②⟺①) Diagonalize the matrix Λ_{ab} by choosing a different basis $\{F_a\}$ for $\mathscr{E}$.
- (①⟺③) Here we use the recovery condition from the main theorem of [49].
  Let U be the recovery map such that

$$U\left(E|\overline{\psi}\rangle\right) = a|\overline{\psi}\rangle|anc_1\rangle;\;\; U\left(E|\overline{\varphi}\rangle\right) = b|\overline{\varphi}\rangle|anc_2\rangle,$$

$$\Rightarrow UE\left(|\overline{\psi}\rangle + |\overline{\varphi}\rangle\right) = c\left(|\overline{\psi}\rangle + |\overline{\varphi}\rangle\right)|anc_3\rangle = a|\overline{\psi}\rangle|anc_1\rangle + b|\overline{\varphi}\rangle|anc_2\rangle.$$

  We find that $\langle\overline{\psi}|E^\dagger E|\overline{\psi}\rangle = |a|^2 = |b|^2 = \langle\overline{\varphi}|E^\dagger E|\overline{\varphi}\rangle$.

- (③⟺②) Consider $E = E_a \pm E_b$; $E_a \pm iE_b$. We compute $\langle\overline{\psi_i}|E_a^\dagger E_b|\overline{\psi_i}\rangle = \Lambda_{ab}$ for all encoding $|\overline{\psi}\rangle$ while choosing for $|\overline{\psi}\rangle = |\overline{\psi_i}\rangle \pm |\overline{\psi_j}\rangle; |\overline{\psi_i}\rangle \pm i|\overline{\psi_j}\rangle$ and we get ②.

□

We comment on the meaning of the above theorem in the following remark.

Remark 2.35. *We recast the equivalent conditions of the theorem using $E = E_a^\dagger E_b$ where E now is any operator acting on $2t$ qubits:*

- ② *is replaced by* ❷.

  ❷ *For any orthonormal basis $\{|\overline{\psi}\rangle\} \in \mathbf{C}$,*

  $$\langle\overline{\psi_i}|E|\overline{\psi_j}\rangle = 0, \quad (i \neq j), \tag{2.20}$$

  $$\langle\overline{\psi_i}|E|\overline{\psi_i}\rangle = \Lambda(E), \;\; \textit{for all operators } E \textit{ acting on } \mathscr{E}. \tag{2.21}$$

  What Eq.(❷.2.20) says is that in correcting errors, we will never confuse two different basis vectors. While Eq.(❷.2.21) says that learning about the error can not give us any information whatsoever about which of the basis states we have. This knowledge would constitute a measurement, which in turn would collapse the superposition of basis vectors and thus would disturb the original state. As a consequence, this will prevent us from learning about the error in the first place and thus we spiral down into a tautological logic. This will be a very crucial point when we prove some of the most important theorems in quantum secret sharing.

- ③ *is replaced by* ❸.

  ❸ *For any properly normalized codeword $|\overline{\psi}\rangle \in \mathbf{C}$, and all E acting on $\mathscr{E}$*

  $$\langle\overline{\psi}|E|\overline{\psi}\rangle = \Lambda(E). \tag{2.22}$$

  *What Eq.(❸.2.22) says is that protecting the state against errors (or noise) is the same as preventing the environment from extracting any information about that state. Here one can think of the environment as representing any set that is not allowed to look at the state; a set known as an **unauthorized set** in secret sharing nomenclature.*

In terms of density matrices, for a non-degenerate code of distance d, and codeword $|\overline{\psi}\rangle$, choosing any t qubits in the block has the property that if we trace over the remaining $(n-t)$ qubits we obtain

$$\rho_t = Tr_{n-t}|\overline{\psi}\rangle\langle\overline{\psi}| = \frac{I}{2^t}, \tag{2.23}$$

That is, we get the totally mixed density matrix, which is again to say that in a $d = (t+1)$-code, we cannot aquire any information about the encoded data by observing any t-qubits in the block ($\rho_t \propto$ a constant matrix independent of the codeword).

We now give the formal definition of a quantum error correction code.

Definition 2.36. *An $((n,K,d))$ is a **QECC** encoding a K-dimensional subspace into n physical qubits with distance d, which for Stabilizer codes is an $[[n,k,d]]$-quantum error correcting code with $K = 2^k$.*

We can now recast definition 2.31 in light of theorem (2.34) and summarize the essence of quantum error correction in the following corollary.

Definition 2.37. *The* distance *of a* QECC *is defined as the minimum-weight Pauli operator P for which*

$$\langle\overline{\psi_i}|P|\overline{\psi_j}\rangle \neq \Lambda(P)\delta_{ij}.$$

Corollary 2.38. *An $[[n,k,d]]$-*QECC*:*

❶ *of distance $2t+1$ will correct t qubit errors (i.e. if $Q = Q_1 \otimes \cdots Q_n$ where $Q_i : \mathscr{H}_i \to \mathscr{H}'_i$ acts as a quantum channel, then Q acts as the identity on $n-t$ qubits and may do anything on t qubits).*

❷ *of distance d will correct $(d-1)$-qubit erasure errors (those are the errors that occur at known locations, that is the quantum channel Q now produces an extra register that tells us which t-qubits were affected).*

We commented above (c.f. ℹ$\mathscr{N}.\mathscr{B}.$ after def. 2.33) on the degeneracy of a *QECC*. Here we state explicitly when this degeneracy occurs.

Definition 2.39. *A QECC is* degenerate *for a set of linearly independent sets of errors $\mathscr{E}$ if the Hermitian matrix Λ_{ab} (in theorem2.34) does not have maximum rank (i.e. not all the columns are linearly independent). Moreover, it is* degenerate *if it is degenerate for $\mathscr{E}$=$\{P \in \mathscr{P}_n : wt(P) < t, d = 2t+1\}$.*

ℹ $\mathscr{N}.\mathscr{B}.$ a non-degenerate code takes linearly independent errors to linearly independent states, but this is no longer true if the code is degenerate.

Remark 2.40. *In a* non-degenerate *stabilizer code, the distance $d =$* min*(weight) in $N(S)$. Otherwise, we need to look at the minimum weight in $N(S)\backslash S$ to get the distance of the stabilizer code.*

2.2 The Making of Quantum Codes

We briefly give some constructions of important quantum codes since both quantum error correction and quantum secret sharing are quantum codes after all.

2.2.1 Hamming Codes and Calderbank-Shor-Stean (CSS)-Codes

Let r denote the length of the vectors in the code **C**. The classical linear code $[n,k,d]$ has a generator matrix G (c.f. Eq.2.1) of $n = 2^r - 1$-linearly independent columns and $k = n - r$-raws (encoded bits).

Example 2.41. $[7,4,3]$-***Hamming Code***

*We take $r = 3$ here for the sake of the discussion and to simplify the constructions. We will build a 3-*Error Correcting Code *(*ECC*). Therefore, $n = 2^3 - 1 = 7$; $k = n - r = 7 - 3 = 4$; with $d = 3$ and therefore defines a $[7,4,3]$-code that can thus correct $t = \lfloor \frac{d-1}{2} \rfloor = 1$-error. The parity check matrix H (c.f. definition2.4) is given by:*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \tag{2.24}$$

While G has to satisfy $HG^T = 0$ (i.e. we need 4-raws perpendicular to the 3-raws in H) and thus

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \qquad (2.25)$$

In general, whenever the codes are linear (which is the only case we have considered here) we can convert from a classical code to a stabilizer code by converting:
The Parity check matrix ⟶ Stabilizer; that is the raws of H ⟶ generators of the code space S.

Example 2.42. $[7,4,3]$-***Hamming Code***$\longrightarrow$ $[[7,1,3]]$**-** ***quantum Code***
For example to convert the $[7,4,3]$-classical code above into a quantum code S we do the following:

- *To correct one bit flip, convert the 1's in $H \xrightarrow{to} Z$'s, and the 0's to I in the quantum code S.*
  H in Equation (2.24) is converted to:

$$\left.\begin{array}{c} Z\,Z\,Z\,Z\,I\,I\,I \\ Z\,Z\,I\,I\,Z\,Z\,I \\ Z\,I\,Z\,I\,Z\,I\,Z \end{array}\right\} \mathbf{C}_1. \qquad (2.26)$$

- *To correct one phase shift error, convert the 1's in $H \xrightarrow{to} X$'s, and the 0's to I.*
  Once again, H in Equation (2.24) is converted to:

$$\left.\begin{array}{c} X\,X\,X\,X\,I\,I\,I \\ X\,X\,I\,I\,X\,X\,I \\ X\,I\,X\,I\,X\,I\,X \end{array}\right\} \mathbf{C}_2. \qquad (2.27)$$

If we put the two codes thus formed $\mathbf{C}_1$ *and* $\mathbf{C}_2$ *we can correct a bit flip and a phase flip error. The quantum code we get is now*

$$\left.\begin{array}{l} (n-k_2)-raws\left\{\left.\begin{array}{c} X\,X\,X\,X\,I\,I\,I \\ X\,X\,I\,I\,X\,X\,I \\ X\,I\,X\,I\,X\,I\,X \end{array}\right\}\mathbf{C}_2\right. \\ (n-k_1)-raws\left\{\left.\begin{array}{c} Z\,Z\,Z\,Z\,I\,I\,I \\ Z\,Z\,I\,I\,Z\,Z\,I \\ Z\,I\,Z\,I\,Z\,I\,Z \end{array}\right\}\mathbf{C}_1.\right. \end{array}\right\}[[7,1,3]]-quantum\ code. \tag{2.28}$$

2.2.1.1 CSS-Codes

Let $\mathbf{C}_1$ be a classical linear code as defined in the previous section with an $(n-k_1)\times n$ -parity check matrix H_1, and let $\mathbf{C}_2$ be a *subspace* of $\mathbf{C}_1$ with $(n-k_2)\times n$-parity check matrix H_2 (with $k_2 < k_1$).
Let the first $(n-k_1)$-rows of H_2 coincide with those of H_1. Thus each word in $\mathbf{C}_2$ is contained in $\mathbf{C}_1$ since there is an additional (k_1-k_2)-linearly independent rows and we write $\mathbf{C}_2 \subset \mathbf{C}_1$.

Codewords in C_2 obey the following linear constraint: The sub-code C_2 defines an *equivalence relation* in C_1 in the following sense:

Definition 2.43. *We say that* $u,v \in \mathbf{C}_1$ *are* ***equivalent*** *(*$u \equiv v$*) if and only if there exists a codeword* $w \in \mathbf{C}_2$ *such that* $u = v + w$*.*

The ***equivalence classes*** are the ***cosets*** of C_2 in C_1.

Next, we form a stabilizer code from those two codes as described in Example 2.42 above.
Thus if $\mathbf{C}_1$ is an $[n,k_1,d_1]$-code and $\mathbf{C}_2$ is an $[n,k_2,d_2]$-code then the ***CSS-code*** is given by

$$[[n,n-(n-k_1)-(n-k_2),d]] = [[n,k_1+k_2-n,d]], \quad \text{with } d \geq \min(d_1,d_2). \tag{2.29}$$

In our previous Example2.42 we had $[[n,k_1+k_2-n,d]] = [[7,4+4-7,3]] = [[7,1,3]]$-

quantum (stabilizer) code as we mentioned above.

The following theorem gives us a basis of vector states for a well specified *CSS*-code.

Theorem 2.44. *Let* $\mathbf{C}_1$ *and* $\mathbf{C}_2$ *be* $[n,k_1,d_1]$ *and* $[n,k_2,d_2]$ *classical linear codes, such that* $\mathbf{C}_2 \subset \mathbf{C}_1$ *and that both* $\mathbf{C}_1$ *and* $\mathbf{C}_2^{\perp}$ *correct* t*-errors. Then for every coset leader* u *of* $\mathbf{C}_1 \backslash \mathbf{C}_2$ *the quantum states given by*

$$|u+\mathbf{C}_2\rangle = \frac{1}{|\mathbf{C}_2|} \sum_{v \in \mathbf{C}_2} |u+v\rangle, \tag{2.30}$$

form a basis for the staibilizer code $[[n,k_1-k_2,d]]$*, with* $d = \min(d_1,d_2)$ *which is able to correct* t*-errors. This code is called* ***Claderbank-Shor-Stean code*** *of* C_1 *over* C_2*.*

Binary *CSS* codes are just a subclass of the more general class of stabilizer codes.

2.2.2 Important Bounds on Quantum Codes

We mentioned above that Shor's nine-qubit code [61] was not not the most effective single error correcting code. So natural questions to ask are: How much better can we do? What constraints are there on the number of encoded bits needed to correct a given error? In this subsection we give some of the most important *quantum bounds* that should shed some light on those questions.

2.2.2.1 The Quantum Hamming Bound

Consider an $[[n,k,d]]$-quantum code with distance $d = 2t+1$. Suppose this code is non degenerate (c.f. definition 2.39).
On any given qubit, there are three possible linearly independent errors (X,Y or Z).
Thus there are

$$3^l \begin{pmatrix} n \\ l \end{pmatrix} = 3^l \frac{n!}{l!(n-l)!},$$

distinct errors in l-qubits out of a block of n-qubits. the total number of ways to have at most t-errors in those n-qubits is given by:

$$\sum_{l=0}^{t} 3^l \begin{pmatrix} n \\ l \end{pmatrix}.$$

If there are k-encoded qubits , then there are 2^k-linearly independent codewords while there are 2^n-orthogonal states in a Hilbert space describing n-qubits. The Hilbert space spanning those 2^n-states has to be large enough to encompass the total number of possible errors of weight up to t taking into account the 2^k- linearly independent codewords. So we arrive at:

$$2^k \sum_{l=0}^{t} 3^l \begin{pmatrix} n \\ l \end{pmatrix} \leq 2^n.$$

Rearranging terms we finally get the ***Quantum Hamming Bound***

$$\sum_{l=0}^{t} 3^l \begin{pmatrix} n \\ l \end{pmatrix} \leq 2^{n-k}. \tag{2.31}$$

For a code encoding a single qubit $k = 1$ and correcting a single error $t = 1$ we get from the Hamming bound $1 + 3n \leq 2^{n-1}$ which is valid for $n \geq 5$. Saturation of the bound gives us a $[[5, 1, 3]]$-quantum code correcting a single error and of distance $d = 3$. This reduction in the number of qubits required for *QECC* was due to DiVencenzo and Shor [26]. From the above bound $n = 5$ is the optimal number to correct all types of single-qubit errors.

2.2.2.2 The No-Cloning Bound and the Quantum Singleton Bound

We focussed in the previous paragraph on non-degenerate codes and derived the quantum Hamming bound and found that $n = 5$ was saturating this bound. Now what if non-degenerate codes were able to give us a lower bound on n say $n = 4$. If this was the case we would be able to have a $[[4, 1, 3]]$-quantum code correcting a single bit error. But a code that can correct t errors at arbitrary location can correct $2t$-errors at known locations (c.f. Corollary 2.38). Then this would allow us to use this $[[4,1,3]]$-*QECC* to encode a single qubit into one block of four and split this block into two sub-blocks each containing two qubits. If we append $|00\rangle$ to each of the sub-blocks, the original block would have been replicated twice. Moreover since we can correct $2t$ errors whose location we know, we can thus use this procedure to correct for errors in each block and recover the original quantum state. Thus we would end up with two faithful copies of the original quantum state which would clearly violate the no-cloning theorem 1.19.

Generalizing the above reasoning, for an $[[n,k,d]]$- quantum error code correcting $d-1=t$-errors we get the ***no-cloning bound***

$$n > 2(d-1) \tag{2.32}$$

The factor of 2 is reminiscent of not violating the no-cloning theorem. Therefore whether the code is degenerate or not, $n=5$ is the best we can do.

An improvement on the *no-cloning bound* Eq.(2.32) above is the ***quantum singleton bound*** which we give without proof (c.f. Preskill for a detailed proof based on the subadditivity of the Von Neumann entropy)

$$n-k \geq 2(d-1). \tag{2.33}$$

2.3 Summary

We gave a quick yet thorough review of classical and quantum error correcting codes. We saw that quantum and classical codes are in many respects similar. In classical coding theory, logical codes of k-bits are encoded into codewords of $n>k$-bits. Those n-bits are chosen among a larger set of 2^n-*possible* words of n-bits in such a way that an alteration to at most t-bits of those (due to noise or any source of error) can be recovered. Thus this specific set of codewords form an $[n,k,t]$-code which encodes k-bits into n-bits and corrects at most t-bits. The repetition code is the simplest example of such codes, where we have $k=1$, $n=3$ and $t=1$ giving us a $[3,1,1]$-classical code. On the other hand, in quantum error corrections, the main problem is to find a suitable set of 2^k-quantum codewords of n-qubits such that quantum information can be protected from interactions with the environment which usually leads to the corruption of the quantum data. Those quantum-codewords form a $[[n,k,d]]$-quantum error correcting code which corrects up to $d-1$ errors where d is the distance of the code.

