PRINCETON UNIVERSITY

Augmented ((t,n))-threshold Quantum Secret Sharing Schemes

by

Steven Chien

Submitted in partial fulfillment
of the requirements for the degree of
Bachelor of Science in Engineering
Department of Electrical Engineering
Princeton University

Advised by
Mark Zhandry

May 4th, 2020

I hereby declare that this Independent work represents my own work in accordance with University regulations.

Steven Chien

PRINCETON UNIVERSITY

Augmented ((t,n))-threshold Quantum Secret Sharing Schemes

by Steven Chien
Department of Electrical Engineering

Threshold secret sharing schemes are procedures in which groups of a sufficient size can work together to recover a shared secret. In this thesis, we analyze quantum threshold schemes, which are threshold secret sharing schemes applied to quantum information. Many of the restrictions on quantum secret sharing schemes arise from the no-cloning theorem. We investigate the potential benefit of implementing quantum threshold schemes using two or more identical copies of a secret quantum state. This idea is motivated by the possibility that the availability of multiple copies of the secret can circumvent the restrictions imposed by the no-cloning theorem. Our approach takes advantage of the multiple copies by using the union of two or more access structures, one for each quantum state, in order to implement secret sharing schemes that would otherwise not be realizable. We find that we are indeed able to implement a wider range of access structures, but we show that we can only realize one new threshold scheme for every new copy of the share, given a fixed number of players.

Acknowledgements

To my advisor, ***Professor Zhandry****: Thank you for all of your guidance this year. My discussions with you were engaging and thought-provoking, and this thesis would not have been possible without your help;*

To ***Ruth Ochs****: Thank you for always taking the time to check in on me and see how I was doing. That means more to me than I could ever express. Thank you for exposing me to so many different composers and pieces this semester. I looked forward to class and precept with you every week – even the virtual ones! I know that these symphonies will stay a part of me for the rest of my life;*

To ***Vayne****: Thank you for cheering me on during the final stretches of this thesis. Your motivation and energy pushed me through this last week;*

To ***Dora*** *and* ***Aaron****: Thank you for being the best thesis fairies ever! Thank you for your words of encouragement and the delicious snacks. For the past few weeks, I was a machine turning cookies into thesis;*

To ***Jerry****,* ***Alex****,* ***Karen****, and* ***Mary****: Thank you so much for taking the time to read my thesis and help me revise it;*

To PU PERC, and especially my fellow seniors, ***Henry*** *and* ***Reilly****: Thank you for being there since day one. Thank you for four great years of music, for the countries we've explored on tour, and for countless concerts together! Though you will both be on the other coast next year, I know that it will only be a matter of time before we see each other again;*

To ***Clockwork Ultimate****: Thank you for being my family at Princeton. Thank you for giving me a place to learn and grow as a person and as a player. Thank you for the long drives and fun conversations, for the morning practices and team brunches, and of course, for the Party Bus;*

To ***Bill****,* ***Daniel****,* ***Jason****,* ***Jerry****,* ***Jorge****,* ***Pranav****, and* ***Yang****: Thank you for accompanying me through my Princeton journey, and for the many laughs along the way. Our weekly Zoom calls during these more isolated times have lifted my spirits and made everything so much more bearable;*

To one of my closest friends, ***Jess****: Thank you for being the best car lab, final project, and COS assignment (I'm probably forgetting a few) partner I could ever ask for. Not sure if I should thank you for declaring ELE with me because look at what we had to do;*

To my classmates and my friends in the department, ***Abby****,* ***Alex****,* ***Clare****,* ***Kevin****, and* ***Trisha****: Thank you for making our ELE classes a pleasure to attend. Thank you for all of the late nights spent together on psets and for the countless hours together in the lab;*

To my family, ***Mom****,* ***Dad****, and* ***Mei Mei****: Thank you for all of the home-cooked meals, sliced fruit, and tasty desserts. Thank you for your love and support, but most importantly, thank you for not being too loud when I was working on this thesis.*

Contents

Symbols and Abbreviations

$\|\Psi\rangle$	quantum state
ρ	density operator or density matrix
U	unitary operator
$\mathrm{tr}\,(\rho)$	trace
$\mathrm{tr}_Y\,(\rho)$	partial trace over Y
$S(\rho)$	von Neumann entropy
$S(X,Y)$	joint entropy
$S(X\|Y)$	conditional entropy
$I(X:Y)$	mutual information
G	graph
G^c	complement of graph
$K(a,b)$	Kneser graph
K_n	complete graph on n vertices
$\chi(G)$	chromatic number of G
$\theta(G)$	clique cover number of G
$\mathcal{D}$	dealer
$\mathcal{S}$	secret
$\mathcal{P}$	players
Γ	access structure
(t,n)	t-out-of-n threshold scheme
$((t,n))$	quantum t-out-of-n threshold scheme
GHZ	Greenberger-Horne-Zeilinger
QEC	Quantum Error Correction
QSS	Quantum Secret Sharing
QTS	Quantum Threshold Scheme

Chapter 1

Introduction

"If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em."
– Jennifer and Peter Shor

Quantum computing is an exciting and active field of research. Much of the work being done today deals with the implementation of quantum information and quantum hardware. However, the ability to use quantum computers to store and manipulate information demands secure encryption schemes and robust error correction. This has motivated an expansive amount of literature in the fields of quantum cryptography and quantum error correction (QEC).

Research in quantum cryptography advances with two main goals. The first is to provide quantum implementations of useful classical cryptographic procedures. This is important if we are to ever use quantum computers to manipulate, store, and transfer sensitive data. The second is to develop schemes that are secure not only against classical computers, but also against quantum computers. One concern is that quantum computers will enable us to break certain classical encryption schemes, and to an extent, this is true. A popular example of a potentially insecure encryption scheme is RSA, whose security depends on the computational complexity of factoring large numbers. The vulnerability comes from the existence of an efficient *quantum* algorithm for factoring integers, invented by Peter Shor [1].

Error correction is something that we take for granted in today's computers. However, it poses a particularly difficult problem in quantum computers. One difficulty is that the

physical implementation of quantum information is relatively fragile, and is susceptible to effects like decoherence from external systems. One of the main challenges is a consequence of the *no-cloning theorem*, which states that we cannot make a copy, or a clone, of an unknown quantum state. Many error correcting schemes in classical computers rely on the ability to copy information, using the extra copies to create redundancy. These obstacles might suggest that error correcting in quantum computers is doomed to fail; surprisingly, this is not the case.