CHAPTER 3

FROM CLASSICAL TO QUANTUM SECRET SHARING

In this chapter, we will explore a domain of cryptography that is (in my opinion) one of the most elegant subjects in this discipline, namely secret sharing, which was introduced independently in 1979 by Blakley [7] and Shamir [59] as a way to solve the problem of secure key distribution among several parties. The beauty of this branch of cryptography emanates not only from its practical use, but especially from relating diverse subjects from different branches of mathematics and computer science, from graph theory to coding theory and error correction codes, from geometric constructions to algebraic ones and beyond.

3.1 The Classical World

In this section we start by exploring the classical domain of secret sharing and in doing so we will need to review some known concepts, definitions and various constructions pertinent to classical secret sharing protocols. These constructions will pave the way for the quantum domain, which as we will see is quite different from its classical counterpart and will be the subject of the next section.

3.1.1 Classical Secret Sharing

Imagine a bank manager who is going abroad and would like to delegate his secret combination (to the vault) to his sub managers (say there are n of them), in such a way that not trusting individually anyone in particular he would like that at least k of them (with $k \leq n$) be present at any given time when the secret combination is to be used. Those k sub-managers have to cooperate all together to reconstruct the secret while any $k-1$ of them get absolutely no information about the secret. This is known as a (k,n)-threshold scheme, which is an example of the more general problem known as *secret sharing*. It was first solved in 1979 by Blakley [7] and independently by Shamir [59], who showed how to reconstruct the secret in what became known as (k,n)-*threshold secret sharing schemes*, i.e. k shares are needed out of n to reconstruct the secret while $k-1$ shares get no information at all about the secret.

Before delving into formal constructions and theorems, let us look at the simplest secret (*splitting*) scenario.

Problem 3.1. ***Secret Splitting[1]: a two-party case***

Consider the case where we have a message M, represented as an integer[2], that we would like to split between two people, say Alice and Bob in such a way that neither of them alone can reconstruct the message M, but together they can.

Solution

Give Alice a random uniformly picked *integer r and give Bob* $M-r$.

To reconstruct the secret, Alice and Bob simply add their pieces together.

$\mathscr{N}.\mathscr{B}$. One has to do all the arithmetics modulo a large integer p where we assume that the integers are uniformly picked (i.e. with a probability of $\frac{1}{p}$ each).

Problem 3.2. ***Secret Splitting: a generalization***

We consider the generalization of the previous problem (3.1) where we now want to split the secret S among n participants, in such a way that all of them collaborate to reconstruct S, while any coalition of $n-1$ *participants get no useful information whatsoever about the secret.*

Solution

Choose $n-1$ *random integers* $r_1, r_2, \cdots, r_{n-1}$ *and give them to* $n-1$ *of the participants, while give the remaining person* $S - \sum_{i=1}^{n-1} r_i (mod\ p)$.

Clearly, to reconstruct the secret S all of the n-participants need to collaborate; they just need to add up their shares, while $n-1$ *of them will get no information at all about the secret given that each share is randomly picked, the* n^{th} *participant will be left with a random number as well.*

[1] Secret splitting refers to an (n,n) threshold scheme, where absolutely all shares are needed to reconstruct the secret.

[2] All the arithmetic is modular.

ℹ $\mathcal{N}.\mathcal{B}$. The previous two problems are special cases of a (k,n)-*threshold scheme* with $k=n$ i.e. an (n,n)-threshold scheme.
We move on now to Shamir and Blakley's solutions to the (k,n) threshold scheme problem.

Example 3.3. ***Blakely and Shamir in: Tales from the Crypt***$_{ogram}$
We are back again with the bank manager and his crypt (or vault) and we would like to examine how Blakley and Shamir resolved the given puzzle of secret reconstruction. We will present Shamir's solution first since it is more transparent than Blakley's approach. The latter will be more appreciated once we have seen Shamir's at work.

- ***Shamir's Approach*** *[59]*
  In our tail from the crypt, the manager wants to share his secret combination to the crypt with specific subsets of his employees. In formal secret sharing scenarios the manager is known as the dealer $\mathscr{D}$ and the set of employees is known as the set of players or participants $\mathscr{P}$. The protocol goes as follows:

  – (**Share construction**) *The dealer $\mathscr{D}$ splits the secret S into shares S_i (or* shadows *as they are also known) by picking randomly a $k-1$-degree polynomial where all arithmetics is done in*[3] *$GF(p)$.*

  $$q(x) \equiv a_0 + a_1 x + a_2 x^2 + \cdots a_{k-1} x^{k-1} \mod p,$$

  where $a_0 = S$. Now, set $y_1 = q(1), y_2 = q(2), \cdots, y_n = q(n)$.
  Here $y_i \equiv q(i) \mod p$ is understood[4]*.*

  – (**Share Distribution**) *The dealer $\mathscr{D}$ gives out the pair (i, y_i) to each player P_i.*
  $\mathcal{N}.\mathcal{B}$. The prime p is known to all but the polynomial $q(x)$ is kept secret.

  – (**Secret Reconstruction**) *Now, suppose k participants get together and share their pairs in order to recover the secret S. This can always be done because*

[3] We take p to be a large prime number so that $GF(p) \simeq \mathbb{Z}_p$.

[4] What we have done here, is to pick distinct integers $x_1, \cdots, x_n$ all $\mod p$, that without loss of generality we have set to $1, 2, \cdots, n$ as a reasonable choice.

there exists a unique $(k-1)$*-degree polynomial going through any given k points. We present two elegant efficient ways for doing this:*

$*$ (**Linear System Approach**)

Given those k points $(x_1, y_1), \cdots, (x_k, y_k)$*, we want to reconstruct the* $k-1$*-degree polynomial* $q(x)$*, keeping in mind that* $S = a_0$ *and*

$y_i \equiv a_0 + a_1 x_i + \cdots + a_k x_i^{k-1} \mod p.$

Thus, we have a linear system of k-equations that we can cast in matrix form

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix}$$

This matrix (call it V) is known as a Vandermonde matrix.

It has a unique solution provided its determinant is non-zero (mod p).

One can show that the determinant is given by

$$\det V = \prod_{1 \le i < j \le k} (x_i - x_j)$$

We see that the determinant is zero when two of the x_i*'s coincide (modulo p). Thus the system has a unique solution as long as they are distinct (here the primality of p plays a major role to ensure this).*

$*$ (**Lagrange Interpolation Method**)

An alternative approach is to use the Lagrange interpolation method *to reconstruct the polynomial* $q(x)$ *(and hence the secret message) given that we know k of its values* (x_k, y_k)*.*

Recall that the coefficients $a_1, \cdots, a_{k-1}$ *are randomly chosen from a uniform distribution over the integers in the range* $[0, p)$*.*

$$\text{Let } l_i(x) \equiv \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \mod p. \tag{3.1}$$

*The **Lagrange interpolation polynomial** is defined as*

$$P(x) = \sum_{i=1}^{k} y_i l_i(x), \tag{3.2}$$

satisfying the requirement that $P(x_l) := y_l \ \forall \ 1 \leq l \leq k$.

For example when $x = x_1$ we get

$P(x_1) = y_1 l_1(x_1) + y_2 l_2(x_1) + \cdots \equiv y_1 \cdot 1 + y_2 \cdot 0 + \ldots \equiv y_1 \mod p.$

To reconstruct the secret message all one has to do is to evaluate

$P(x)|_{x=0}$, and thus we get

$$S = P(0) \equiv \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{-x_j}{x_i - x_j} \mod p. \tag{3.3}$$

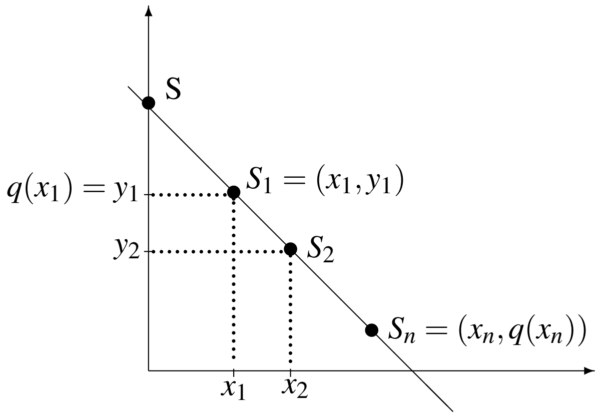


Figure 3.1: Shamir's Secret Sharing Scheme.

ℹ *$\mathcal{N}.\mathcal{B}$. As can be seen in fig.(3.1), even with the lack of a single share (point), the secret can still be any equiprobable value in $[0, p)$.*

- ***Blakley's Approach** [7]*

The idea behind Blakley's (k, n) threshold secret sharing scheme (also known as a vector scheme*) is to use* hyperplane geometry *to hide and reconstruct the secret. In this scenario, the secret is a point in k-dimensional hyperspace (over a finite field) and the n shares are affine hyperplanes that pass through this point (i.e. each share is the equation of a* $(k-1)$*-dimensional hyperplane that includes the point). To reconstruct the secret, k players come together to solve the system of equations (i.e. the intersection of those hyperplanes is the desired secret (point)).*

- (**Share construction**) *The dealer* $\mathscr{D}$ *picks a secret* $S = s_0$ *that he will want coalitions of k participants to be able to recover while any* $k-1$ *of them get no information about it.*

  - $\mathscr{D}$ *chooses at random a large prime* $p > s_0$ *and integers* $s_1, s_2, \cdots, s_{k-1}$ *(where again all arithmetic is done modulo p)*[5]*, and thus defines a point* $Q = (s_0, s_1, s_2 \cdots, s_{k-1})$ *in k-dimensional space.*

  - The secret will be taken to be the first coordinate of Q.

  - Now, the dealer $\mathscr{D}$ *chooses at random* $(k-1)$*-independent coefficients* $a_0^{(i)}, a_1^{(i)}, \cdots, a_{k-2}^{(i)}(\mod p)$*,* $for\ each$ $1 \leq i \leq n$*, while setting*

$$y^{(i)} = s_{k-1} - \sum_{j=0}^{k-2} a_j^{(i)} s_j \mod p.$$

- (**Share Distribution**) *The dealer* $\mathscr{D}$ *gives out* securely *the following hyperplane (labeled by i) to the corresponding participant* P_i

$$x_{k-1} = \sum_{j=0}^{k-2} a_j^{(i)} x_j + y^{(i)} \mod p,$$

  where the y^i*'s,* $0 \leq i \leq k-1$*, are free variables.*

- (**Secret Reconstruction**) *To reconstruct the secret (i.e. to find the given point Q), k of the* P_i*'s (in our scenario sub-managers) pool together their shares. These shares represent k distinct hyperplane equations and thus a linear sys-*

[5] We work again in $GF(p)$.

tem of equations that we cast in matrix form:

$$\begin{pmatrix} a_0^{(1)} & a_1^{(1)} & \cdots & -1 \\ a_0^{(2)} & a_1^{(2)} & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{(k)} & a_1^{(k)} & \cdots & -1 \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{k-1} \end{pmatrix} \equiv \begin{pmatrix} -y^{(1)} \\ -y^{(2)} \\ \vdots \\ -y^{(k)} \end{pmatrix}$$

As long as the determinant of this matrix is non zero, (i.e. as long as the columns a linearly independent or non-zero) the matrix can be inverted (all done modulo p) and thus recover the point Q and in particular its first coordinate $s_0 = S$ which is our sought out secret.

As in Shamir's scheme, if less than k participants try to recover the secret, even $k-1$ of them, they will be left out with an equiprobable possibility of intersection points. Since there would be a hyperplane equation missing that is needed to determine uniquely the given point Q and thus in our tail, the $k-1$ sub-managers would get no information at all about the secret s_0.

We start by exploring some formal definitions of the classical domain of secret sharing schemes, in particular to introduce nomenclature and important notions that carry over to the quantum realm. We strongly emphasize the fact that *classical constructions do not carry over automatically to the construction of quantum secret sharing schemes*. The quantum world imposes strong conditions on the allowed schemes as we will discuss shortly.

3.1.2 Formal Definitions and Constructions

We start by defining formally which sets and subsets of players are allowed to reconstruct the secret and which are not.

Let $\mathscr{P} = \{P_i : 1 \leq i \leq n\}$ be the set of players; and $\mathscr{S}$ the share set (i.e. the set of all possible shares). To avoid confusion with the set of possible shares, and for historical reasons, we will use $\mathscr{K}$ to denote the set of all possible secrets, because originally secret sharing schemes where introduced to solve the problem of securely sharing secret keys K_i.

Definition 3.4. *A set* Γ *of subsets of* $\mathscr{P}$ *is called* ***monotone*** *if*

$$\left(A \in \Gamma \; \mathit{and} \; A \subseteq A'\right) \Rightarrow A' \in \Gamma.$$

That is, Γ *is closed upward.*

Definition 3.5. *An* ***access structure*** Γ*, where* Γ *is monotone, is a set of subsets of* $\mathscr{P}$*, which is to say that* $\Gamma \subseteq 2^{\mathscr{P}}$*. Elements of* Γ *are those subsets of players that should be able to reconstruct the secret and are thus called* authorized sets. *Those subsets that cannot recover the secret are called* unauthorized sets.

Note that Γ has to be monotone for this notion to make sense (see definition 3.4).

Definition 3.6. *A* ***Secret Sharing Scheme (SSS)*** *is a protocol that enables a dealer* $\mathscr{D}$ *to distribute a secret S among a set of players* $\mathscr{P}$ *such that only specific groups of people can reconstruct the secret (the authorized sets).*
A secret sharing scheme is completely characterized by its access structure Γ.

ℹ $\mathscr{N}.\mathscr{B}$. Because Γ is monotone, any superset A' of any authorized set A in Γ is itself an authorized set of players, since the additional players in $A' \backslash A$ can be ignored in the secret reconstruction. This brings us to the following practical definition:

Definition 3.7. *An access structure* Γ *is completely defined by its* ***minimal*** *set* Γ_0 *where* $A \in \Gamma_0$ *if each proper subset of A is not in* Γ*:*

$$\Gamma = \{A \subseteq \mathscr{P} : B \subseteq A, A \in \Gamma_0\}.$$

Γ *is then called the* closure *of* Γ_0 *and we write* $\Gamma = cl(\Gamma_0)$*, while* Γ_0 *is also known as the basis of* Γ.

ℹ $\mathscr{N}.\mathscr{B}$. Usually, only the minimal sets of an access structure are given.

Definition 3.8. *A secret sharing scheme with corresponding access structure* Γ *is called **perfect** if every subset of players in* Γ *can recover the secret with* absolute certainty *while every set not in* Γ *gets no information whatsoever about the secret through collective knowledge of their shares.*

Remark 3.9. *In a perfect secret sharing scheme either the secret is revealed or it is completely hidden.*

We introduced above an example of a special class of secret sharing schemes, the (k,n) *threshold* scheme via Shamir and Blakley's constructions as well as the more special case of secret splitting scheme when $k=n$ i.e. the (n,n)-scheme. We now give the formal definition of a threshold scheme.

Definition 3.10. *A* (k,n) *threshold scheme, with* $1 \leq k \leq n$*, is a secret sharing scheme with corresponding access structure*

$$\Gamma = \{A \subseteq \mathscr{P} : |A| \geq k\}. \tag{3.4}$$

3.1.2.1 A General Model

We present a general model for secret sharing scheme due to Brickell and Stinson [12]. Let $\mathscr{F}$ represent the set of distribution rules (see below), $\mathscr{P}$ the set of participants, $\mathscr{K}$ the set of all possible secrets and $\mathscr{S}$ the set of all possible shares.

Definition 3.11. *A* distribution rule *is a function*

$$f : \mathscr{P} \cup \{\mathscr{D}\} \to \mathscr{K} \cup \mathscr{S},$$

satisfying $f(\mathscr{D}) \in \mathscr{K}$*, and* $f(P_i) \in \mathscr{S}$ *for* $1 \leq i \leq n$*, where* $\mathscr{D}$ *is the dealer (the trusted authority).*

The distribution rule represents one of the possible ways to distribute the shares to the participants. For example $f(\mathscr{D})$ is the secret being shared while $f(P_i)$ is the share given to P_i.