An important cryptographic procedure related to error correction is called secret sharing. The goal of secret sharing is to take sensitive data (the secret) and distribute it among a set of participants in such a way that requires sufficiently large subsets of those participants to work together in order to reconstruct the secret. There are many situations in which these schemes are useful. These situations are often characterized by: information that is too sensitive for just one person to have access; mutual distrust, yet a need to cooperate among members of a group; or the need to distribute power among multiple people. Example applications include giving a group of bank executives access to a vault, requiring multiple officials to launch nuclear warheads, or creating secure voting procedures for a board of directors. For these reasons, developing secure and efficient methods of sharing quantum secrets is an important task.

When applied to quantum information, these cryptographic procedures are known as *quantum secret sharing* (QSS), and they are a well-studied field in quantum cryptography. In 1999, Hillery, Bužek, and Berthiaume are credited with presenting one of the first schemes that involves using Greenberger-Horne-Zeilinger (GHZ) states to split quantum information into two parts such that both are necessary to recover the original information [2]. Gottesman, Cleve, and Lo use quantum error correcting codes to implement both threshold schemes and schemes with general access structures [3]. Smith presents a construction for general access structures using monotone span programs [4]. Later, Gottesman proves several important theorems, including one that gives us necessary and sufficient conditions on the structure of quantum secret sharing schemes [5].

Quantum error correction and quantum secret sharing go hand in hand. In essence, the goal of quantum error correction is to encode information in a way that allows the reconstruction of the original information in the absence of some part of the encoding. Quantum secret sharing has precisely the same goal with a few added constraints. And so, we are not so surprised that the main limitation of quantum secret sharing is also a result of the *no-cloning theorem*. The primary goal of this thesis is to explore ideas that can circumvent this limitation.

This is not a new idea. In 2004, Singh and Srikanth approached the problem by keeping a certain number of quantum shares with the dealer during the secret sharing procedure.

They show that they are able to completely remove the restriction imposed by the no-cloning theorem [6]. However, we have slight reservations with their approach, which are explained in Chapter 4.

In this thesis, we present a different approach to loosening the restriction of the no-cloning theorem. We explore quantum secret sharing schemes that use more than one copy of a quantum state, and use a graph theoretical approach to characterize the class of schemes that become possible to implement. Specifically, we find that any quantum threshold scheme of the form $((t, 2t - 2 + k, k))$ is valid under our construction; on the other hand, any scheme of the form $((t, 2t - 1 + k, k))$ is not valid.

In Chapter 2, we present relevant background in quantum computation and quantum information. After that, in chapter 3, we bring in some definitions and results from graph theory. In Chapter 4, we present definitions and results related to classical and quantum secret sharing schemes. We introduce our approach to circumventing the no-cloning theorem using multiple copies of the quantum secret and show some preliminary results in chapter 5. In Chapter 6, we prove more general claims about our scheme, and present our main findings. It is here that we we give a short corollary that provides a closed-form solution for the minimum number of shares that must reside with the dealer in Singh and Srikanth's *Assisted Quantum Threshold Scheme*. In the final chapter, we discuss the implications of our findings and explore future work.

Chapter 2

Quantum Computation and Quantum Information

2.1 Quantum Computation

Before we talk about quantum cryptography, it is important to cover a few important concepts in quantum computation. This section will give a mathematical description of quantum systems and discuss some of their important properties. Much of this section comes from Nielsen and Chuang's book on quantum computation and quantum information. For a more comprehensive treatment, please refer to their text [7].

2.1.1 Quantum States

An isolated **quantum system** is associated with a **Hilbert space** $\mathcal{H}$. The system is described completely by its **state vector**, which is a unit vector in the **state space** $\mathcal{H}$.

The simplest, but most applicable quantum mechanical system that we will use is the **qubit**, or the "quantum bit". The qubit lies in a two-dimensional Hilbert space, and is denoted as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

where $|\alpha|^2 + |\beta|^2 = 1$. The normalization of the constant terms ensure that $|\psi\rangle$ is a unit vector. $|0\rangle$ and $|1\rangle$ form an orthonormal basis for the two-dimensional hilbert space. A

general state vector in an n dimensional Hilbert space is denoted:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle \tag{2.2}$$

The states $|i\rangle$ for $i \in \{1, ..., n\}$ represent an orthonormal basis, and the constants $\alpha_1, ..., \alpha_n$ are complex numbers normalized such that $\sum_{i=1}^{n} \alpha_i = 1$.

We say that the quantum state $|\psi\rangle$ is in a **superposition** of the states: $\{|i\rangle\}$.

The above formulation is called a state vector. Another formulation that represents a quantum state is a **density operator** or **density matrix**, generally denoted as ρ. One application where the density operator shines is in describing **mixed states**. A mixed state describes a quantum system in which there is uncertainty about its exact state. These are also known as ensembles of pure states: $\{|\psi_i\rangle, p_i\}$. $|\psi_i\rangle$ is one of the possible states the system is in, and the corresponding probability that the system is in state $|\psi_i\rangle$ is p_i. Then, the density operator describing this quantum subsystem is:

$$\rho = \sum_{i} p_i * |\psi_i\rangle \langle\psi_i| \tag{2.3}$$

Note that a mixed state is different than a superposition of states. A mixed state has to do with uncertainty about which state a quantum system is in. However, if a system is known to be in a superposition state, then there is no uncertainty. That state would be a pure state.

One of the most important applications of the density operator is the ability to describe quantum subsystems. Say that we have a density operator ρ that represents the composite of two quantum systems X and Y. Then, the density operator representing just the quantum system X is:

$$\rho^X \equiv \mathrm{tr}_Y(\rho) \tag{2.4}$$

This is known as the (partial trace) over system Y, and the resulting ρ^X is known as the **reduced density operator**. Note that if we perform a partial trace over subsystem Y, then we obtain the reduced density operator describing the subsystem X. The importance of the reduced density operator comes from the fact that it returns the correct measurements statistics for measurements done on subsystem X.