Notation 3.12. *Let $\mathscr{F}$ be as above, and for a given $K \in \mathscr{K}$, we denote by $\mathscr{F}_K$ the set:*

$$\mathscr{F}_K = \{f \in \mathscr{F} : f(\mathscr{D}) = K\}.$$

When the dealer $\mathscr{D}$ wishes to share a secret $K \in \mathscr{K}$, he will chose randomly a distribution rule $f \in \mathscr{F}_K$ and use it to distribute the secret K.
Please note that the set $\mathscr{F}_K$ is public knowledge and there is no need to hide it. Also, this model is completely general and can be used to study any given construction in secret sharing. It can be appropriately modified to be used in the quantum setting and is construction independent.
The following definition gives conditions as to when a set of distribution rules for a given scheme realizes a specified access structure Γ.

Definition 3.13. ***General setting definition***
Given an access structure Γ and a set of distribution rules $\mathscr{F}$, we introduce the following two properties:

- *(*) Let $A \in \Gamma$, and suppose, $f, g \in \mathscr{F}$. If $f(P_i) = g(P_i)$ for all $P_i \in A$, then $f(\mathscr{D}) = g(\mathscr{D})$.*

- *(**) Let $A \notin \Gamma$ and suppose $f : A \to \mathscr{S}$. Then there exists a non negative integer $\lambda(f, A)$, such that for all $K \in \mathscr{K}$,*

$$|\{g \in \mathscr{F}_K : g(P_i) = f(P_i),\ \forall\ P_i \in A\}| = \lambda(f, A).$$

Theorem 3.14. *[12] Given a collection of distribution rules $\mathscr{F}$ that satisfy conditions (*) and (**) of definition (3.13); then $\mathscr{F}$ is a perfect secret sharing scheme realizing the access structure Γ.*

Note that the *share* of a participant refers specifically to the information the dealer $\mathscr{D}$ sends in private to the participant.

Remark 3.15. *What property (*) says is that the shares given to an authorized subset* uniquely *determines the secret.*

Remark 3.16. *Property (**) says that the shares given to an unauthorized subset give no information about the secret. This is because given an assignment of shares f (where $f : A \to \mathscr{S}$) to an unauthorized set A, the conditional probability distribution on $\mathscr{K}$ is the same as the* a priori *probability distribution on $\mathscr{K}$. That is if $p_{\mathscr{K}}$ is the probability distribution over $\mathscr{K}$ and that for every $K \in \mathscr{K}$, $\mathscr{D}$ chooses uniformly a distribution rule $f_{\mathscr{K}} \in \mathscr{F}_K$ (i.e. each with probability $\frac{1}{|\mathscr{F}_K|}$), then when the participants of an unauthorized subset $A \notin \Gamma$ get their shares together (which is represented by $f : A \to \mathscr{S}$) to reconstruct the secret and compute the conditional probability distribution $p_{\mathscr{K}}(K|f)$ one finds that $p_{\mathscr{K}} = p_{\mathscr{K}}(K|f)$.*
This situation is very similar to the concept of perfect secrecy *and the name perfect secret sharing scheme is thus justified.*

Theorem 3.17. *[38] Any monotone access structure can be realized by a perfect secret sharing scheme.*

Before we show how this general model can be used to construct a given scheme, we give one more important definition, that of the *information rate* of a secret sharing scheme, which enables us to measure its efficiency.

Definition 3.18. *[12] Given the model introduced in definition (3.13), suppose $\mathscr{F}$ is a set of distribution rules for a secret sharing scheme. For $1 \leq i \leq n$, we define the set of all possible shares that player P_i might receive*

$$\mathscr{S}_i = \{f(P_i) : f \in \mathscr{F}\}.$$

where clearly $\mathscr{S}_i \subseteq \mathscr{S}$. Once again, let $\mathscr{K}$ denote the set of all possible secrets with $|\mathscr{K}| < \infty$. We can thus think of $K \in \mathscr{K}$ (on account of the finiteness of the set $\mathscr{K}$) as being represented (without loss of generality) by a bit-string of length $\log_2 |\mathscr{K}|$ *via an appropriate binary encoding. Similarly, we can think of the share that P_i receives as*

containing $\log_2|\mathscr{S}_i|$*-bits of information.*
Thus we can define the individual information rate *denoted by* τ_i *for* P_i *as*

$$\tau_i \equiv \frac{\log_2|\mathscr{K}|}{\log_2|\mathscr{S}_i|}, \tag{3.5}$$

while the information rate of the scheme *is denoted by* τ *and is defined as*

$$\tau = \max\{\tau_i : 1 \leq i \leq n\}.$$

Thus τ_i is the ratio between the length in the number of bits of a share and that of the secret.

Lemma 3.19. *Suppose* $\mathscr{F}$ *is the set of distribution rules for a perfect secret sharing scheme realizing an access structure* Γ*. Then in any given scheme,* $\tau \leq 1$*.*

Proof. Let $A \in \Gamma_0$ (c.f. def.(3.7)) and let $P_i \in A$. By $A_{|P_i}$ we mean the player P_i deleted from the set A, i.e. $A_{|P_i} \equiv A \backslash \{P_i\}$.
Choose any distribution rule $g \in \mathscr{F}$, and let $g^{\perp}$ denote the restriction of g to $A_{|P_i}$.
By definition of Γ_0, $A_{|P_i} \notin \Gamma$. Therefore, there exists a non negative integer $\lambda(g^{\perp}, A_{|P_i})$ satisfying condition (**) of definition (3.13).
Furthermore, for each $K \in \mathscr{K}$, and for all $P_j \in A_{|P_i}$, there is a distribution rule $g_K^{\perp} \in \mathscr{F}_K$ such that $g_K^{\perp}(P_j) = g^{\perp}(P_j)$. By property (*) in definition (3.13), $g_K^{\perp}(P_i) \neq g_{K'}^{\perp}(P_i)$ if $K \neq K'$.
Hence, $|\mathscr{S}_i| \geq |\mathscr{K}|$, and thus $\tau \leq 1$. □

Remark 3.20. *Practically speaking, for a secret sharing scheme to be of value, we do not want to distribute too much secret information (i.e. too many shares versus the length of the secret itself). We thus want the information rate* τ *to be as close as possible to unity.*

Definition 3.21. *A secret sharing scheme with information rate* $\tau = 1$ *is termed* ideal *on behalf of* $\tau = 1$ *being the optimal situation.*

A general access structure that can be realized as an ideal secret sharing scheme is said to be ideal itself. In this general case, no restrictions on the dimension of the secret is imposed. This being said, not every access structure can be realized with unit information rate. One of the important problems in secret sharing is to determine, given a (monotone) access structure, whether or not there exists an ideal secret sharing scheme.

As promised, we now give a very elegant construction termed *the vector space construction*, due to Brickell [11], that illustrates perfectly the general construction outlined above and is an example of an ideal secret sharing scheme.

3.1.2.2 The Vector Space Construction (Brickell '89 [11])

Let Γ be an access structure, $\mathscr{K}$ the set of all possible secrets and $\mathscr{S}_i$ the set of all possible shares that the player P_i might get.

Notation 3.22. *By $GF(q)^d$ we denote the vector space of all d-tuples over the* Galois field *$GF(q)$, where $d \geq 2$ and q is taken to be a prime, thus giving us the isomorphism $GF(q) \simeq \mathbb{Z}_q$.*
Note also, that by $\langle v_1, \cdots, v_i \rangle$ (for some i) we will denote the subspace *spanned by the vectors v_i. This establishes what we mean by the notation $\langle \cdots \rangle$ as it appears subsequently.*

Suppose there exists a function $\varphi : \mathscr{P} \cup \{\mathscr{D}\} \to GF(q)^d$, satisfying

$$\varphi(\mathscr{D}) \in \langle \varphi(P_i) : P_i \in A \rangle \Leftrightarrow A \in \Gamma. \tag{3.6}$$

That is the vector $\varphi(\mathscr{D})$ can be expressed as a linear combination of the vectors in the set $\{\varphi(P_i) : P_i \in A\}$ if and only if A is an authorized subset of Γ.
We construct an ideal secret sharing scheme with $\mathscr{K} = \mathscr{S}_i = GF(q), 1 \leq i \leq n$.

Distribution Rules of the Scheme
For every vector $\vec{a} = (a_1, a_2, \cdots, a_d) \in GF(q)^d$ we define a distribution rule $f_{\vec{a}}$ where

$$f_{\vec{a}} = \underbrace{\vec{a} \cdot \varphi(x),}_{\text{Inner product in } GF(q).} \qquad \forall\, x \in \mathscr{P} \cup \{\mathscr{D}\}. \tag{3.7}$$

Theorem 3.23. *Suppose φ satisfies the condition in Eq.(3.6) above, then the collection of distribution rules $\mathscr{F} = \{f_{\vec{a}} : \vec{a} \in GF(q)^d\}$ is an ideal secret sharing scheme realizing the access structure Γ.*

Proof. Suppose $K \in \mathscr{K}$ is the secret that we want to reconstruct.
If A is an authorized subset of Γ, then the participants in A should be able to compute K. Since A is authorized, we have that $\varphi(\mathscr{D}) \in \langle \varphi(P_i) : P_i \in A \rangle$ therefore, we can write

$$\varphi(\mathscr{D}) = \sum_{\{i:P_i \in A\}} c_i \varphi(P_i), \text{ with each } c_i \in GF(q). \tag{3.8}$$

Let $s_i \in \mathscr{S}_i$ denote the share given to player P_i, and let $\vec{a}$ be an arbitrary (unknown to P_i) vector chosen by the dealer $\mathscr{D}$. Then $s_i = \vec{a} \cdot \varphi(P_i)$.
Now since $K = \vec{a} \cdot \varphi(\mathscr{D})$ we get:

$$\begin{aligned} \vec{a} \cdot \varphi(\mathscr{D}) &= \vec{a} \cdot \sum_{\{i:P_i \in A\}} c_i \varphi(P_i) = \sum_{\{i:P_i \in A\}} c_i \vec{a} \cdot \varphi(P_i) \\ &= K = \sum_{\{i:P_i \in A\}} c_i s_i, \end{aligned} \tag{3.9}$$

and therefore condition (*) of definition (3.13) holds.
Now, if $A \notin \Gamma$ i.e. A is an unauthorized set, let m denotes the dimension of the subspace $\Delta_i = \{\varphi(P_i) : P_i \in A\}$. Again, let $\mathscr{D}$ choose uniformly at random a secret $K \in \mathscr{K}$ and consider the system of equations

$$\varphi(P_i) \cdot \vec{a} = s_i, \ (\forall \ P_i \in A) \ \text{ and } \varphi(\mathscr{D}) \cdot \vec{a} = K.$$

The solution space of this system has dimension $d - m - 1$ and is thus independent of the secret K. Therefore no $\{P_i\} \in A \notin \Gamma$ can get any information about the secret. □

We now give an illustration of the above construction revisiting Shamir's protocol introduced earlier in Example (3.3) but recast in the vector space construction formalism.

Example 3.24. **(Shamir's (k,n)-threshold scheme revisited)**
Let $d = k$, with each vector $\vec{a} \in GF(q)^k$ and let $\varphi(P_i) = (1, x_i, x_i^2, \cdots, x_i^{k-1}) \ \forall \ 1 \leq i \leq n$,

where each x_i *is the x-coordinate given to the participant* P_i *such that* $s_i = K + \sum_{j=1}^{k-1} a_j x_i^j$. *Let* $\varphi(\mathscr{D}) = (1,0,\cdots,0)$, *with as distribution rules* $f_{\vec{a}} = \vec{a}\cdot\ \varphi(x)$, $\forall\, x \in GF(q)^d$, *where the vector* $\vec{a} = (a_0, a_1, \cdots, a_{k-1})$ *is arbitrary and picked by the dealer* $\mathscr{D}$.
We verify that we are getting the correct distribution rules:

$$\begin{aligned}\varphi(\mathscr{D})\cdot\vec{a} &= (1,0,\cdots,0)\cdot(a_0,a_1,\cdots,a_{k-1})\\ &= a_0 \mod q = K, \ \surd\end{aligned}$$

which is the secret to be shared among the players.
$\mathscr{D}$ *computes each share* s_i

$$\begin{aligned}s_i &= \vec{a}\cdot\varphi(P_i),\\ &= (a_0,a_1,a_2,\cdots,a_{k-1})\cdot(1,x_i,x_i^2,\cdots,x_i^{k-1}) \mod q,\\ &= a_0 + a_1 x_i + a_2 x_i^2 + \cdots + a_{k-1} x_i^{k-1} \mod q, \ \forall\, 1 \le i \le n.\end{aligned}$$

So each player P_i *is given as his/her share* $(x_i, s_i) \equiv (i, s_i)$ *where we have chosen without loss of generality each* $x_i = i$ *as we did above in example(3.3).*
To solve the system of equations, k participants come together with their shares handy and may use one of the two methods outlined in example(3.3) either the Lagrange interpolation method *or the* linear system approach. *Here we make use of the Lagrange interpolation method to reconstruct the secret K.*
From Eqs.(3.3 ,3.2)

$$\begin{aligned}\sum_{j=1}^{k} s_{i_j} \prod_{\substack{1\le k<n,\\ j\neq k}} \frac{-x_{i_k}}{x_{i_j}-x_{i_k}}\Big|_{x_i=i} &= \sum_{j=1}^{k} s_{i_j} \underbrace{\prod_{\substack{1\le k<n,\\ j\neq k}} \frac{-i_k}{i_j-i_k}}_{\ell_j(0)\equiv\ell_j^{\,0}} \mod p, \ \forall\, 1 \le j \le n,\\ &= \sum_{j=1}^{k} \ell_j^{\,0} s_{i_j}\\ &= K. \ \surd \end{aligned} \tag{3.10}$$

Where in the vector space construction we can identify the $c_j \equiv \ell_j^0$ *as is required in Eq.(3.9) to reconstruct the secret K.*

3.2 Quantum Secret Sharing

Leaving the classical world behind, we start our exploration of the quantum domain of secret sharing. We mentioned already in the introduction to this chapter that classical constructions of secret sharing schemes do not carry over automatically into the quantum domain. The main restriction on quantum secret sharing schemes emanates from the *no-cloning theorem 1.19*. Informally, this is because if we had no further restrictions on which authorized sets can reconstruct the secret, we would be able to clone the unknown (secret) state and thus violate one of this fundamental theorem of *QIT*. When we discussed quantum error corrections in Chapter 2, the same reasoning led us to the *quantum no-cloning bound* Eq.(2.32).

Quantum Secret Sharing (*QSS*) schemes generalize in two possible ways the classical ones. We use a quantum state to (a) share either a secret quantum state or to (b) share a classical secret. An advantage of the latter over classical secret sharing schemes is that sometimes the size of the shares can be half that of the size of the secret, whereas we have shown in the general construction scheme in the classical case that the information rate τ is at best unity (c.f. lemma (3.19)). On the other hand, if one shares a secret quantum state, the results of lemma (3.19) still hold in the quantum scenario.

One of the first attempts at generalizing classical secret sharing to the quantum domain was that of Hillery, Bužek and Berthiaume [36]. Although we will not be concerned with eavesdroppers (the way they did), by definition of threshold schemes, we will be concerned with coalitions of players who try to recover the secret. Those sets are known as unauthorized sets. These adversaries do exist in the classical world, but take on a new flavour in the quantum domain, in view of the quantum no cloning theorem.

ℹ $\mathscr{N}.\mathscr{B}$. From the start we should point that the two settings are very different in their philosophies, classically one wants to recover a sequence of bits while quantum mechanically one wants to bring back a physical particle in the correct state.

3.2.1 Properties of Quantum Secret Sharing Schemes

In our exploration of quantum secret sharing, we will often be concerned with a special class of schemes, mainly **Q***uantum* **T***hreshold* **S***chemes* (*QTS*). When we state a theorem without specifying that it is a threshold scheme, we mean that the result holds for the more general case (i.e. for more general access structures than those obeying a threshold scheme).

We start with the definition of a quantum threshold secret sharing scheme, which parallels that of the classical case (c.f def. 3.10).