Another important technique that takes advantage of the density operator formulation is **purification**. This is a procedure in which we begin with some quantum system A which is in a mixed state. We introduce a "reference" system R such that the composite

system AR is in a pure state, and $|AR\rangle$ reduces to ρ^A when we trace over the reference system R. It is always possible to do this.

It is important to note that both the state vector and density operator formulations are equally valid ways of describing a quantum system. Now, having talked about mathematical descriptions of quantum systems, it is only natural to then consider how we can manipulate those systems.

2.1.2 Quantum Operations

The evolution of a quantum system can be described using **quantum operations**. A quantum operation is a unitary operator U that acts on a quantum system denoted $|\psi\rangle$.

Definition 2.1. Unitary Operator. A **unitary operator** $U; \mathcal{H} \to \mathcal{H}$ is a linear operator on a Hilbert space $\mathcal{H}$ that satisfies:

$$U^\dagger U = UU^\dagger = I \tag{2.5}$$

where $U^\dagger$ is the adjoint of U.

Any unitary matrix U describes a valid quantum operation that can be used to evolve a quantum system. This specific constraint comes from the requirement that quantum operations be reversible. We know that any unitary matrix U is reversible because if we apply U to a quantum state $|\psi\rangle$, and then apply $U^\dagger$ to the evolved state $U|\psi\rangle$, we get $U^\dagger U|\psi\rangle = |\psi\rangle$.

Examples of some commonly used operators are the 4 Pauli operators:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.6}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.7}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.8}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.9}$$

If the evolution of a closed quantum system is described by the unitary operator U, and the system was originally in the state $|\psi\rangle$, then we denote the evolved system as:

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \tag{2.10}$$

Using the density operator formulation, let ρ describe the ensemble of states where the closed quantum system was originally in state $|\psi_i\rangle$ with probability, p_i, the evolution is described as:

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \xrightarrow{U} \sum_i p_i U |\psi_i\rangle \langle\psi_i| U^\dagger \tag{2.11}$$

$$\xrightarrow{U} U \left(\sum_i p_i |\psi_i\rangle \langle\psi_i| \right) U^\dagger \tag{2.12}$$

$$\xrightarrow{U} U \rho U^\dagger \tag{2.13}$$

2.1.3 Entanglement

So far, our discussion has focused on quantum systems describing just a single qubit. In general, we can extend this description to systems that contain multiple qubits. Let a system X correspond to a qubit in the state $|\psi\rangle$, and a system Y correspond to a qubit in the state $|\phi\rangle$. Then, we say that XY denotes a **composite system**, which, in this case, is a system containing both X and Y. These systems can interact in a number of ways. One of these ways is for X and Y to remain independent and uncorrelated. Then, the mathematical representation of XY is:

$$|\psi\rangle \otimes |\phi\rangle \tag{2.14}$$

This is also called a **product state**, and it means that the composite system XY can be decomposed into smaller parts via a tensor product. We can treat these smaller systems as if they are independent of one another.

The more interesting way that two quantum systems can interact with each other is called **quantum entanglement**. This is a fascinating and unique phenomenon in quantum mechanics, and is often considered a hallmark of the field. Consider the state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

This state is one of four states that form the "Bell basis", which was named after John S. Bell for his famous 1964 paper [8]. The state describes a system of two qubits, where the individual states of each qubit cannot be separated with a tensor product. What is even more interesting is that the two qubits are anti-correlated. By performing a measurement on one of the two qubits, you can know, with certainty, the state of the other qubit, even if the two qubits are separated over a large distance.

Quantum entanglement is one of the main features of quantum computation that allows for the development of novel algorithms and novel cryptographic procedures. It is used in many quantum computing algorithms and is at the heart of almost every quantum secret sharing scheme, which we will talk about more in later chapters.

2.2 The No-Cloning Theorem

One of the most important theorems in quantum computing is the **no-cloning theorem**. Here, we present the theorem with proof referencing Mermin's 2007 text [9].

No-Cloning Theorem. *Given an unknown, arbitrary quantum state ψ, there is no valid operator U that can create an identical copy of this state. More formally there exists no operator such that $U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle$.*

Proof. Assume for the sake of contradiction that there is such an operator. Then $U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle$ and $U(|\phi\rangle |0\rangle) = |\phi\rangle |\phi\rangle$, for arbitrary quantum states $|\psi\rangle, |\phi\rangle$. Then:

$$U(\alpha |\psi\rangle + \beta |\phi\rangle) \otimes |0\rangle = (\alpha |\psi\rangle + \beta |\phi\rangle) \otimes (\alpha |\psi\rangle + \beta |\phi\rangle) \tag{2.15}$$

$$= \alpha^2 \langle\phi|\phi\rangle + \beta^2 \langle\psi|\psi\rangle + \alpha\beta \langle\phi|\psi\rangle + \alpha\beta \langle\psi|\phi\rangle \tag{2.16}$$

But by linearity, we also have:

$$U(\alpha |\psi\rangle + \beta |\phi\rangle) \otimes |0\rangle = \alpha U |\psi\rangle |0\rangle + \beta U |\phi\rangle |0\rangle \tag{2.17}$$

$$= \alpha |\psi\rangle |\psi\rangle + \beta |\phi\rangle |\phi\rangle \tag{2.18}$$

Equation 2.16 and Equation 2.18 can only be the same if one of α or β is equal to 0, which contradicts the assumption that $|\psi\rangle, |\phi\rangle$ are arbitrary. □

Remark. Note that the theorem statement can also be made replacing $|0\rangle$ with an arbitrary state $|e\rangle$. What is important is that there is no unitary operator that acts as a "general purpose copier". For example, it would be easy to create an operator that can copy a state $|\phi\rangle$ if we know for a fact that the state is either $|0\rangle$ or $|1\rangle$ [9]. In general, a cloning device can only clone states which are orthogonal to each other [7].