Notation 3.25. *By $((k,n))$ we denote a quantum threshold scheme (with a set of double parentheses) in contrast to the classical threshold scheme (with single parentesis) (k,n).*

Definition 3.26. *We define a $((k,n))$* threshold scheme *to be a method to encode and divide a secret quantum state among n participants such that k of them, pooling their quantum shares together, can reconstruct the unknown quantum state, while $k-1$ players get no information* whatsoever *about the unknown quantum state (i.e. the secret).*
A general *quantum secret sharing scheme is completely characterized by its access structure Γ (c.f. def. 3.5).*

Remark 3.27. *The fact that $k-1$ of the players get no information about the secret state is equivalent to saying that their reduced density matrix is independent of the value of the secret. We can already draw a parallel with* QECC *and especially the discussion following Eq.(2.23). In both cases, the needed useful information about the qubits is missing. In* QECC*, the missing qubits prevent us from correcting the error and thus reconstruct the original state, while in* QSS *the missing shares prevent the $k-1$ participants from reconstructing the secret.*

Before delving into formal definitions and theorems, we start with an example to illustrate the philosophy behind secret state reconstruction in *QSS*. We will consider a $((2,3))$ threshold scheme, where the secret state is a *qutrit*, a three-dimensional quantum state to be shared among three players in such a way that any two of them combining their quantum shares can reconstruct the secret state, but the secret remains completely unknown to anyone holding only one share.

Example 3.28. ((2,3))-Quantum Threshold Scheme

We illustrate the different aspects of the definition 3.26.

➠**(Encoding)**

Since quantum secret sharing is a quantum code, the dealer $\mathscr{D}$ needs to encode the secret state into a bigger space, the coding space, and to do so he uses the following operation: Let $U_{2,3}$ be an isometry *(i.e. a map that preserves the distance between vectors) such that*

$$\begin{aligned} U_{2,3}(\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle) \;=\; & \frac{\alpha}{\sqrt{3}}(|000\rangle+|111\rangle+|222\rangle)+\frac{\beta}{\sqrt{3}}(|012\rangle+|120\rangle+|201\rangle)+ \\ & \frac{\gamma}{\sqrt{3}}(|021\rangle+|102\rangle+|210\rangle), \end{aligned} \tag{3.11}$$

where all α,β and $\gamma\in\mathbb{C}$ are subject to the normalization condition $|\alpha|^2+|\beta|^2+|\gamma|^2=1$.

📱 **Share Distribution**

Each share is a qutrit and the dealer $\mathscr{D}$ gives one share to each player.

⌕ **Secret Reconstruction**

To recover the secret state, any two players can add together their shares ($\bmod 3$*). Say for example that players P_2 and P_3 want to recover the secret. P_2 adds his share to P_3 and then P_3 adds the resulting share to P_2; this is done trit by trit and thus they are left in the following global state:*

$$\frac{1}{\sqrt{3}}(|00\rangle_{1,3}+|12\rangle_{1,3}+|21\rangle_{1,3})(\;\alpha|0\rangle_2+\beta|1\rangle_2+\gamma|2\rangle_2\;),$$

and thus player P_2 has the secret quantum state.

Since the isometry $U_{2,3}$ preserves the cyclic permutation symmetry of the qutrits, the reconstruction procedure for any other pairs of players is similar to the one detailed above.

On the other hand, if only one player tries to recover the secret state, one finds that his *density matrix (tracing out the shares of the other two players) is in the totally mixed state, and therefore he has no information whatsoever about the original state.*

ℹ$\mathscr{N}.\mathscr{B}.$ Recall in our discussion of *QECC* that we had recourse to the *error syndrome* to be able to correct for an unknown error without ever measuring the state itself, otherwise we would have collapsed it irreversibly. Here we are faced with the same difficulty: we should be careful not to measure individually the shares while reconstructing the secret. Otherwise, we would lose all possible superpositions and fail to recover the original state.

In the above $((2,3))$-scheme, if we disregard the third input dimension, we have readily constructed a $((2,3))$-quantum secret sharing scheme that can share a secret qubit state, while each share still remains a qutrit. On the other hand, we cannot have at the same time a scheme that shares a secret which is a qubit while the shares remain qubits as well, since we would have constructed a quantum error correction scheme capable of recovering from one erasure in which the qubit to be transmitted is encoded into three qubits, which was shown not to exist in [32].

We can arrive at the same conclusion by applying the no-cloning bound Eq.(2.32) with $d-1=2$ (since this is an $[[n=3,k=1,d=3]]$-*QECC*) and thus get $n>4$ excluding the $n=3$ case; while by the proof of the no-cloning bound above the $n=4$ case was already excluded. We thus see the tight connections between the machinery of quantum error corrections and quantum secret sharing, which once again although elegant, is not surprising given that both are quantum codes and must respect the same quantum constraints and bounds (c.f. the section 2.2.2).

Furthermore, if we trace over a share in $((2,3))$ we get a $((2,2))$-QSS scheme (that is the set of all the players taken together is the only authorized set while just one missing player would invalidate the state reconstruction procedure). This turns out to be a special case of a more general theorem [24]:

Theorem 3.29. *From any $((k,n))$ threshold scheme with $n>k$, a $((k,n-1))$ threshold scheme can be constructed by discarding one share.*

We saw in the classical case, that a (k,n) threshold scheme exists for every value of

$n \geq k$. However, this does not hold in the quantum world, due to the quantum *no-cloning theorem* [25, 66] which leads us to the following theorem [24].

Theorem 3.30. *If $n \geq 2k$ then no $((k,n))$ threshold scheme exists.*

Proof. Assume a $((k,n))$ threshold scheme exists with $n \geq 2k$. We will show that we thus could bypass the no-cloning theorem and xerox the unknown quantum state as follows: First, we would apply the $((k,n))$ scheme to the secret state to produce n shares. Then, we could take two disjoint sets of k shares, and reconstruct two independent copies of the original state. This procedure clearly contradicts the *no-cloning theorem* 1.19. □

We next make the distinction between pure and mixed states quantum secret sharing (*QSS*) schemes, before looking at the *QECC/QSS* schemes correspondence.

Definition 3.31. *In a **pure state scheme** the system of all the shares taken together is in a pure state for every encoding of a pure state of the secret. When the encoding of a pure state of the system results in a mixed state, the scheme is termed **mixed state scheme**.*

Remark 3.32. *If one measures the efficiency of a quantum secret sharing scheme in terms of the number of shares per participant, then we need the implicit condition that each share is of the same size of that of the secret.*

Surprisingly, mixed state schemes can achieve better performance (in terms of share size) than pure state schemes, as we shall soon discover.

3.2.2 The *QSS/QECC* Correspondence and its Consequences

Classically, one can always associate an error correcting code to a perfect secret sharing scheme; though determining the access structure of the associated scheme can be a very difficult task. On the other hand, quantum mechanically this transition from quantum error correcting codes to quantum secret sharing schemes is not so straightforward since the no cloning theorem has to be respected and puts constraints on the allowed access structures.

In this subsection we explicitly reformulate the quantum error correction schemes in terms of the secret sharing nomenclature (and/or vice versa), which enables us to readily prove some important theorems on quantum secret sharing schemes.
Let the set of n players be denoted by $\mathscr{P}$ and let $f : |\psi\rangle \longmapsto |\phi\rangle$ be the encoding of the states $|\psi\rangle$ onto codewords $|\phi\rangle$.

1. Recall that an authorized subset $A \in \Gamma$ of players is the collection of those players who can recover the secret encoded quantum state. We first reformulate this condition in terms of correcting erasure errors:
   In order for a set A of players to be able to reconstruct the state, the overall encoding f must have the property that it can correct for the erasure of the qubits held by the players not in A.
   That is to say, $A \in \Gamma$ is an authorized set if the encoding f corrects erasure errors for the shares held by the complement $\{P_1, \cdots P_n\} \backslash A$ of A.

2. Let ρ denote the density matrix of the codewords $|\phi\rangle$. That is, ρ is a description of the global state of shares distributed to the players P_i in $\mathscr{P}$. Now, we recall that a set of players $B \notin \Gamma$ who cannot (and is not allowed to) reconstruct the secret state is termed *unauthorized set*. In *QECC* those subsets of players should have no information about the original encoded states, which translates as follows in terms of their density matrix.
   The density matrix ρ_B associated with any subset $B \notin \Gamma$ is independent of the encoded state $|\phi\rangle$; for if this were not true, then players in B would be able to gain information about $|\phi\rangle$ by making an appropriate measurement that would (at least) partially distinguish $\rho_B(|\phi\rangle)$ from $\rho_B(|\varphi\rangle)$ for some pair of states $|\phi\rangle$ and $|\varphi\rangle$ with different density matrices ρ_B.

3. Next, we make use of the reformulated *QECC* conditions (c.f. remark 2.35) to prove the following lemma. In Corollary 3.35 below, we give a similar proof using the no-cloning theorem to show how both techniques are complementary.

   Lemma 3.33. *For a pure state quantum secret sharing scheme (c.f. def. 3.31), a set B is unauthorized if and only if its complement B^c is an authorized set.*

Proof. Let A and B be complementary sets. A is an authorized set if and only if the encoding f can correct erasure errors on B, which by the *QECC* condition (in density matrix form) is equivalent to saying that $\mathrm{Tr}(\rho E)$ is independent of the encoded state $|\phi\rangle$ for all operators E acting on B.

Now, since E acts only on the set B, we have that $\mathrm{Tr}(\rho E) = \mathrm{Tr}_B(\rho_B E)$ and by a proper choice of basis for E (for example $E = |j\rangle\langle k|$) ,we find that $\mathrm{Tr}_B(\rho_B E)$ is independent of $|\phi\rangle$ for all E if and only if ρ_B is itself independent of $|\phi\rangle$ for all E. This is precisely the definition given in part (2) of an unauthorized set.

Which is also to say that $\langle\phi|E|\phi\rangle = \Lambda(E)$ is independent of $|\phi\rangle$ exactly the *QECC* condition in Eq.(2.22).

Thus A is authorized if and only if B is unauthorized. □

We finally recast all that we have said above in the following theorem (slightly reformulated), which first appeared in [24].

Theorem 3.34. *Let $\mathscr{C}$ be a subspace of a Hilbert space $\mathscr{H}$ that can be written as tensor product of the Hilbert spaces of various coordinates. Let $f : |\psi\rangle \longmapsto |\phi\rangle$ be an encoding with $\mathscr{C}$ as its image. Then f is a pure state quantum secret sharing scheme if and only if*

$$\langle\phi|E|\phi\rangle = \Lambda(E) \tag{3.12}$$

(i.e. independent of $|\phi\rangle$) whenever E is any operator acting on the complement of an authorized set or when E is any operator acting on an unauthorized set.

Proof. The discussion of (1), (2) and the proof of (3) readily yields the stated theorem. □

A natural corollary of theorem 3.34, which shows how special pure state schemes are in the sense that they are only possible for a highly restricted class of access structures, is the following [31]:

Corollary 3.35. *In a pure state quantum secret sharing scheme, every authorized set is precisely the complement of an unauthorized set (and vice-versa).*

Proof. If the complement B of an authorized set A was also an authorized set, we could thus create two identical and independent copies of the secret state precisely violating the quantum no-cloning theorem. Therefore the complement of an authorized set is always an unauthorized set.
On the other hand by the proof of Lemma 3.33, if $\langle\phi|E|\phi\rangle = \Lambda(E)$ holds, we can correct erasures on B and therefore reconstruct the secret on the complement of B i.e. on A which is an authorized set. Therefore, the complement of an unauthorized set is always an authorized set. □

We also note the following terminology:

Definition 3.36. *A quantum access structure Γ is called **maximal** if the authorized and unauthorized sets are complements of each other.*

Furthermore, in the more specific case of threshold schemes, we can derive an exact equation relating the threshold number of shares to the total number of participants provided the encoding gives rise to a pure quantum threshold scheme:

Corollary 3.37. *Any $((k,n))$ pure state threshold scheme satisfies $n = 2k-1$.*

Proof. Once again, let the set of n players be denoted by $\mathscr{P}$ and let A and B be complementary sets. Assume that A contains t players. Therefore $|B| = n-t$. Since A is authorized if and only if B is unauthorized (by Cor.3.35), we must have that $t \geq k$ if and only if $n-t \leq k-1$. For $t = k$ we get that $n-k \leq k-1$, which is rearranged to $n \leq 2k-1$. On the other hand, for $t = k-1$, we get $n-k+1 > k-1$, or $n > 2k-2$. For those two inequalities to be simultaneously valid, it must be that $n = 2k-1$. These are the only allowed values for a pure state quantum threshold secret sharing scheme. □

ℹ$\mathscr{N}.\mathscr{B}$. We note therefore that in a *pure* quantum threshold scheme $((k,n))$, the number of players n must be odd and that its access structure Γ must be *maximal*. This last corollary does not apply to *mixed* state schemes. We will see later (c.f. Corollary 3.39 and Theorem 3.42) that one can construct $((k,n))$ threshold schemes with $n < 2k-1$.

In [24] it is remarked that indeed this *QECC/QSS* correspondence is further enhanced via the following theorem, which is a generalization of the fact that the five-qubit quantum code proposed in [20, 30], mainly the $[[5,1,3]]$-stabilizer code, yields readily a $((3,5))$-quantum threshold scheme since it corrects any two erasure errors[6] enabling the secret to be reconstructed from any three given shares; while from two or less shares no information whatsoever can be extracted about the original data.

Theorem 3.38. *If a quantum code with codewords of length $2k-1$ corrects $k-1$ erasure errors which for stabilizer codes (c.f. section 2.1.2) is a $[[2k-1,1,k]]_q$ code, where q is the dimensionality of each coordinate and of the encoded state, then it is also a $((k,2k-1))$ threshold scheme.*

Proof. First suppose we start with a set A of k shares. This set precisely excludes $k-1$ shares and by the properties of stabilizer codes we know that this code corrects $k-1$ erasure errors and thus the secret can be reconstructed from those k shares held by A and is therefore an authorized set.
On the other hand given a set B of $k-1$ shares, this subset excludes precisely k shares, from which we know the secret can be reconstructed. Now assume we can gain some information about the secret by observing the $k-1$ shares in B. Since this is the quantum world, we know that any gain of information about a state instantaneously collapses it and thus there is no way we can recover the secret from those k shares (since they are now disturbed) and thus we run into a contradiction. □

Combining Theorem 3.29 with Theorem 3.38 above, we get the following corollary

Corollary 3.39. *From a $[[2k-1,1,k]]_q$ code, a $((k,n))$ threshold scheme can be constructed for any $n < 2k$.*

For example, as already mentioned above, from the five-qubit code $[[5,1,3]]$, we get a $((3,5))$-quantum threshold scheme and by applying the corollary above a $((3,4))$ and $((3,3))$ threshold schemes can be obtained by discarding shares.

[6] Recall that an erasure error is a general error on a known coordinate such that a quantum error-correcting code of distance d can correct $d-1$ erasure errors or $\lfloor (d-1)/2 \rfloor$ general errors.

On the other hand, in Example 3.28 as a consequence of Theorem 3.38, we have that the $((2,3))$-quantum threshold scheme is a $[[3,1,2]]_3$-quantum error correcting stabilizer code of length 3 correcting one erasure error with dimension $q=3$, i.e. a qutrit as described in the example.

Remark 3.40. *In some sense, every quantum secret sharing scheme is an error correcting code but unfortunately the reverse is not true as we will first see in the following example. We deffer to the end of this chapter for the possibility of overcoming this limitation (c.f. Corollary 3.54).*

Example 3.41. ***Is the*** $[[4,1,2]]$***-QECC a*** $((3,4))$***-QTS ?***
Consider the following four qubit-encoding which corrects one erasure error [32, 65]:

$$V_{3,4} : \alpha|0\rangle + \beta|1\rangle \longmapsto \frac{1}{2}\alpha(|0000\rangle + |1111\rangle) + \frac{1}{2}\beta(|0011\rangle + |1100\rangle) \equiv |\Lambda\rangle. \quad (3.13)$$

We know from Corollary 3.37 that this cannot be a $((3,4))$ *QTS because* $4 \neq 2\times 3-1$*; let us see where it fails.*

➠**(Encoding)**

The dealer $\mathscr{D}$ *uses the map* $V_{3,4}$ *to encode the secret state* $|\Psi_S\rangle = \alpha|0\rangle + \beta|1\rangle$ *as shown above to get* $|\Lambda\rangle$*, with the promise that* $|\alpha|^2 + |\beta|^2 = 1$.

📱 **(Share Distribution)**

Then $\mathscr{D}$ *gives each Player* P_i $(1 \leq i \leq 4)$ *a quantum share from* $|\Lambda\rangle$ *(keeping in mind that each share is a qubit).*

⌕ **(Secret Reconstruction)**

To recover the secret state $|\Psi_S\rangle$ *three players out of four need to cooperate. For example:*

- *The two players* P_4 *and* P_3 *cooperate such that* P_4 *adds his share to* $P_3 \mod 2$*:*

$$|\Lambda\rangle \longmapsto \frac{1}{2}\alpha(|0000\rangle + |1101\rangle) + \frac{1}{2}\beta(|0001\rangle + |1100\rangle) \equiv |\Lambda_{4,3}\rangle$$

.