2.3 Quantum Information Theory

When designing cryptographic schemes, it is important to work with quantitative definitions of information. This allows us to rigorously prove claims about the security of our procedures. An important concept in classical information theory is **entropy**. Entropy can be thought of as the amount of uncertainty associated with the value of a quantity. In classical information theory, entropy is defined over probability distributions. These give us the probabilities that a quantity, like a random variable, takes on certain values. Classical information theory uses a measure of entropy called **Shannon entropy**:

Definition 2.2. Shannon Entropy. The **Shannon entropy** of a probability distribution is defined as:

$$H(X) \equiv \sum_x p_x \log(p_x) \tag{2.19}$$

This idea is transferable to quantum information. Quantum systems can be modelled as probability distributions, where the "values" that the system can take on are quantum states, and their associated probabilities are encoded in the density operator that represents the system. The quantum analogue of Shannon entropy is called **von Neumann entropy**, and is defined below:

Definition 2.3. von Neumann Entropy. The **von Neumann entropy** of a quantum system ρ is defined as:

$$S(\rho) \equiv -\text{tr}\left(\rho \log(\rho)\right) \tag{2.20}$$

where tr (ρ) is the **trace** over ρ. The von Neumann entropy has an alternative definition using the eigenvalues of ρ:

$$S(\rho) = -\sum_x \lambda_x \log(\lambda_x) \tag{2.21}$$

Remark. The von Neumann entropy $S(\rho)$ is non-negative.

Because entropy is a measure of uncertainty, the von Neumann entropy of a pure state, where there is no uncertainty about the state of the system, is 0. On the other hand, the maximum entropy that a quantum system can have is when it is in a **maximally mixed state**, just as we would expect the Shannon entropy to be maximized over a uniform distribution. If a quantum system is in one of d possible pure states, each with equal probability, then we say that it is in a maximally mixed state. The density operator for

this system is:

$$\rho = \sum_{i=0}^{d-1} \frac{1}{d} |i\rangle \langle i| = \frac{1}{d} I \tag{2.22}$$

And the von Neumann entropy of the maximally mixed state:

$$S(\rho) = S(\tfrac{1}{d} I) = \log(d) \tag{2.23}$$

In quantum mechanics, we often work with two more quantum systems that interact with each other. An important entropy-like definition involving two or more systems is called the **relative entropy**, which measures the closeness of two probability distributions. In the case of quantum information, it measures the closeness of two quantum systems. We define quantum relative entropy below:

Definition 2.4. Quantum Relative Entropy. Suppose there are two density operators ρ and σ. The **relative entropy** of ρ to σ is:

$$S(\rho||\sigma) \equiv \text{tr}\left(\rho \log(\rho)\right) - \text{tr}\left(\rho \log(\sigma)\right) \tag{2.24}$$

Remark. The relative von Neumann entropy of ρ to σ $S(\rho||\sigma)$ is non-negative.

Another definition related to the interaction between systems is the **joint entropy**. Consider two quantum systems X and Y. We denote the composite system of them to be XY, and their density operator to be ρ^{XY}.

Definition 2.5. Joint Entropy. The **joint entropy** of a composite system XY is simply the entropy defined on the density operator of the composite system:

$$S(X, Y) = S(\rho^{XY}) = -\text{tr}\left(\rho^{XY} \log(\rho^{XY})\right) \tag{2.25}$$

As one might expect, the joint entropy can also be defined as function of the entropies of each system separately. To talk about that, we need to provide a couple more important definitions.

Definition 2.6. Conditional Entropy. Say that we have two quantum systems X, Y, but we have full information about Y. Then we define the entropy of X **conditional** on knowing Y to be:

$$S(X|Y) \equiv S(X, Y) - S(Y) \tag{2.26}$$

Example 2.1. If we have a composite system XY in a product state, that is, the state of the system can be written as $\rho \otimes \sigma$, then the joint entropy is:

$$S(X, Y) = S(X) + S(Y) \tag{2.27}$$

This implies that the conditional entropy $S(X|Y) = S(X)$, which makes sense. If a composite system is in a product state, then there is no entanglement between the two systems. Information about one system does not give any information about the other.

In cases where there is entanglement, we can reach some interesting results. Again, consider the composite system XY of X and Y, and this time assume that XY is in a pure entangled state. The entropy of XY is actually *smaller* than the entropy of either X or Y alone. Moreover, by Definition 2.6, the conditional entropy $S(X|Y)$ is actually negative. This seems incorrect – how could a larger system possibly have less uncertainty than one of its subsystems, and what does negative conditional entropy even mean? The short answer is that knowledge of one system can give complete information about another system, like we saw for the Bell state in Subsection 2.1.3. This is just one of the many counterintuitive results that come from quantum entanglement.

Another quantity that relates to the information content of two systems is the **mutual information**. This is a measure of how much information the two systems have in common.

Definition 2.7. Mutual Information. The **mutual information** of two quantum systems X, Y is defined as:

$$I(X : Y) \equiv S(X) + S(Y) - S(X, Y) \tag{2.28}$$

Using our definitions, one can see that the mutual information is also closely tied to the conditional entropy:

$$I(X : Y) = S(X) - S(X|Y) = S(Y) - S(Y|X) \tag{2.29}$$

Chapter 3

Graphs

Access structures lend themselves naturally to graphical representations. Here, we show a few basic definitions and results from graph theory, as they will become useful in our discussion.

Definition 3.1. Graph. A **graph** $G = (V, E)$ is composed of a set of vertices and a set of edges. Each edge is incident to two vertices.

We say that two vertices are **adjacent** if they are incident to the same edge.

Definition 3.2. Vertex Induced Subgraph. A **vertex-induced subgraph** of $G = (V, E)$ by the vertex set V' is the graph G' with vertex set V' and edge set consisting those edges with both endpoints in V'. This is also called an *induced subgraph.*

Definition 3.3. Complement. The **complement** of a graph $G = (V, E)$ is the graph $G^c = (V, E^c)$. There is an edge between two vertices $u, v \in V$ in G^c if u and v are not adjacent in G.

Definition 3.4. Stable Set. A **stable set** in a graph $G = (V, E)$ is a subset of vertices $V_s \subseteq V$ where there are no edges $e \in E$ that have both endpoints in V_s.

Definition 3.5. Bipartite Graph. A **bipartite graph** is a graph in which the vertices can be separated into two stable sets.

Bipartite graphs are an important class of graphs because of their wide applicability, and because of their relatively simple structure, there exist numerous results regarding them. One elementary result provides both a necessary and sufficient condition for bipartite graphs.

Theorem. *A graph is bipartite if and only if it does not contain any odd cycles.*

Definition 3.6. Complete Graph. A **complete graph** is a graph where each vertex is adjacent to every other vertex. A complete graph with n nodes is often denoted as K_n.

If a vertex-induced subgraph is a complete graph, then we call that induced subgraph a **clique**.

Remark. Any induced subgraph of a complete graph is a clique.

Definition 3.7. Chromatic Number. A vertex coloring of a graph G assigns each vertex in V a color such that two vertices of the same color are not adjacent. The **chromatic number** of a graph $\chi(G)$ is the minimum number of colors needed to do a vertex coloring on G.

Remark. The chromatic number of K_n is n. The chromatic number of a bipartite graph is 2.

Definition 3.8. Clique Cover Number. The **clique cover number** is the minimum number of cliques needed to cover the vertex set V of G.

Proposition 3.1. *The clique cover number of a graph G is equal to the chromatic number of the complement of the graph G^c:*

$$\theta(G) = \chi(G^c) \tag{3.1}$$

Proof. Each clique in G is a stable set in G^c. In a vertex coloring of G, vertices that form a stable set can all be the same color. Therefore if you find a partition of the vertices in a graph such that each subset of vertices is a stable set, the minimum cardinality of that partition is the same as its chromatic number. □

The following definition will be useful in our analysis in later chapters.

Definition 3.9. Kneser Graph. A **Kneser Graph**, denoted $K(a, b)$, is a graph with the set of all b-subsets of a as the vertex set. There is an edge between two vertices if the subsets that they represent are disjoint. This graph has $\binom{a}{b}$ vertices.

This class of graphs was introduced by Lovaśz in 1978 [10], which he used to prove Kneser's Conjecture, originally posed by Martin Kneser in 1955.

Kneser's Conjecture. *Whenever the t-subsets of a $(2t + j)$-set are divided into $j + 1$ classes, then two disjoint subsets end up in the same class.*

The above conjecture, which has now been proven, is stated as a set theoretical result, and is equivalent to the following result on Kneser graphs:

Corollary 3.2. *Let $k = j + 1$. $K(2t - 1 + k, t)$* ***is not*** *k-colorable.*

Proof. This result follows directly from the definition of a Kneser Graph. A $K(2t - 1 + k, t)$ has a vertex for every t-subset of $2t - 1 + k$. There is an edge between two vertices if they are disjoint. Consider a minimum vertex coloring on this graph. If two vertices represent disjoint sets, then they must be adjacent. So in the vertex coloring, they cannot be the same color. Kneser's Conjecture states that if we attempt to split the vertices of the graph into k separate groups, then there must be at least one pair of adjacent vertices that end up in the same group. Therefore, a k-coloring cannot exist for this graph, so $K(2t - 1 + k, t)$ is not k-colorable. □

Chapter 4

Secret Sharing

In this chapter we will describe secret sharing schemes and talk about some of their properties and definitions. Then, we will extend our discussion to quantum secret sharing schemes, and present some preliminary definitions and results.

4.1 Classical Secret Sharing

A secret sharing scheme allows some **secret** $\mathcal{S}$ to be divided into **shares** and distributed by some **dealer** $\mathcal{D}$ to a set of **participants** or **players** $\mathcal{P}$. Each secret sharing scheme has a corresponding **access structure** denoted by Γ. Γ defines the set of **authorized subsets** of $\mathcal{P}$ that have access to the secret. A subset of participants $A \in \Gamma$ should be able to reconstruct the original secret in its entirety, but a a set $B \notin \Gamma$ should have **no information** about the secret, in the sense that all possible values of the secret are equally likely. It is this final condition that makes implementing secret sharing schemes more difficult and interesting than just, say, taking a string and dividing it into equal chunks and giving one chunk to each person. Let us present some more formalized definitions:

Definition 4.1. Access Structure. An **access structure** is often denoted as Γ. An access structure specifies the set of all authorized subsets of players that are able to recover the secret.

Definition 4.2. Authorized Set. An **authorized set** is a subset $A \subseteq \mathcal{P}$ such that $A \in \Gamma$ for an access structure Γ. The participants in an authorized set A have the ability to access the secret together.

Definition 4.3. Monotone Access Structure. An access structure Γ is **monotone** if $B \in \Gamma$ and $B \subseteq C$ implies $C \in \Gamma$.

Definition 4.3 is particularly useful to us. Essentially, if some subset of participants is in the access structure, then all supersets of that subset should also be in the access structure. For the task of secret sharing, this definition is intuitive, if not necessary. Indeed, it would be difficult to conceive of a secret sharing procedure that implements an access structure that is *not* monotone. Later on, we will see that the property of monotonicity is not only necessary for the realizability of quantum access structures, but it is also one of two sufficient conditions.

Definition 4.4. Minimal Access Structure. An access structure Γ is **minimal** if $A \in \Gamma$ implies for every $A' \in \Gamma \setminus \{A\}$, $A' \not\subset A$. Another name for this is an access structure's **basis**.

Definition 4.5. Minimal Authorized Set. A **minimal authorized set** is simply one of the authorized sets in the minimal access structure.

Observe that any monotone access structure has a **unique minimal access structure**. If we assume that all of the access structures we are talking about are monotone, then this gives us a much simpler way to analyze access structures.

Example 4.1. Let $\mathcal{P} = \{A, B, C, D\}$. Let $\Gamma_1 = \{(A, B), (A, C), (A, D)\}$. Let $\Gamma_2 = \{(A, B), (A, C), (A, D), (A, B, C)\}$. Assuming both access structures are monotone, then Γ_1 and Γ_2 represent the same access structure, because $(A, C) \subset (A, B, C)$. However, Γ_1 is a minimal access structure, and in fact, it is the **unique** minimal access structure of Γ_2. We say that Γ_1 and Γ_2 each have 3 minimal authorized sets.

In a way, we can think of the minimal authorized sets as the "smallest common denominators" which make up an access structure. We do not need to include an authorized set (A, B, C) because it is implied to be authorized if (A, B) is already a part of the access structure.

Definition 4.6. Threshold Scheme. A (t, n)**-threshold secret sharing scheme**, or just "threshold scheme" is a secret sharing scheme among n players such that at least t of those players must combine their respective shares in order to access the secret. The access structure for this scheme is composed of every subset of $\mathcal{P}$ of size t. This is also referred to as the set of all t-subsets of n.