- *Next, P_2 and P_4 cooperate, such that P_2 adds her share to P_4:*

$$|\Lambda_{4,3}\rangle \longmapsto \frac{1}{2}\alpha(|0000\rangle + |1100\rangle) + \frac{1}{2}\beta(|0001\rangle + |1101\rangle) \equiv |\Lambda_{2,4}\rangle.$$

Grouping together the shares:

$$|\Lambda_{2,4}\rangle = \frac{1}{2}(|000\rangle + |110\rangle)\underbrace{(\alpha|0\rangle_4 + \beta|1\rangle_4)}_{|\Psi_S\rangle}.$$

Thus we see that player P_4 has the secret state and therefore the $[[4,1,2]]$-quantum error correcting code looks like a $((3,4))$ secret sharing threshold scheme.

☡ *That would be the end of the story if we forgot that QTS must be* perfect *secret sharing schemes. We want to make sure that no information leaks to less than three players. To check for this possibility we compute the reduced density matrix on any two players, say (without loss of generality) for example of players P_1 and P_3.*

$$\rho_{13} = \frac{1}{2}|\alpha|^2(|00\rangle\langle 00| + |11\rangle\langle 11|) + \frac{1}{2}|\beta|^2(|01\rangle\langle 01| + |10\rangle\langle 10|).$$

In view of the result, we conclude that if the two players cooperate, their density matrix depends on α and β and thus can get statistical information about their relative values. Already if they measure their qubits they can differentiate the secret α from β just by announcing if they get the same $\{\{00\},\{11\}\}$ or different results $\{\{10\},\{01\}\}$ respectively.

For completeness, if we compute the reduced density matrix for just one player say P_1 we get

$$\rho_1 = \frac{1}{2}(|\alpha|^2(|0\rangle\langle 0| + |1\rangle\langle 1|) + \frac{1}{2}|\beta|^2(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2},$$

and therefore the reduced density matrix depends neither on α nor on β; i.e. no single player gets any information about the secret as should have been the case with two players as well.

This was an example of a quantum code that is an error correcting code but not a *perfect* $((k,n))$ secret sharing scheme, since information about the secret is leaked out to less than k cooperating players. We will not consider such imperfect schemes from now on.

Finally, we give the reciprocal of Theorem 3.30, which first appeared in [24] where the authors gave a constructive proof using a class of *quantum polynomial codes* similar to those defined by Aharonov and Ben-Or in [1]. The authors gave a construction for such a code whenever $m < 2k$ where m is the length parameter of the code and of (quantum polynomial) degree $k-1$. They showed how the encoded data can always be recovered from any set of k of its m coordinates. Thus, they constructed an $[[m,1,k]]$-quantum code for the specific case of $m = 2k-1$ and by applying Corollary 3.39 they obtained the desired $((k,n))$- threshold scheme when $n = m$.

Theorem 3.42. *[24] If $n < 2k$, then a $((k,n))$-threshold scheme exists. Moreover, the dimension of each share can be bounded from above by $2\max(2k-1,s)$, where s is the dimension of the quantum secret.*

Although we have said that pure quantum secret sharing schemes are a special case, they still play a fundamental role in the general theory of *QSS* as we will see in the following section by presenting more properties of general access structures and a generalization of Theorem 3.29 which was given for the special case of threshold schemes.

3.2.3 A Closer Look at General Access Structures

In this section, we are concerned with constructing general access structures and to do so we take a small step back and look once again at the classical world. In classical secret sharing, any monotone access structure (c.f. Definition 3.4) can be described by concatenating threshold schemes [31]. The concatenation is done in the following way: the shares of one scheme is used as the secret to be shared by the other scheme. We give an example to illustrate the idea and by the same token review some ideas from classical schemes.

Example 3.43. *Consider the set of players $\mathscr{P}_4 = \{P_1,P_2,P_3,P_4\}$ and the following access structure*[7] $\Gamma = \{\{P_1,P_2,P_3\},\{P_1,P_4\}\}$. *For this purpose, we are going to use a* $(5,7)$*-classical threshold scheme. The dealer $\mathscr{D}$ has a total of seven shares to distribute among $\mathscr{P}_4$ and any subset of Γ having five (or more) of those shares will be able to reconstruct $\mathscr{S}$. In order to realize the first authorized set (call it A), we give three shares to player P_1, and one share each to players P_2 and P_3. In order to realize the second authorized set $B = \{P_1,P_4\}$, we give P_1 three shares but this time two shares to P_4.*
ℹ$\mathscr{N}.\mathscr{B}$. *When the number of shares given to each player is not identical we call such a scheme* ***asymmetric****.*
For more general schemes, the technique known as "concatenation" can be used. We illustrate this technique with the same access structure Γ above to share a secret $\mathscr{S}$.
① *First construct a $(1,2)$ threshold scheme for $\mathscr{S}$ (note that such a scheme is trivial). Let the shares be s_1 and s_2.*
② *Next, we construct a $(3,3)$ threshold scheme for s_1 and give one share to each player in $A = \{P_1,P_2,P_3\}$.*
③ *Repeat the same for the subset B i.e. share s_2 as a secret among P_1 and P_4.*
In this way we have created a secret sharing scheme for Γ by concatenating threshold schemes as described above.

An important lesson from the above example is the way we concatenate the schemes to get another scheme. In [31] Gottesman gives an explanation why this technique works. The main idea is actually borrowed from a very important classical construction [5]: *The Monotone Circuit Construction* [38] reviewed in [64]. As the name implies it is a construction that readily respects the main property common to classical and quantum secret sharing schemes, namely *monotonicity* (c.f. Definition 3.4) but some care needs to be taken in generalizing the construction to the quantum domain.

Any access structure can be written in a *disjunctive* normal form, which is the **OR** of

[7] We emphasize that the secret sharing protocol is completely determined by its access structure Γ and although in this example we have only four players we do not want to realize an arbitrary four-player SSS, but we want to realize ***the*** access structure given above and that is why we need a $(5,7)$-threshold scheme instead of say a trivial $(4,4)$ scheme (giving each player a single share) which would be a 4-player scheme but would not realize the associated Γ.

a list of authorized sets. For our example above, with the access structure Γ and the two authorized subsets A and B, the normal form realizing Γ is $(P_1$ **AND** P_2 **AND** $P_3)$ **OR** $(P_1$ **AND** $P_4)$, where we see the importance of the share holder P_1 for the success of the scheme. We note that the **AND** gate corresponds to (t,t) threshold schemes, with $t = 3$ for "P_1 **AND** P_2 **AND** P_3" and $t = 2$ for "P_1 **AND** P_4". We also note that the **AND** gate corresponds to a $(2,2)$ threshold scheme. This is true of the **AND** gate in $(P_1$ **AND** $P_4)$ but not those in $(P_1$ **AND** P_2 **AND** $P_3)$ having one authorized set P_1 **AND** P_4, while the **OR** gate corresponds to a $(1,2)$ threshold scheme since all the variables in the predicate are fulfilled i.e. either the authorized subset A **OR** B can reconstruct the secret. This is thus done by concatenating the appropriate set of threshold schemes. This technique would not work directly in the quantum domain because the QTS that would be needed to implement the **OR** gate doe snot exist.

Before discussing the quantum analog of the previous example, we need the following theorem, which first appeared in [31]. The theorem helps a great deal in generalizing pure state secret sharing schemes and shows the important role they play in *QSS* constructions. Here, we give the proof that D. Gottesman gave in [31] while the access structure for the corresponding pure state scheme was given by A. Smith [62] using the *Monotone Span Program* construction (*MSP* for short), which we will sketch very briefly in the next section.

Theorem 3.44. *Every mixed state QSS scheme can be described as a pure state QSS scheme by discarding one share.*

Proof. **[31]** Let $\mathscr{S}$ be the Hilbert space of the secret and let V be a superoperator mapping $\mathscr{S}$ to density operators on $\mathscr{H}$. If the encoding is a mixed state encoding we can purify it by adding an extra share. Denote the space corresponding to the extra share by $\mathscr{E}$. The superoperator V can thus be extended to a unitary mapping $\mathscr{S} \longmapsto \mathscr{H} \otimes \mathscr{E}$. Purifying the scheme will not turn authorized sets into unauthorized sets or vise versa. Once again we use the *QSS/QECC* correspondance in what follows:

Consider a set U containing the extra share $\mathscr{E}$ we look at its complement U^c (such that $\mathscr{E} \notin U^c$). If U^c is an authorized set then we can correct for erasure errors on U and condition 2.22 and its consequence Equation 2.23 hold and thus we can get no information whatsoever about the secret from U. On the other hand, if U^c is an unauthorized set, we can correct erasure on its complement and thus reconstruct the unknown state from just U and therefore U is an authorized set. To recover the original mixed state scheme we just need to discard the extra share $\mathscr{E}$. □

This theorem generalizes Theorem 3.29 for threshold schemes. It is one of the cornerstones of quantum secret sharing theory since any theorem or statement about *QSS* can now be proved by just giving the proof for the purification of the scheme if the latter is mixed. Working with pure state schemes is far more elegant than with mixed states since one has powerful tools and techniques not available for the latter.

For example the quantum information theoretical approach to quantum secret sharing [48] and to quantum error correcting codes [21] relies extensively on the purification technique to compute the entropy of a secret and thus the mutual information between the secret state and its reference system or the amount of information that a given set of players can gain from their coalition (c.f. [57] for detailed calculations in that direction).

The following theorem asserts that we can concatenate quantum schemes to get a new one which is also a valid secret sharing scheme. The proof given by Gottesman in [31] follows closely that of Theorem 3.44 given above using the *QECC/QSS* correspondence together with the property of monotonicity of a larger set which has as one of its subsets an authorized set.

Theorem 3.45. *If $\mathscr{S}_1$ and $\mathscr{S}_2$ are quantum secret sharing schemes, then the scheme formed by expanding each share in $\mathscr{S}_1$ as the secret of $\mathscr{S}_2$ is also a secret sharing scheme.*

The theorem tells us how to concatenate the schemes and thus we are finally ready to revisit the quantum version of Example 3.43.

Example 3.46. $((2,3))$***-Concatenated Quantum Schemes***

The construction we described in Example 3.43 fails when we consider its quantum counterpart because the no-cloning theorem prevents us from having a valid $((1,2))$

secret sharing scheme i.e. the **OR** *gate cannot be used in the quantum version of concatenating schemes as we had already observed. To overcome this difficulty, Gottesman suggests in [31] to replace the* **OR** *gate by the* majority function*; i.e. replacing the* $(1,2)$*-classical scheme by an* $((r,2r-1))$ *quantum scheme where r is the number of authorized sets in the access structure one wants to construct. That is, r of the quantum shares will be those of the desired access structure while the remaining* $r-1$*-quantum shares will be those forming another access structure much simpler to construct.*

For the access structure of Example 3.43 $\Gamma = \{A_1, A_2\}$ *where* $A_1 = \{P_1, P_2, P_3\}$ *and* $A_2 = \{P_1, P_4\}$ *with secret* $\mathscr{S}$*, we first note that because of the monotonic property of threshold schemes, adding an extra share to an authorized set will not alter its capability to reconstruct the secret while we have to be cautious in doing so to respect the quantum nocloning theorem.*

We construct a $((2,3))$*-quantum concatenated scheme as follows:*

Let the secret we want to share be $\mathscr{S}$ *and denote the shares of the* $((2,3))$*-quantum threshold scheme by* s_1*,* s_2 *and* s_3*.*

❶ *First, we construct a* maximal access structure *(c.f. Definition 3.36) for* Γ *above by recalling that the complements of the authorized sets namely* $\{P_4\}$ *and* $\{P_2, P_3\}$ *or any of their subsets, should not be added to the new access structure we are trying to construct. This leaves us with two subsets* $A_3 = \{P_2, P_4\}$ *and* $A_4 = \{P_3, P_4\}$*. Thus the new access structure is now given by* $\Gamma' = \{\{P_1, P_2, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}\}$ *which is* maximal.

❷ *Now, as in the classical case, let* s_1 *be the secret we will share via a* $((3,3))$-QTS *for the players in the subset* A_1 *and* s_2 *the secret for the* $((2,2))$-QTS *for those in* A_2*.*

❸ *We note that* $\Gamma \subset \Gamma'$ *and assume that a scheme for such a maximal access structure exists*[8]*. Then we can share* s_3 *using this scheme for* Γ' *and by Theorem 3.45, we would have completed our construction of a quantum concatenated schemes.*

[8] If it does not exist, this technique does not work.

This scheme is summarized by the following equation [31]

$$((2,3))-scheme\begin{cases} ((3,3)) & : \quad P_1,\ P_2,\ P_3 \\ ((2,2)) & : \quad P_1,\ P_4 \\ \Gamma' & \end{cases} \tag{3.14}$$

The scheme is read as follows: The three rows represent the shares of the $((2,3))$*-scheme. The first two rows are threshold schemes, while the last row is the maximal access structure* Γ'*. Any two rows (out of three) is sufficient to reconstruct the secret* $\mathscr{S}$*. Here for example, player* P_1 *gets a share from each row while player* P_4 *would get only two, one from the second row and one from the third.*

Example 3.46 above is a special case of the general $((r,2r-1))$-quantum scheme. In [31] Gottesman gives the recursive construction in the general case, which itself is a proof for the following core theorem involving quantum secret sharing schemes that in some sense summarizes all the properties and theorems we have presented so far:

Theorem 3.47. *A quantum secret sharing scheme exists for an access structure* Γ *if and only if* Γ *is monotone and satisfies the quantum no-cloning theorem. Furthermore, for any* maximal *quantum access structure, a pure state scheme exists.*

3.2.3.1 Monotone Span Program (MSP)

As we mentioned earlier, the construction of an access structure for the pure state scheme of Theorem 3.44 was given in [62] using the Monotone Span Program:

Definition 3.48. *A* **monotone span program** *(MSP) over a set P is a triple* $(\mathbb{K},M,\psi)$ *where* $\mathbb{K}$ *is a finite field, M is a* $d\times e$ *matrix over* $\mathbb{K}$ *and* $\psi:\{1,\ldots,d\}\to P$ *is a surjective function which (effectively) labels each row of M by a member of P.*

The idea behind using *MSP* to construct *QTS* is to be able to relate *QTS* to *CSS* codes (c.f. Section 2.2.1.1). One starts by constructing a matrix from a *CSS* code that is needed for the *MSP* construction. Then this matrix is used to show that a *CSS* code over two classical *MDS* codes with parameters $[[2k-1,k,k]]_q$ and $[[2k-1,k-1,k+1]]_q$ (c.f. the construction of Theorem 2.44) can be interpreted as a $((k,2k-1))$ *QTS*. Finally, one can prove that a $((k,2k-1))$ *QTS* made from the *MSP* construction can be translated into a $[[2k-1,1,k]]_q$ quantum *MDS* code thus relating the *MSP* construction to Gottesman's theorem cited above. The details of the construction can be found in the original paper by A. Smith [62] and an information theoretical approach to the *MSP* construction could be found in [57].

3.3 Quantum Secret Sharing Without Quantum Channels

Up to know, we never questioned what kind of resources were needed for constructing quantum threshold schemes. Since we still do not have a scalable quantum computer, we need to be as economic as possible in our quantum devices. It is still far from trivial to be able to manipulate a large number of qubits as would require the implementation of any given quantum algorithm.

Here since we are mainly concerned with quantum secret sharing protocols, we look at what we have presented so far to guide us to solve this quantum economical question. For example, the recursive construction of a $((r,2r-1))$-general secret sharing scheme as demonstrated in Example 3.46 is far from being efficient. We see this first, because we need a plethora of quantum shares when constructing the maximal access structure Γ'. Second, the threshold schemes in the first and second rows of Equation 3.14 depend on the details of the schemes themselves and unless those schemes are efficient, the entire procedure becomes exceedingly needy in quantum shares. Of course, the best way to save on our quantum computer is to use as few quantum shares as possible, and in doing so we also save on the quantum channels that are needed between the users to reconstruct the secret. We therefore save on the technology and on the number of qubits that are needed to be under control to implement such an important scheme as secret sharing.

In this section, we present a protocol that we first introduced in [13] that resolves this issue of needing a plethora of quantum shares per player. In fact our protocol is maximally efficient in the sense that it requires one quantum share per player. This quantum share is the one given to each player by the dealer $\mathscr{D}$. So in an n-player protocol we only need a total of n quantum shares to implement it. Therefore, we only need one quantum channel[9] between the dealer $\mathscr{D}$ and each player P_i (where $1 \leq i \leq n$). The reconstruction procedure between players can be achieved with purely classical communication between the players, although the resulting reconstructed state is quantum.