For our (t, n) threshold scheme defined above, the *access structure* can be defined more formally as such: $\Gamma = \{A | A \subseteq \mathcal{P}, |A| = t\}$.

Example 4.2. Take the set of participants $\mathcal{P} = \{p_1, p_2, p_3\}$. Let $\Gamma = \{p_1p_2, p_2p_3, p_3p_1\}$. This access structure describes a $(2, 3)$-threshold scheme. At least 2 out of the 3 players are needed to reconstruct the secret.

As we mentioned above, Shamir developed one of the first implementations for a perfect threshold scheme based on polynomial interpolation [11]. A perfect secret sharing scheme is defined as one where authorized subsets have access to the secret, and unauthorized subsets have no information at all, in an information theoretical sense, of the secret. Despite their shares, all possible values of the secret are possible.

Shamir's scheme is a (t, n)-threshold scheme. The scheme works as so. First, encode the secret as a number such that the secret is retrievable in its original form. Then, randomly generate a $(t-1)$th-degree polynomial such that the constant term is the number encoding the secret. For each of the n players, generate and distribute one of the pairs $(i, p(i))$, where $i \in [1, \cdots, n]$. Each pair of numbers acts as a player's share of the secret. If t or more players work together and pool their shares, they can reconstruct the unique $(t-1)$th-degree polynomial p that generated those pairs, and then $p(0)$ reveals the secret. Having only $t-1$ or fewer pairs gives no information about the secret, because there would be infinitely many polynomials of degree $t-1$ passing through those $t-1$ or fewer pairs, and all values of the secret would be equally likely.

4.2 Quantum Secret Sharing

A quantum secret sharing scheme is the quantum analogue of a classical secret sharing scheme in the sense that the information to be shared is quantum. This idea was first introduced by Hillery et al. in 1999 [2]. In their paper, they give an example of a $((2, 3))$-threshold quantum secret sharing scheme implemented using Greenberger-Horne-Zeilinger (GHZ) states. This was then extended by the work of Cleve, Gottesman, and Lo [3]. They introduce the idea of a quantum access structure, and propose implementations for general quantum secret sharing schemes. We start off by extending some definitions from the previous section.

Definition 4.7. Quantum Threshold Scheme. A $((t, n))$-quantum threshold scheme (QTS) is a (t, n)-threshold secret sharing scheme applied to a quantum secret. We use double parentheses to illustrate that the scheme is quantum. The quantum secret is denoted $|\psi\rangle$. As in the classical case, we take a quantum secret and divide it into n shares to distribute among a set of participants. We require at least t of those participants to combine their shares in order to recover the quantum state $|\psi\rangle$.

As with classical secret sharing, a QTS is a specific class of a quantum secret sharing schemes – one with a particular access structure. All of the other definitions from

classical secret sharing are applicable in the quantum case. However, additional restrictions apply to quantum secret sharing schemes that do not apply to their classical counterparts.

Theorem 4.1. *A QSS scheme exists for a general access structure* Γ *only if for every* $A_1, A_2 \in \Gamma$, $A_1 \cap A_2 \neq \emptyset$.

Proof. Let us assume, for the sake of contradiction, that there exists a scheme where two disjoint subsets of players can each recover the secret quantum state. Then, we would have the possibility of two disjoint groups each obtaining their own copy of the secret. In a sense, this creates a way to copy a general quantum state. This is not possible because it violates the no-cloning theorem, so this scheme could not exist. □

Corollary 4.2. *A QTS* $((t, n))$ *is valid only if* $t > \frac{n}{2}$.

Proof. This is a direct result of Theorem 4.1. If $t \leq \frac{n}{2}$, then there would exist at least two authorized subsets that are disjoint. □

Note that this theorem presents only a necessary condition for the existence of a QTS, not a sufficient one. However, we can indeed prove stronger claims. In 2000, Gottesman showed that a quantum secret sharing scheme exists for an access structure Γ as long as Γ is monotone and Theorem 4.1 is satisfied [5]:

Theorem 4.3. *A quantum secret sharing scheme exists for an access structure iff the access structure is monotone and the no-cloning theorem is not violated.*

In later discussion, we are going to call any QSS scheme that satisfies the conditions of Theorem 4.3 valid. As we can see, the no-cloning theorem imposes our most strict limitation on the existence of QSS schemes, and this can pose practical limitations to implementing secret sharing schemes in quantum computing. To see why, consider a valid access structure that satisfies the no-cloning theorem. In such an access structure, each authorized set must intersect **every** other authorized set. Or in other terms, each pair of authorized sets must have at least one player in common. This is a somewhat unnatural constraint to impose on an access structure, and can limit the usefulness of the procedure.

4.3 A Quantum Information Theoretical Model for Quantum Secret Sharing

When discussing quantum cryptography, quantum information theory can be a very important tool. It will allow us to provide a precise definition for quantum secret sharing and make rigorous claims. Relative to the amount of literature on these schemes, previous work on a quantum information theoretical approach to QSS is rather limited.

Imai et al. were one of the first to propose an information theoretical model for quantum secret sharing [12]. Later, Rietjens applies this definition in the analysis of a number of different quantum secret sharing implementations [13]. More recently, Bai et al. generalize Imai's initial definition so that it can apply to more quantum secret sharing schemes. However, this comes at the cost of schemes that are potentially less secure. First, we present the definition from [12]:

Let S be the quantum system of the secret. The system S can take on the possible states: $\{|\psi_i\rangle\}$ each with probability p_i. The density operator representing the secret is then:

$$\rho_s = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \tag{4.1}$$

Then $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ is the set of players, where we will take P_i to represent both the i-th player **and** the shares in possession of P_i, for notational simplicity. Similarly, $A \subseteq \mathcal{P}$ will both represent a subset of the players $\mathcal{P}$ and also the set of shares in the possession of that subset of players. We let R be a reference system such that the composite system RS is in a pure state.

A quantum secret sharing scheme is a **completely positive map** Λ (maps positive elements to positive elements) such that:

$$\Lambda_D : S(\mathcal{H}_\mathcal{S}) \to S(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n) \tag{4.2}$$

Where $\mathcal{H}_i$ is the Hilbert space containing the shares of player i, and $S(\mathcal{H}_A)$ is the state space of quantum system A. After the operation, the state $|RS\rangle$ becomes $|RP_1P_2 \ldots P_n\rangle$.