What we have described so far sounds like quantum teleportation (c.f. the preliminary section). Thus why can't we trivially use quantum teleportation [6] to share our given secret quantum state? Indeed in [3], using quantum teleportation, it was shown how to construct a $((2,2))$-quantum threshold scheme which can be straightforwardly generalized to $((n,n))$-*QTS*. The problem with the construction is twofolds:

1. The construction in [3] gives a non-perfect threshold scheme. That is, although the n players can reconstruct the quantum secret perfectly, it is not true that coalitions of less than n players get no information about the secret. In fact it was shown in [57] using information theoretical tools that indeed this was the case and thus concluded that the protocol was a non perfect quantum threshold scheme. The same problem was encountered earlier in Example 3.41, which prevented us from triumphantly say that: "every quantum error correcting code is also a quantum secret sharing scheme". The example was introduced mainly to refute this kind of non-perfect threshold schemes.

2. The construction uses *quadratically* more quantum shares than our protocol. We state this as a theorem and give the proof [13]:

Theorem 3.49. *In a one-qubit teleportation-based $((n,n))$-secret sharing scheme, $\frac{n^2-n}{2}$ shared $|\Psi^-\rangle$ states are necessary and sufficient for the reconstruction of the secret. Moreover, if we add the requirement that each share of the encoded state (in the distribution phase of the protocol) consists of one qubit, the total number of qubits required for the teleportation-based scheme is n^2.*

Proof. As usual, let $\mathscr{D}$ be the dealer and let $\mathscr{P}$ be the total set of participants. Since each participant $P_i \in \mathscr{P}$ (with $1 \leq i \leq n$) is the potential receiver of the secret state, each P_i

[9] That is only one use of the quantum channel.

must be linked to every other participant by at least one disjoint path consisting of $|\Psi^-\rangle$ states. In other words, if we see the participants as vertices v_i, and the shared EPR-pairs (i.e. entanglement) as edges e_{ij}, thus forming what is known as a K_n *EPR*-graph, we have that each vertex v_i must have degree $d(v_i) \geq n-1$. Counting the degree at each vertex yields a lower bound of $n(n-1)/2$ for the total number of edges. Since the complete EPR-graph K_n, satisfies our criteria, we have the desired result.
Finally, since the dealer $\mathscr{D}$ gives each participant P_i one qubit as a share, we have thus a total of $n+2\underbrace{\frac{1}{2}(n^2-n)}_{\text{edges}} = n^2$ qubits required for this teleportation-based scenario. □

Clearly, to overcome the problems mentioned above, we need a protocol that preserves secrecy, respects the threshold structure of the *QSS*-scheme and uses only one quantum share per player. Before presenting our protocol, which respects those characteristics, we need an important tool know as *quantum encryption* first introduced in [2].

3.3.1 Quantum Encryption of Qubits

The encryption scheme of qubits works as follows: Suppose we have an n-qubit quantum state $|\Psi\rangle$ and a random sequence of $2n$ classical bits. We associate to each qubit a pair of classical bits a qubit that determines which transformation $\sigma \in \{I, X, Y, Z\}$ is to be applied to the respective qubit. If the pair is $\{00\}$, the identity I is applied to the qubit; if $\{01\}$, X is applied; if $\{10\}$, Y is applied and finally if the pair is $\{11\}$ we apply Z. Clearly if σ is chosen uniformly at random in the set, the resulting quantum state $|\Psi'\rangle$ is completely mixture i.e.

$$\rho_{|\Psi'\rangle} = \frac{1}{4}\left(I|\Psi'\rangle\langle\Psi'|I + X|\Psi'\rangle\langle\Psi'|X + Y|\Psi'\rangle\langle\Psi'|Y + Z|\Psi'\rangle\langle\Psi'|Z\right) = \frac{1}{2}I,$$

i.e. the totally mixed state for any given $|\Psi'\rangle$.

However, with the knowledge of the classical $2n$-bit sequence, the sequence of operators that was applied to $|\Psi\rangle$ is known therefore the process can be reversed and the state $|\Psi\rangle$ recovered.

ℹ$\mathscr{N}.\mathscr{B}$. Thus, classical data can be used to encrypt quantum data.

We will also need the following definition:

Definition 3.50. *Informally, by a* Local Operation and Classical Communication (LOCC) *measurement we mean one that can be implemented by two (or more) parties using only local quantum operations and classical communication.*

3.3.2 Protocol for Quantum Secret Sharing with LOCC

We finally present our $((n,n))$-threshold *Quantum Secret Sharing with Classical Reconstruction* (QSS-CR) protocol (c.f. Figure 3.2 for a diagrammatic representation). In the first and most crucial step, we will use a partial encryption as opposed to the full encryption presented above, but the idea remains identical.

Suppose the dealer $\mathscr{D}$ wishes to share the quantum secret state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ among a set $\mathscr{P}$ of n participants (with the usual normalization condition $|\alpha|^2 + |\beta|^2 = 1$).

1. ⚂⚄ **(Partial encryption)**

   The dealer chooses uniformly at random $x \in \{0,1\}$.

   ① If $x = 0$, he does nothing (i.e. applies the identity) to $|\Psi\rangle$ for this step.

   ② If $x = 1$, he applies the negation transformation, N (c.f. Equation 1.2).

   Let the resulting state be $|\Psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$.

2. ➠**(Encoding)**

   The dealer encodes $|\Psi'\rangle$ into an n-qubit state by creating $n-1$ *pseudo-copies*; the resulting state is a GHZ-state mainly:

$$|\Psi''\rangle = \alpha'|0^n\rangle + \beta'|1^n\rangle \tag{3.15}$$

3. 📱 **(Share Distribution)**

   The dealer $\mathscr{D}$ picks uniformly at random a bit string $x' = x_1x_2\ldots x_n$ such that $\bigoplus_{i=1}^{n} x_i = x$ (i.e s.t. the parity $\Pi(x') = x$) and gives each player P_i a share consisting of a classical bit x_i and of a qubit $|\cdot\rangle_i$ from $|\Psi''\rangle$.

4. ⌕ **(Secret Reconstruction)**

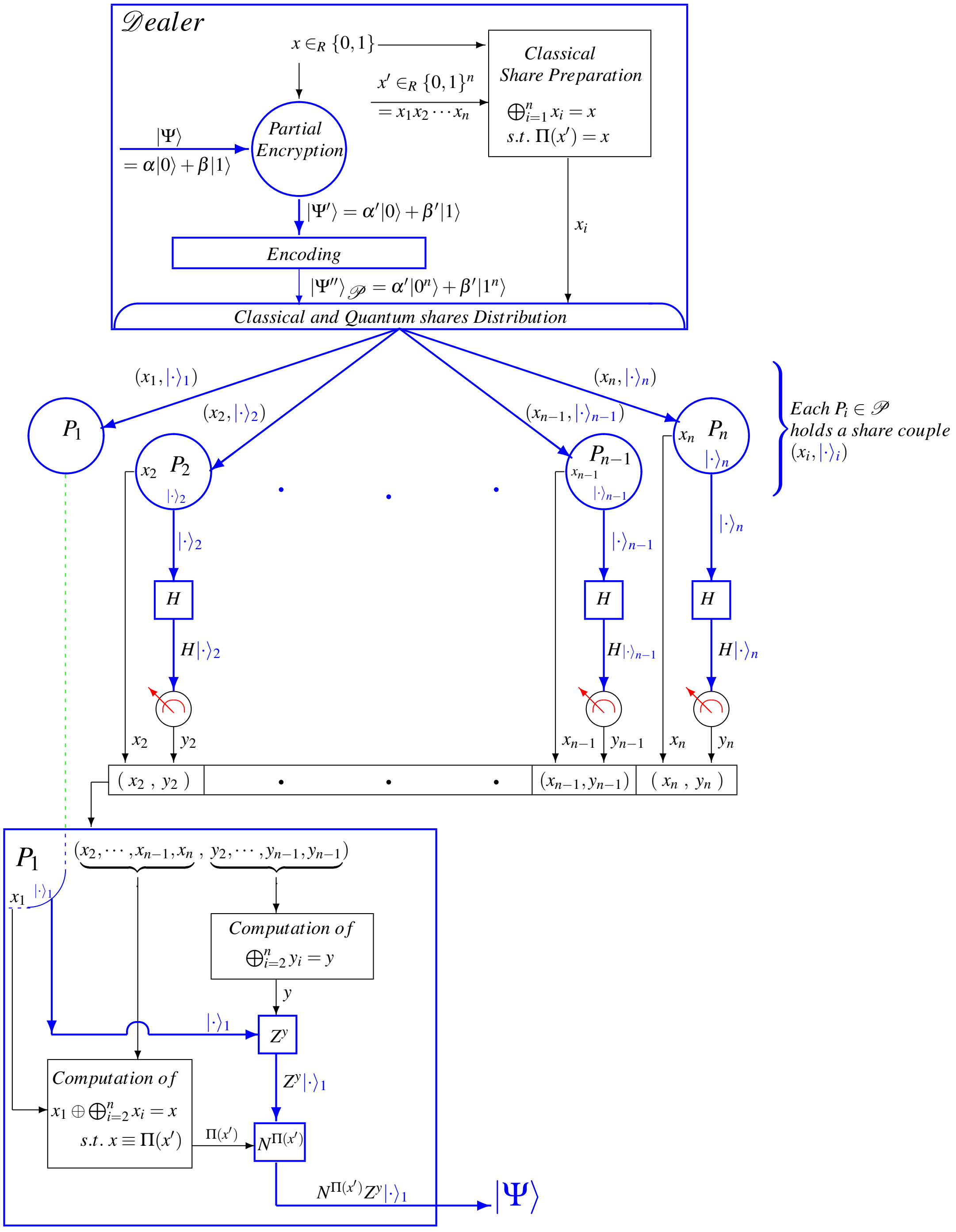
The players decide who will receive the secret; say that they agree on player 1. Then they do the following:

- Player i $(i = 2, 3, \ldots, n)$ applies the Hadamard transform H (c.f. Equation 1.4) to his qubit.
- Player i $(i = 2, 3, \ldots, n)$ measures his qubit in the computational basis.
  Let the outcome be y_i. This value, along with x_i is sent to P_1.
- Player 1 computes $y = \bigoplus_{i=2}^{n} y_i$.
  If $y = 0$, he does nothing. If $y = 1$, he applies Z to his qubit:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.16}$$

- Player 1 computes $x = \bigoplus_{i=1}^{n} x_i$.
  ① If $x = 0$, he does nothing.
  ② If $x = 1$, he applies N to his qubit.
  The result is the reconstructed secret.

Figure 3.2: The QSS-Protocol with Classical Reconstruction.


$\mathscr{D}ealer$
$x \in_R \{0,1\}$
Classical Share Preparation
$\bigoplus_{i=1}^{n} x_i = x$
$s.t.\ \Pi(x') = x$
$x' \in_R \{0,1\}^n$
$= x_1 x_2 \cdots x_n$
$|\Psi\rangle$
$= \alpha|0\rangle + \beta|1\rangle$
Partial Encryption
$|\Psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$
x_i
Encoding
$|\Psi''\rangle_{\mathscr{P}} = \alpha'|0^n\rangle + \beta'|1^n\rangle$
Classical and Quantum shares Distribution
$(x_1, |\cdot\rangle_1)$
$(x_2, |\cdot\rangle_2)$
$(x_{n-1}, |\cdot\rangle_{n-1})$
$(x_n, |\cdot\rangle_n)$
Each $P_i \in \mathscr{P}$ holds a share couple $(x_i, |\cdot\rangle_i)$
P_1
P_2
x_2
$|\cdot\rangle_2$
P_{n-1}
x_{n-1}
$|\cdot\rangle_{n-1}$
P_n
x_n
$|\cdot\rangle_n$
H
$H|\cdot\rangle_2$
$H|\cdot\rangle_{n-1}$
$H|\cdot\rangle_n$
y_2
y_{n-1}
y_n
(x_2, y_2)
(x_{n-1}, y_{n-1})
(x_n, y_n)
$(x_2, \cdots, x_{n-1}, x_n, y_2, \cdots, y_{n-1}, y_{n-1})$
x_1
$|\cdot\rangle_1$
Computation of $\bigoplus_{i=2}^{n} y_i = y$
y
Z^y
$Z^y|\cdot\rangle_1$
Computation of $x_1 \oplus \bigoplus_{i=2}^{n} x_i = x$
$s.t.\ x \equiv \Pi(x')$
$\Pi(x')$
$N^{\Pi(x')}$
$N^{\Pi(x')} Z^y |\cdot\rangle_1$
$|\Psi\rangle$

☞ In the diagram above, the time flow is from top to bottom. The blue material denotes quantum objects (i.e. qubits, quantum channels, and necessary quantum transformations). For example the arrows emanating from the dealer to the players denote quantum channels. When arrows and boxes are black, only classical operations and channels are needed.

3.3.2.1 Correctness and Privacy

We now show using the mathematical properties of the GHZ-state introduced in Section 1.1.3 that our *QSS-CR* protocol produces the correct output (Theorem 3.51) and that it is secure against collusion of less than n players (Theorem 3.52).

Theorem 3.51. *At the end of the* QSS-CR *protocol, the intended recipient has the initial quantum state* $|\Psi\rangle$.

Proof. After the execution of the *Partial Encryption*, the *Encoding* and *Share Distribution* steps of the protocol, the n players decide who will receive the secret state. Say they agree (without loss of generality) on the n^{th} player P_n. We follow the steps of the *Secret Reconstruction* phase.
After the *Encoding* step, the state of the n shares is:

$$|\Psi''\rangle = \alpha'|0^n\rangle + \beta'|1^n\rangle \tag{3.17}$$

Let $\mathscr{P}$ denote the set of all players. Now all $P_i \in \mathscr{P}$ (for $1 \leq i \leq n-1$) apply to their shares the Hadamard transform:

$$\begin{aligned}
|\Psi\rangle_{\mathscr{P}} = (H^{n-1} \otimes I)|\Psi''\rangle &= \alpha' H^{n-1} \underbrace{|00\ldots0\rangle}_{n-1} |0\rangle_n + \beta' H^{n-1} \underbrace{|11\ldots1\rangle}_{n-1} |1\rangle_n, \\
&= \frac{\alpha'}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle|0\rangle_n + \frac{\beta'}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{P(y)} |y\rangle|1\rangle_n, \\
&= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle \otimes (\alpha'|0\rangle_n + (-1)^{P(y)}\beta'|1\rangle_n), \qquad (3.18)
\end{aligned}$$

where $P(y) = y_1 + y_2 + \ldots y_{n-1}$, $N = 2^{n-1}$ and we made use of the properties of the Hadamard transformed GHZ-state Equation 1.26 (appropriately modified).
Let $|\Psi^{(y)}\rangle$ denote the state:

$$|\Psi^{(y)}\rangle \equiv \alpha'|0\rangle + (-1)^{P(y)}\beta'|1\rangle. \tag{3.19}$$

We compute the density matrix of the system $|\Psi\rangle_{\mathscr{P}}$.

$$\rho_{\mathscr{P}} = \frac{1}{N}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1} |y\rangle\langle y'| \otimes |\Psi^{(y)}\rangle_n\langle\Psi^{(y')}|. \tag{3.20}$$

Now players P_i $(i = 1,2,\ldots,n-1)$ measure their qubits in the computational basis (i.e. we trace over those shares).

$$\begin{aligned}
\rho_{P_n} &= \sum_{k=0}^{N-1} (\langle k| \otimes I)\ \rho_{\mathscr{P}}\ (|k\rangle \otimes I), \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1} (\langle k| \otimes I)\ |y\rangle\langle y'| \otimes |\Psi^{(y)}\rangle_n\langle\Psi^{(y')}|\ (|k\rangle \otimes I), \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1} \underbrace{\langle k|y\rangle}_{\delta_{k,y}} |\Psi^{(y)}\rangle_n\langle\Psi^{(y')}| \underbrace{\langle y'|k\rangle}_{\delta_{k,y'}}, \\
&= \frac{1}{N}\sum_{y=0}^{N-1} |\Psi^{(y)}\rangle_n\langle\Psi^{(y)}|.
\end{aligned} \tag{3.21}$$

Let the result of player P_i's measurement of his qubit be y_i. Each P_i now sends the couple (x_i, y_i) to player P_n where x_i is the bit received from the dealer $\mathscr{D}$ subject to the partial encryption condition $x = \bigoplus_{i=1}^{n} x_i$.

Now, since P_n has received all the y_i's he can compute $P(y) = y_1 + y_2 + \ldots + y_{n-1}$, which appears in $|\Psi^{(y)}\rangle_n$ and therefore the sum in Equation 3.21 evaluates to $N|\Psi^{(y)}\rangle_n\langle\Psi^{(y)}|$ for the given $P(y)$ i.e.

$$\rho_{P_n} = |\Psi^{(y)}\rangle_n\langle\Psi^{(y)}|. \tag{3.22}$$

Expanding Equation 3.22

$$\begin{aligned}
\rho_{P_n} &= |\alpha'|^2|0\rangle\langle 0| + (-1)^{P(y)}\left(\alpha'\beta'^*|0\rangle\langle 1| + \beta'\alpha'^*|1\rangle\langle 0|\right) + |\beta'|^2|1\rangle\langle 1| \\
&= \begin{pmatrix} |\alpha'|^2 & (-1)^{P(y)}\alpha'\beta'^* \\ (-1)^{P(y)}\beta'\alpha'^* & |\beta'|^2 \end{pmatrix}
\end{aligned} \tag{3.23}$$

Since player P_n has all the y_i's he computes $P(y)$.
If $P(y)=0$, he has readily the (partially encrypted) secret state:

$$\begin{aligned}\rho_{P_n}^{Final} &= I\,\rho_{P_n}^{(0)}\,I = \begin{pmatrix} |\alpha'|^2 & \alpha'\beta'^* \\ \beta'\alpha'^* & |\beta'|^2 \end{pmatrix} \\ &= |\Psi'\rangle\langle\Psi'|. \end{aligned} \tag{3.24}$$

While if $P(y)=1$ he applies the Z operator to his qubit to recover the original state

$$\begin{aligned}\rho_{P_n}^{Final} &= Z\,\rho_{P_n}^{(1)}\,Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} |\alpha'|^2 & -\alpha'\beta'^* \\ -\beta'\alpha'^* & |\beta'|^2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= |\Psi'\rangle\langle\Psi'|, \end{aligned} \tag{3.25}$$

where $\rho_{P_n}^0$ and $\rho_{P_n}^1$ denote ρ_{P_n} evaluated at $P(y)=0$ and $P(y)=1$ respectively.

Since P_n also has all the x_i's he can now compute $x=\bigoplus_{i=1}^n x_i$ and now decrypt his state via

$$(\alpha',\beta') = \begin{cases} (\alpha,\beta) & \text{if } x=0, \text{ i.e. he does nothing,} \\ \\ (\beta,\alpha) & \text{if } x=1, \text{ i.e. he applies } N. \end{cases} \tag{3.26}$$

□

Theorem 3.52. *In the* QSS-CR *protocol, any subset of $k<n$ players can get no information whatsoever about the initial state $|\Psi\rangle$.*

Proof. We assume that players $P_1,P_2,\ldots,P_{n-1}$ pool their quantum shares together as well as their classical bits x_i in an attempt to recover the original state. We now show that their joint state is independent of the initial secret state $|\Psi\rangle$.

Taking into account the partial encryption of the original state, and denoting by $\Pi(x')\in\{0,1\}$ the parity of $x'=x_1x_2\cdots x_n$ subject to the condition $x=\bigoplus_{i=1}^n x_i$ we have that the total density matrix of the system that the dealer $\mathscr{D}$ now holds is given by:

$$\begin{aligned}\rho_{\mathscr{D}}^{Full} &= \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes N^{\Pi(x')}|\Psi\rangle\langle\Psi|N^{\Pi(x')}, \\ &= \frac{1}{2}\rho_{|\Psi\rangle} + \frac{1}{2}\rho_{N|\Psi\rangle}. \end{aligned} \tag{3.27}$$

Recall that after encoding and share distribution the density matrix of the n players was again given by

$$\rho_{\mathscr{P}} = \frac{1}{N}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1} |y\rangle\langle y'| \otimes |\Psi^{(y)}\rangle_n\langle\Psi^{(y')}|. \tag{3.28}$$

with $|\Psi^{(y)}\rangle \equiv \alpha'|0\rangle + (-1)^{P(y)}\beta'|1\rangle$. Combining equations (3.27) and (3.28) we thus have that the full density matrix of the $\mathscr{P}$-set is given by

$$\rho_{\mathscr{P}}^{Full} = \frac{1}{2N}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1} |y\rangle\langle y'| \otimes \underbrace{\left(|\Psi^{(y)}\rangle_n\langle\Psi^{(y')}| + N|\Psi^{(y)}\rangle_n\langle\Psi^{(y')}|N\right)}_{\rho_{P_n}^{Full}}. \tag{3.29}$$

In matrix form:

$$\begin{aligned}\rho_{P_n}^{Full} &= \begin{pmatrix} |\alpha'|^2 & (-1)^{P(y')}\alpha'\beta'^* \\ (-1)^{P(y)}\beta'\alpha'^* & (-1)^{P(y)+P(y')}|\beta'|^2 \end{pmatrix} + \begin{pmatrix} |\beta'|^2 & (-1)^{P(y')}\beta'\alpha'^* \\ (-1)^{P(y)}\alpha'\beta'^* & (-1)^{P(y)+P(y')}|\alpha'|^2 \end{pmatrix} \\ &= \begin{pmatrix} |\alpha'|^2+|\beta'|^2 & (-1)^{P(y')}\left(\alpha'\beta'^*+\beta'\alpha'^*\right) \\ (-1)^{P(y)}\left(\beta'\alpha'^*+\alpha'\beta'^*\right) & (-1)^{P(y)+P(y')}\left(|\beta'|^2+|\alpha'|^2\right) \end{pmatrix}. \end{aligned}$$

This can be simplified on account of the normalization condition $|\alpha'|^2 + |\beta'|^2 = 1$ and $(-1)^{P(y)+P(y')} = 1(\mod 2)$ to:

$$\rho_{P_n}^{Full} = \begin{pmatrix} 1 & (-1)^{P(y')}\,2\Re\left(\alpha'\beta'^*\right) \\ (-1)^{P(y)}\,2\Re\left(\alpha'\beta'^*\right) & 1 \end{pmatrix}. \tag{3.30}$$

Where $\Re\left(\alpha'\beta'^*\right)$ denotes the real part of the expression.

We trace over the share of P_n since we have no access to it on account of the $n-1$ players trying to recover the secret state without P_n's collaboration. In matrix form this reduces to:

$$\begin{aligned}
\rho^{Full}_{\mathscr{P}\backslash P_n} &= \frac{1}{2N}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1}|y\rangle\langle y'|\otimes\left[\underbrace{\begin{pmatrix}1 & 0\end{pmatrix}\rho^{Full}_{P_n}\begin{pmatrix}1\\0\end{pmatrix}}_{1}+\underbrace{\begin{pmatrix}0 & 1\end{pmatrix}\rho^{Full}_{P_n}\begin{pmatrix}0\\1\end{pmatrix}}_{1}\right]\\
&= \frac{1}{N}\sum_{y=0}^{N-1}\sum_{y'=0}^{N-1}|y\rangle\langle y'|. \qquad (3.31)
\end{aligned}$$

Therefore, we see that the density matrix of the $(n-1)$ players is completely independent of the secret state $|\Psi\rangle$. □

Remark 3.53. *We thus note that the* Partial Encryption *step saves the day since the classical bits $x_1, x_2, \ldots, x_{n-1}$ are uniformly distributed over all possible combinations and thus being independent of all the other steps in the protocol, reveal nothing about x, itself leaving P_n's qubit in the totally mixed state. And thus the set $\mathscr{P}\backslash P_n$ is left with a uniform combination of all possible $y \in \{0,1\}^{n-1}$.*

Going back to remark 3.40 at the end of Section 3.2.2, on one hand, we mentioned that all quantum secret sharing schemes were quantum error correction codes but that the reverse was not necessary true. We gave an example of such a case (cf. Ex.3.41). On the other hand, we also mentioned the possibility of overcoming such a limitation i.e. transforming a quantum error correcting code that at first sight was not a perfect quantum secret sharing schemes into one. The following corollary to remark 3.53 shows how we can go about doing this:

Corollary 3.54. *The* $[[4,1,2]]$*-QECC of Example 3.41 can be turned into a perfect* $((3,4))$*-QTS provided we partially encrypt the state prior to encoding.*

Proof. As in Example 3.41, let the state we want to encode be $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. After partial encryption we have the state $|\psi\rangle \mapsto |\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ with

$$(\alpha', \beta') = \begin{cases} (\alpha, \beta) & \text{if } x = 0, \\ \\ (\beta, \alpha) & \text{if } x = 1, \end{cases} \tag{3.32}$$

where the variable x was picked uniformly at random in $\{0, 1\}$ by the dealer $\mathscr{D}$.

Since this encryption holds independently of any arbitrary unitary transformation the collaborating unauthorized players decide to apply to their shares, it will prevent them from getting any useful statistical information about α and/or β.

In order to recover the original state, the players proceed as in Example 3.41, while the encryption variable x could be shared using a classical threshold scheme such as Shamir or Blakley's (c.f. Example 3.3 above).

In particular, in this example any set of two or less players would get no such statistical information as is required by a perfect *QSS*. Therefore, only the intended authorized sets will be able to recover the original state and we are left with a perfect $((3, 4))$-QSS scheme. □

3.4 Summary

In this core chapter, we presented the classical and quantum theories of secret sharing schemes, emphasizing the most important properties, constructions and theorems that are known in the literature. We also gave classical and quantum examples to support and solidify the theoretical ideas introduced throughout the text. The major lines of the chapter consisted on linking quantum error correcting codes (presented in chapter 2) with quantum secret sharing.

Our major contribution to QSS was the presentation of a *perfect* $((n, n))$ quantum threshold scheme with LOCC that minimized the number of quantum shares needed to reconstruct the quantum secret state. We were able to reduce the number of quantum shares to a single one per player putting our protocol within reach of an experimental implementation. The robustness of our resulting perfect scheme rested on the use of a partial quantum encryption step prior to the encoding of the secret state. This crucial step prevented any leakage of statistical information about the secret state to unauthorized sets of players. We used the same technique (c.f. Corollary 3.54) to show that it was possible to convert a QECC code to a *perfect* QSS schemes which without the partial encryption step was given in [24] as an example of the statement that “All quantum secret sharing schemes are quantum error correcting codes but that *the reverse is not necessary true*”.

CONCLUSION AND FUTURE WORK

We have seen throughout this thesis the interplay between quantum error corrections and quantum secret sharing protocols, especially at the quantum level. Based on these observations, we presented in chapter 2 a glimpse at the theory of classical and quantum error correction codes, while we discussed the theory of classical and quantum secret sharing in chapter 3. One of our goals was to draw parallels between those two complementary domains and in doing so we were able to present formal proofs of general theorems in the theory of quantum secret sharing using first principles of the theory of quantum error correction.

We have seen how the GHZ state gives rise to an elegant and efficient quantum secret sharing protocol with purely classical communication during the reconstruction phase. Because we have significantly lowered the quantum memory requirements, our protocol may be within reach of experimental implementations. At the end of the chapter we discussed as well the possibility of transforming quantum error correcting codes into perfect quantum secret sharing schemes.

Throughout our discussion of secret sharing, we only focused on *perfect* schemes (c.f. Definition 3.8) considering non perfect ones as being shortcomings of the protocols. For example the $((n,n))$-quantum secret threshold scheme based on teleportation [3] was shown in [57] to leak information to non authorized sets of players and thus was non secure. Once again partial encryption as discussed in our quantum protocol comes to the rescue. It suffices to partially encrypt the secret quantum state prior to encoding to turn the protocol into a perfect scheme. Apart from this security question, the efficiency of this teleportation based protocol was questionable. It required n quantum shares per player for a total of n^2 qushares; while in our protocol we only needed a single quantum share per participant for a total of n qushares [13], which as stated above is of great practical interest. Here we coined the term *qushare* for quantum share.

Other interesting schemes that we did not discuss in this thesis consider sharing a classical secret (as opposed to a quantum secret state) using quantum schemes (i.e. using quantum information to securely share a classical secret) [31, 39]. In [44] the authors tried to present a unified framework for quantum secret sharing using graph states [34] by having simultaneously a secure and an efficient scheme (i.e. using only n qushares). They partially succeed in their task. They were able to securely present a threshold scheme in the case of sharing a classical secret, but when the secret to be shared was a quantum state, their threshold scheme suffered from the same problem as the teleportation based protocol. They did not get a perfect threshold scheme and as a consequence unauthorized sets were able to get relevant statistical information about the secret. They pointed out this limitation in [45]. Thus, our protocol remains the only efficient and secure $((n,n))$-quantum threshold scheme with classical reconstruction phase.

Finally, we mention a very promising and interesting approach to quantum secret sharing, which makes use of the theory of *Matroids* [51, 52] to link pure *CSS*-codes (c.f. Section 2.2.1.1) to quantum secret sharing schemes. This approach appears to work provided the secret being shared is classical [53–55], while it fails in the case of sharing a quantum state. The main aim of this approach is to develop efficient quantum secret sharing schemes given that classically, the most efficient schemes have been induced by matroids.

Although a lot of work has been done in the theory of quantum secret sharing, there are a few swampy roads relating the classical theory to its quantum counterpart (c.f. Figure 3.3 below). Shedding light on those swamps might give us very interesting links between matroids, graph states, CSS-codes and MSP-approaches in the context of Quantum Information Theory.

The figure below depicts the road from classical to quantum secret sharing. It shows also the links between quantum error corrections and the theory of secret sharing. The dotted (*blue*) arrows show that the quantum counterpart was built from the classical concept in question. While the double headed arrows show the possibility of moving from one domain to the other. The important question mark in the middle of the diagram points to a very interesting open question: “*Are Ideal schemes and matroids related to Monotone Span Programs as applied to quantum secret sharing and if so what are the more general consequence of such a correspondence?*”

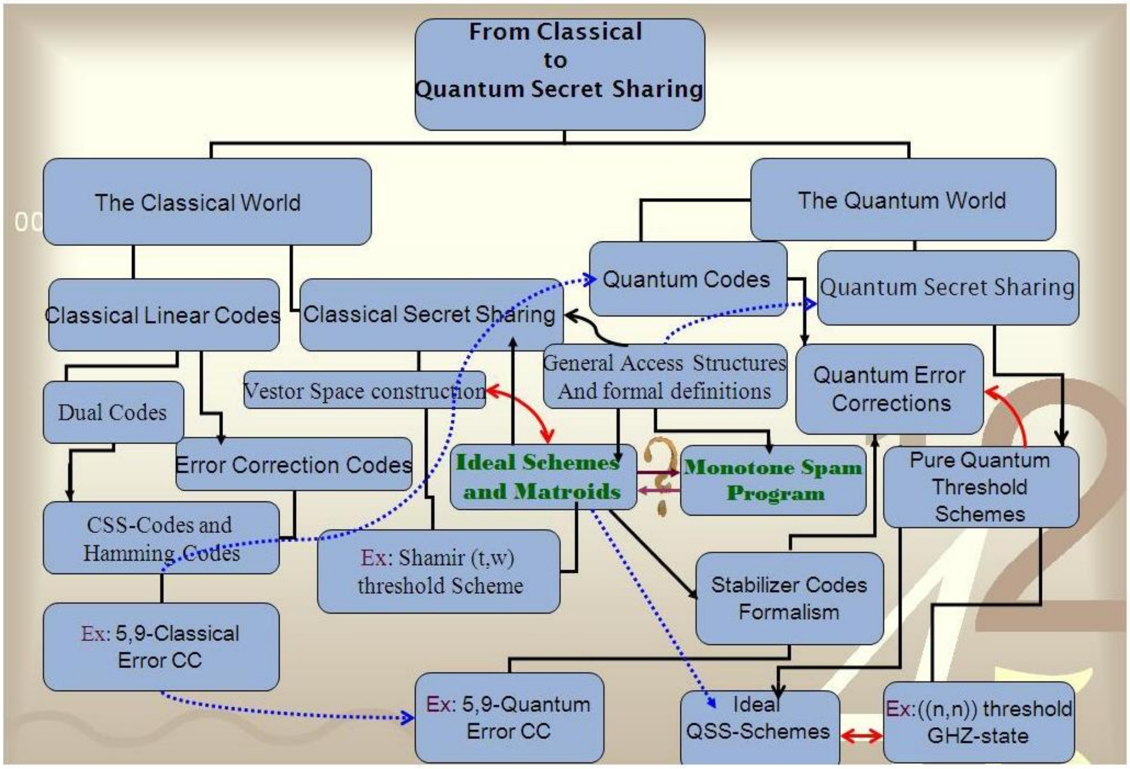


Figure 3.3: The Swampy Road.