Definition 4.8. Perfect Quantum Secret Sharing Scheme. A **perfect quantum secret sharing scheme** is one that satisfies the following conditions:

1. Recoverability requirement: For all $A \in \Gamma$, there exists a recovery map $T_A : \mathcal{H}_A \to \mathcal{H}_S$ such that

$$\rho^{RA} \to |RS\rangle \tag{4.3}$$

$$I(R : A) = I(R : S) \tag{4.4}$$

2. Secrecy requirement: For all $B \notin \Gamma$ we have that:

$$I(R : B) = 0 \tag{4.5}$$

Intuitively, this means that the quantum system of the shares in the possession of any authorized set should have the same information content as the quantum system of the secret, and the quantum system of any unauthorized set has no information at all about the secret.

We make sure to indicate that this scheme is *perfect*, because it is also possible to create schemes that are imperfect. Bai et al. refer to this as a **generalized information theoretical model**, meaning unauthorized sets do have some amount of information about the secret. Using similar notation, the above formulation, $I(R : B) < I(R : S)$, but $I(R : B) \neq 0$ [14]. Naturally, relaxing this constraint increases the number of schemes that satisfy the definition. For the purposes of our thesis, we will stick with the stricter definition proposed by Imai.

The following theorem characterizes schemes that are known to be perfect. This will help us later in analyzing the security of our implementation.

Theorem 4.4. *A quantum secret sharing scheme in which the unauthorized sets are exactly the complements of the authorized sets is perfect. Specifically, this is a scheme where:*

$$A \in \Gamma \to A^c \notin \Gamma \tag{4.6}$$

$$B \notin \Gamma \to B^c \in \Gamma \tag{4.7}$$

Gottesman presented the first proof for this, and referred to access structures of this form as **maximal** access structures [5]. This name comes from the fact we cannot add anymore sets into a maximal access structure Γ without violating the no-cloning theorem. Suppose that we did try to add a set into Γ. Then by the definition of maximal, we must have added a set to Γ whose complement was already in Γ. This violates the no-cloning theorem.

Remark. An access structure can be both minimal and maximal at the same time.

4.4 Circumventing the No-Cloning Theorem

4.4.1 Assisted Quantum Secret Sharing

Theorem 4.3 shows us that the no-cloning theorem imposes the strictest bounds on the number of realizable quantum secret sharing schemes. In their paper, Singh and Srikanth introduce a new scheme called the **assisted quantum secret sharing scheme** [6].

Definition 4.9. Assisted Quantum Secret Sharing Scheme. This is a quantum secret sharing procedure which involves the dealer in reconstruction. The dealer retains several shares in its own possession, called *resident shares*. All other shares are called *player shares*.

What is significant here is that the dealer must be trustworthy, and reconstruction of the secret must be done by the dealer. Singh and Srikanth introduce a graphical representation of the access structure to aid in their discussion. They call this graph an *access structure graph* (AS graph), which we define formally below:

Definition 4.10. Access Structure Graph. An **access structure graph** (or AS graph) is a graph $G = (V, E)$ where $V = \Gamma$ and $E = \{(A_i \cap A_j \neq \emptyset) \forall\, i, j, i \neq j\}$.

Each authorized set in the access structure corresponds to a vertex in the graph, and there are edges between two vertices if their authorized sets intersect. This graph is useful because we can draw connections between properties of the graph and properties of the access structure, like the one here:

Proposition 4.5. *Let* $\Gamma = \{A_1, A_2, \ldots, A_r\}$ *be the access structure.* Γ *satisfies the no-cloning theorem iff its AS graph is a complete graph [6].*

Proof. By Theorem 4.1, we know that each pair of authorized subsets must have a nonempty intersection. Each of these intersections correspond to an edge in the AS graph, so there must be an edge between every pair of vertices.

If Γ does not satisfy the no-cloning theorem, then we know that there must be at least one pair of authorized sets that do not intersect each other. These corresponding vertices in the AS graph are non-adjacent. □

If the access structure Γ does not satisfy the no-cloning theorem, we know that its AS graph is not a complete graph. However, we can still use its AS graph to our advantage. We use the graph to find a clique covering, or as Singh and Srikanth call it, a set of *partially linked classes* [6]. Each clique/class represents a subset of Γ that would satisfy

the no-cloning theorem alone. Let us say that we separate the graph into λ partially linked classes. Then we only need $\lambda - 1$ resident shares to realize the original access structure.

What we do is we split the original quantum secret using a $((\lambda, 2\lambda - 1))$ quantum threshold scheme. Of these shares, $\lambda - 1$ are dealer shares and stay in the possession of the dealer. The remaining λ shares are distributed to the players, one share for each partially linked class. We apply a secret sharing scheme on each of these player shares so that they implement the access structure corresponding to their class. This way, if the players in an authorized set work together, then they can recover a player share. They combine this with the $\lambda - 1$ shares kept by the dealer and can recover the original secret. Using this construction, the no-cloning theorem no longer restricts the set of access structures that can be implemented.

A problem that the authors leave open is computing the minimum number of resident shares needed to implement a given access structure. This problem is equivalent to finding the clique cover number of a graph, which is an NP-hard problem.

Although this scheme removes the restriction of the no-cloning theorem, we are not entirely satisfied with this approach. As we mentioned above, there is no easy way to find the minimum number of resident shares that are needed to implement an arbitrary access structure.

Additionally, the requirement that the dealer be used for reconstruction in this way is rather unnatural. One might imagine a more exaggerated version of the procedure as follows. The dealer holds onto the quantum secret, and has a list of all of the authorized sets that can access the secret. For any group that would like to reconstruct the secret, the dealer simply checks to see if that group of players is present in their list. If it is, they return the quantum state, and if it is not, then they do nothing. This procedure certainly removes the no-cloning theorem restriction. It may even remove the restriction that access structures need to be monotone. But, it is not really a quantum secret sharing scheme. It goes against the spirit of the game – there is nothing inherently quantum about the procedure, and in a way, it defeats the purpose of secret sharing.