BIBLIOGRAPHY

[1] D. Aharonov and M. Ben-Or, “Fault-tolerant quantum computation with constant error.” *Proc. 29th Ann. ACM Symp. on Theory of Computation*, **176** (ACM, New York, 1998); e-print quant-ph/9611025.

[2] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. “Private quantum channels.” *In 41st IEEE Symposium on Foundations of Computer Science (FOCS 00)*, pp.547-553; e-print quant-ph/0003101

[3] S. Bandyopadhyay, “Teleportation and Secret Sharing with Pure Entangled States.” *Phys. Rev. A*, **62**, 012308, 2000; e-print quant-ph/0002032.

[4] J. S. Bell. “On the Einstein-Podolsky-Rosen paradox.” *Physics*, **1**:195–200, 1965.

[5] J. Benaloh and J. Leichter, “Generalized secret sharing and monotone functions.” *Proc. Crypto' 88*, p. 27, 1990.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.” *Physical Review Letters*, **70**:1895-1899, 1993.

[7] G. Blakley, “Safeguarding cryptographic keys.” *Proc. AFIPS*, **48**, 313–317, 1979.

[8] N. Bohr, “Can Quantum-Mechanical Description of Physical Reality be Considered Complete?” *Phys. Rev.*, **48**, 696, 1935.

[9] G. Brassard, “Quantum communication complexity (a survey).” *Foundations of Physics*, **33**, no. 11, pp. 1593 Ű 1616, 2003; e-print quant-ph/0101005.

[10] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, “Anonymous quantum communication.” *In Proceedings of the 13th Annual International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT 2007)*, pages 460-473, 2007.

[11] E. F. Brickell, “Some ideal secret sharing schemes.” *J. Combin. Math. and Combin. Comput.*, **9**, pp. 105-113, 1989.

[12] E. F. Brickell and D. R. Stinson, “Some improved bounds on the information rate of perfect secret sharing schemes.” *J. Cryptology, 1992*, **5**, Number 1, Pages 29-39.

[13] A. Broadbent, P.-R. Chouha, A. Tapp, “The GHZ State in Secret Sharing and Entanglement Simulation.” *ICQNM, pp. 59-62, 2009 Third International Conference on Quantum, Nano and Micro Technologies, 2009.*

[14] H. Buhrman, R. Cleve, and W. van Dam. “Quantum entanglement and communication complexity.” *SIAM Journal on Computing*, **30**(8):1829–1841, 2001; e-print quant-ph/9705033.

[15] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. “Quantum fingerprinting.” *Phys. Rev. Lett.*, **87**(16), September 26, 2001; e-print quant-ph/0102001.

[16] H. Buhrman, R. Cleve, and A. Wigderson. “Quantum vs. classical communication and computation.” In *Proceedings of 30th ACM STOC*, pages 63–68, 1998; e-print quant-ph/9802040.

[17] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp. “Multiparty quantum communication complexity.” *Physical Review A*, **60**(4):2737–2741, 1999; e-print quant-ph/9710054.

[18] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, “Multiparty quantum communication complexity.” *Phys. Rev. A*, **60**:2737Ű2741, 1999.

[19] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist.” *Phys. Rev. A*, **54**, 1098–1105, 1996; e-print quant-ph/9512032.

[20] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction and orthogonal geometry.” *Phys. Rev. Lett.*, **78**, 405–408, 1997; e-print quant-ph/9605005.

[21] N. J. Cerf and R. Cleve, “Information-theoretic Interpretation of Quantum Error-correcting Codes.” *Phys. Rev. A*, **57**, p. 1477, 1998; e-print quant-ph/9702031.

[22] R. Cleve and H. Buhrman. “Substituting quantum entanglement for communication.” *Physical Review A*, **56**(2):1201–1204, 1997; e-print quant-ph/9704026.

[23] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. “Quantum entanglement and the communication complexity of the inner product function.” In *Proceedings of 1st NASA QCQC conference*, **1509** of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1998; e-print quant-ph/9708019.

[24] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret.” *Phys. Rev. Lett.*, **82**, 648, 1999, e-print quant-ph/9901025.

[25] D. Dieks, “Communication by EPR devices.” *Phys. Lett. A*, **92**, 271–272, 1982.

[26] D.P. DiVincenzo and P.W. Shor, “Fault-tolerant error correction with efficient quantum codes.” Phys. Rev. Lett. **77**, 3260, 1996.

[27] A. Einstein, “On the electrodynamics of moving bodies.” *Annalen Phys*, **17**, 891, 1905. [*Annalen Phys.*, **14**, 194, 2005].

[28] A. Einstein, “On the General Theory of Relativity.” *Sitzungsber. Preuss. Akad. Wiss. Berlin (Math. Phys.)*, **1915**, 778, 1915. [Addendum-ibid. **1915**, 799 (1915)].

[29] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of reality be considered complete?” *Phys. Rev.*, **47**, 777, 1935.

[30] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound.” *Phys. Rev. A*, **54**, 1862–1868, 1996; e-print quant-ph/9604038.

[31] D. Gottesman. “On the theory of quantum secret sharing.” *Phys. Rev. A*, **61** , 042311, 2000. Preprint at quant-ph/9910067, Oct. 1999.

[32] M. Grassl, T. Beth, and T. Pellizzari, “Codes for the quantum erasure channel.” *Phys. Rev. A*, **56**, 33–38, 1997; e-print quant-ph/9610042.

[33] D.M. Greenberger, M.A. Horne, and A. Zeilinger. “Going beyond Bell’s theorem.” *In Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, pages 69-72, 1989.

[34] M. Hein, J. Eisert, and H. J. Briegel. “Multiparty entanglement in graph states.” *Phys. Rev. A*, **69**, 062311, 2004.

[35] W. Heisenberg, “A quantum-theoretical reinterpretation of kinematic and mechanical relations.” *Z. Phys.*, **33**, 879, 1925.

[36] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing.” *Phys. Rev. A*, **59**, 1829Ű1834, 1999; e-print quant-ph/9806063.

[37] A. S. Holevo. “Bounds for the quantity of information transmitted by a quantum communication channel.” *Problemy Peredachi Informatsii*, **9**(3):3–11, 1973. English translation in *Problems of Information Transmission*, **9**:177–183, 1973.

[38] M. Ito, A. Saito, T. Nishizeki, “Secret sharing scheme realizing any access structure.” *Proc. IEEE Globecom*, **87**, pp. 99-102, 1987.

[39] A. Karlsson, M. Koashi, and N. Imoto, “Quantum secret sharing schemes and reversibility of quantum operations.” *Phys. Rev. A*, **59**, 162, 1999.

[40] T. Kuhn, The Structure of Scientific Revolutions. 3rd ed. Chicago, IL: University of Chicago Press, 1996.

[41] Kushilevitz, Eyal and Noam Nisam, Communication complexity. 1st pub. Cambridge: Cambridge University Press, 1997. xiii, 189. ISBN 0-521-56067-5.

[42] D. Lay, Linear Algebra and Its Applications. (1st Ed.) Addison-Wesley, 1997.

[43] F. MacWilliams and N. Sloane, The Theory of Error-Correcting Codes. North-Holland Press, 1977.

[44] D. Markham and B. C. Sanders, “Graph states for quantum secret sharing.” *Phys. Rev. A*, **78**, 042309, 2008.

[45] D. Markham and B. C. Sanders, “Erratum: Graph states for quantum secret sharing.” *Phys. Rev. A*, **83**, 019901(E), 2011.

[46] N.D. Mermin, “Extreme quantum entanglement in a superposition of macroscopically distinct states.” *Phys. Rev. Lett.*, **65**:1838-1840, 1990.

[47] M. Nakahara and T. Ohmi, Quantum Computing: From Linear Algebra to Physical Realizations. Baca Raton, Fl :Taylor & Francis Group, 2008.

[48] A. C. A. Nascimento, P. Tuyls, A. Winter, H. Imai and J. Müller-Quade, “A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes.” *Quantum Information and Computation*, **5**, 1, 205, p. 68-79; e-print quant-ph/0311136, 2003.

[49] M. A. Nielsen and C. M. Caves, “Reversible quantum operations and their application to teleportation.” *Phys. Rev. A*, **55**, pp 2547–2556, 1997; e-print quant-ph/9608001.

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

[51] J. G. Oxley. Matroid Theory. Oxford University Press, New York, 1992.

[52] J. G. Oxley. “What is a Matroid ?” http://www.math.lsu.edu/õxley/survey4.pdf , 2004.

[53] P. K. Sarvepalli and A. Klappenecker. *“Sharing classical secrets with Calderbank-Shor-Steane codes.” Phys. Rev. A*, **80**, 022321, 2009.

[54] P. Sarvepalli and R. Raussendorf. *“Matroids and Quantum Secret Sharing Schemes.” Physical Review A*, **81**, 052333, 2010; e-print: quant-phy/0909.0549v3.

[55] P. Sarvepalli and R. Raussendorf. *“Local Equivalence, Surface-Code States, and Matroids.” Phys. Rev. A*, **82**, 022304, 2010.

[56] J. Preskill, "Quantum Information and computation." Lecture notes for physics 229, California Institute of Technology, 1998.

[57] K. P. T. Rietjens, B. Schoenmakers, and P. T. Tuyls, 2005. "Quantum information theoretical analysis of various constructions for quantum secret sharing." *In Proceedings International Symposium on Information Theory (ISIT 2005, Adelaide, Australia, September 4-9, 2005), pp. 1598-1602. IEEE.*

[58] E. Schr*ö*dinger, "A method of determining quantum-mechanical eigenvalues and eigenfunctions." *Proc. Roy. Irish Acad. (Sect. A)*, **46**, 9, 1940.

[59] A. Shamir, "How to share a secret." *Communications of the ACM*, **22**, 612–613, 1979.

[60] C. E. Shannon. "A mathematical theory of communication." *Bell System Technical Journal*, **27**:379–423, 623–656, 1948.

[61] P. W. Shor "Scheme for reducing decoherence in quantum memory." *Phys. Rev. A*, **52**, pp. 2493-2496, 1195.

[62] A. Smith, "Quantum Secret Sharing for General Access Structures." e-print quantph/ 0001087, 2000.

[63] A. Steane, "Multiple particle interference and quantum error correction." *Proc. Roy. Soc. Lond. A*, **452**, 2551–2577, 1996; e-print quant-ph/9601029.

[64] D. R. Stinson, "An explication of secret sharing schemes." *Designs, Codes and Cryptography*, **2**, pp. 357-390, 1992.

[65] L. Vaidman, L. Goldenberg, and S. Wiesner, "Error prevention scheme with four particles." *Phys. Rev. A*, **54**, pp.1745–1748, 1996; e-print quant-ph/9603031.

[66] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned." *Nature*, **299**, pp.802–803, 1982.

Appendix I

A Presto of Linear Algebra

In this appendix we review some basic facts in linear algebra that are used in the main text. The material follows closely both [42] and [47].

Definition I.1. ***A linear transformation*** *$T : V \rightarrow W$ (where V and W are vector spaces) is a rule that assigns to each vector $\vec{v} \in V$ a unique vector $T(\vec{v})$ in W such that:*

- *(i) $T(\vec{u}+\vec{v}) = T(\vec{u}) + T(\vec{v})$, $\forall\, \vec{u}, \vec{v} \in V$, and*

- *(ii) $T(c\vec{u}) = c\, T(\vec{u}), \quad \forall\, \vec{u} \in V$ and c a scalar.*

Definition I.2. ***The kernel (or null space)*** *of a linear transformation $T : V \rightarrow W$ is the set of all vectors $\vec{u}$ such that $T(\vec{u}) = \vec{0}$, $\vec{0} \in W$.*

Definition I.3. ***The range*** *of a linear transformation $T : V \rightarrow W$ is the set of all vectors $\vec{w} \in W$ of the form $T(\vec{u})$ for some $\vec{u}$ in V.*

We now relate $(n \times n)$-matrices to linear transformations: Consider a linear map $M : \mathbb{C}^n \rightarrow \mathbb{C}^n$ and fix an arbitrary orthonormal basis $\{\hat{e}_k\}$. Let $\vec{v} = \sum_{k=1}^{n} v_k \hat{e}_k$ (i.e. we represent the vector $\vec{v}$ by its local coordinates with each $v_i \in \mathbb{C}$). Linearity of the map M implies that $M\vec{v} = \sum_k v_k\, M\hat{e}_k$. Therefore the action of the map M on an arbitrary vector is well determined provided its action on the basis vectors is given. Since $(M\hat{e}_k) \in \mathbb{C}^n$, we can expand it as

$$M\hat{e}_k = \sum_j \hat{e}_j\, M_{jk}. \tag{I.1}$$

Taking the inner (or *dot*) product between Equation I.1 and $\hat{e}_i$ we get:

$$\hat{e}_i \cdot M\hat{e}_k = \sum_j \underbrace{\hat{e}_i \cdot \hat{e}_j}_{\delta_{ij}}\, M_{jk} = M_{ik}. \tag{I.2}$$

Equation I.2 describes the matrix element of M given an orthonormal basis $\{\hat{e}_k\}$.

Casting the above in terms of Dirac's *bra-ket* notation:

$$M_{ik} = \langle e_i|M|e_k\rangle. \tag{I.3}$$

We thus get:

$$M = \sum_{i,k} M_{ik}|e_i\rangle\langle e_k|, \tag{I.4}$$

which can easily be checked by multiplying M left and right by the *completeness relation* $I = \sum_{i=1}^{n} |e_i\rangle\langle e_i|$ as follow,

$$M = I\ M\ I = \sum_{i,k} |e_i\rangle\langle e_i|M|e_k\rangle\langle e_k| = \sum_{i,k} M_{ik}|e_i\rangle\langle e_k|. \tag{I.5}$$

Definition I.4. *A linear map $M : \mathbb{C}^n \to \mathbb{C}^n$ is called a **linear operator** if*

$$M(c_1|x\rangle + c_2|y\rangle) = c_1 M|x\rangle + c_2 M|y\rangle$$

holds for arbitrary $|x\rangle, |y\rangle \in \mathbb{C}^n$ and $c_i \in \mathbb{C}$.

Definition I.5. *The **rank** of a matrix A is the number of linearly independent columns (or, equivalently, rows) and we write $rank(A)$ to denote it.*

Remark I.6. *If the linear transformation T arises from a matrix transformation say $T(\vec{x}) = A\vec{x}$ for some matrix A and vector $\vec{x} \in V$, then*

$$\ker(T) = Range(T) = Null(A) = Col(A),$$

where $Col(A)$ is the set of the columns of the matrix A.

ℹ $\mathscr{N}.\mathscr{B}.$ In this case, if A is an $(m \times n)$-matrix we also have that

$$Null(A) + rank(A) = n. \tag{I.6}$$

Definition I.7. *Consider a set of vectors* $\{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_p\}$ *in* V*; we write* ***Span***$\{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_p\}$ *for the set of all vectors that can be written as a linear combination of the* $\{\vec{v}_i\}_{i=1}^{p}$.

Definition I.8. *A mapping* $T : \mathbb{R}^n \to \mathbb{R}^m$ *is said to be* ***onto*** $\mathbb{R}^m$ *if each vector* $\vec{b} \in \mathbb{R}^m$ *is the image of at least one* $\vec{x} \in \mathbb{R}^n$ *or equivalently* $\forall\, \vec{b} \in \mathbb{R}^m$ *there exists at least one solution to* $T(\vec{x}) = \vec{b}$.

Definition I.9. T *is said to be* $1:1$ ***(one to one)*** *if for each* $\vec{b} \in \mathbb{R}^m$, $T(\vec{x}) = \vec{b}$ *has either* ***a*** *unique solution* ***or none*** *at all.*

Theorem I.10. (Relation between fundamental subspaces of an $(n \times m)$-matrix A) *Let A be an* $(n \times m)$*-matrix. Then the orthogonal complement of the row space of A is the null-space of A, and the orthogonal complement of the column space of A is the null space of* A^T *(where* A^T *denotes the transpose of A and the row space of A (denoted by* $Row(A)$*) is the set of all rows of the matrix A):*

$$(Row(A))^{\perp} = Null(A) \quad and \quad (Col(A))^{\perp} = Null(A^T). \tag{I.7}$$

This ends our brief exposition and reminder of some of the most pertinent concepts of linear algebra in quantum information theory.