One final problem with the scheme is if two disjoint authorized sets try to recover the secret, then by the no-cloning theorem they still cannot both obtain the secret. This introduces an unintended and artificial limitation in the scheme. Given an implementation of an access structure, it does not seem right that there is an unwritten condition that if one authorized set recovers the secret, then another authorized set cannot.

Observe that such a situation would not happen in an access structure that satisfies the no-cloning theorem. Imagine that there are two authorized sets A_1, A_2 that would both

like to recover the secret. Let's say A_1 does so. Because they must have a non-empty intersection ($A_1 \cap A_2 \neq \emptyset$), then those players in the intersection $A_1 \cap A_2$ would then be able to share access to the secret with A_2, based on the assumption that the members of A_2 have agreed to work together.

In Chapter 5, we propose a novel approach to relaxing the constraint imposed by the no-cloning theorem.

Chapter 5

An Augmented Quantum Threshold Scheme

In this section, we introduce our own idea to circumvent the no-cloning theorem, beginning with the following questions: What can we do if we were to start with two identical copies of a quantum state? What if we have k copies? Can we create a scheme that circumvents the limitations imposed by the no-cloning theorem? If so, what schemes are realizable using this new formulation? In this section, we will explore the properties of such a scheme. We will call this an **augmented quantum threshold scheme**. Let us formalize this idea before exploring its properties below:

Definition 5.1. Augmented Quantum Threshold Scheme. This is a QTS that assumes that we begin with k identical copies of a quantum state prepared in advance. As with the normal QTS, we need at least t individuals to come together to recover the secret quantum state. We will denote an augmented QTS as $((t, n, k))$.

5.1 A Loose Upper Bound

Based on the results presented in Section 4.2, it would be most natural to begin our analysis of an augmented QTS by considering the consequences of the no-cloning theorem. Let us begin with the case where $k = 2$. Then, we can extend Theorem 4.1 in the following way:

Theorem 5.1. *In any valid* $((t, n, 2))$ *scheme, any three authorized subsets cannot be pair-wise disjoint.*

The proof for this theorem is very similar to that of Theorem 4.1. Here is that theorem generalized to k copies for $k \geq 1$:

Theorem 5.2. *In any valid* $((t, n, k))$ *scheme, any* $k + 1$ *authorized subsets cannot be pair-wise disjoint.*

Using these two theorems, we can immediately propose an initial upper bound on the value of n with respect to t and k in the case of threshold schemes. We give the case for $k = 2$ as well as the more general case:

Corollary 5.3. *An augmented QTS of the form* $((t, n, 2))$ *can exist only if* $t > \frac{n}{3}$*, which is equivalent to* $n \leq 3t - 1$*.*

Corollary 5.4. *An augmented QTS of the form* $((t, n, k))$ *can exist only if* $t > \frac{n}{k+1}$*, which is equivalent to* $n \leq (k + 1)t - 1$*.*

Just as Theorems 5.1 and 5.2 extend Theorem 4.1, these Corollaries extend Corollary 4.2, and while they are a good start to our analysis, they only provide to us what schemes are not immediately ruled out by the no-cloning theorem. Figuring out methods of realizing these schemes is a different question, and that is what we consider in the following section.

5.2 A Union of Access Structures Approach

The simplest non-trivial case to implement is a $((2, 4, 2))$ scheme. Using two identical copies of a quantum state, we ask the following question: Is it possible to implement a scheme among four individuals such that only two or more people need to come together to recover the secret. The answer is yes.

To construct this scheme, we will use the following approach: we take the access structure that we want to implement and split it up into two smaller access structures, each of which are valid access structures, which means that on their own, they are monotone and satisfy the no-cloning theorem. By Theorem 4.3, we assume that there exists an implementation of a quantum secret sharing scheme that corresponds to our valid access structures, and we assign one copy to each of them. We will call this procedure the union of access structures approach.

Let the two copies of our quantum secret be $|\psi_1\rangle$ and $|\psi_2\rangle$, and let the participants be labeled p_1, p_2, p_3, p_4. Figure 5.1 shows how we implement the scheme. Each vertex corresponds to one participant. The blue edges denote authorized subsets of size 2 that are a part of the access structure Γ_1 of $|\psi_1\rangle$. Red edges correspond to Γ_2, which is the access structure of $|\psi_2\rangle$.

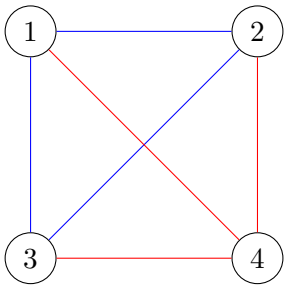

FIGURE 5.1: An image of the access structure for a $((2, 4, 2))$ threshold scheme, using two copies of the quantum state $|\Psi\rangle$

The two access structures are as follows: $\Gamma_1 = \{p_1p_2, p_2p_3, p_3p_1\}$ and $\Gamma_2 = \{p_1p_4, p_2p_4, p_3p_4\}$. Observe that each access structure satisfies is monotone and satisfies the no-cloning theorem, so a $((2, 4, 2))$ scheme exists. Also, note that in this scheme, it would be possible for, say, players 1 and 2 to recover the secret together **AND** players 3 and 4 to recover the secret together, and for the two pairs to do so separately. This is allowed. Each pair would recover a different copy of the state, and there is no way for the two pairs to recover the same copy, which satisfies the no-cloning theorem.

We have shown that we can implement a QTS that would otherwise not be possible in the normal construction. We call any augmented QTS that can be implemented in this way a valid augmented QTS.

5.2.1 A Graphical Representation

Our next step will be to generalize this implementation. We can start off by observing that, in the case of our $((2, 4, 2))$ scheme, we need the union $\Gamma_1 \cup \Gamma_2$ to consist of all subsets of size 2 from a pool of 4 players. Each of these access structures must satisfy Theorem 4.1. So, in general, a $((t, n, 2))$ scheme is realizable if we can take all subsets of size t of the n participants and divide them into 2 groups, where each group consists of an access structure that satisfies Theorem 4.1.

Such a combinatorial problem lends itself easily to a graphical representation, albeit one that is different than the one we used in Figure 5.1. By letting each vertex represent a player, we run into a problem where it is difficult to represent authorized sets of size greater than 2. In these cases, we would need an edge that has as its endpoints 3 or more vertices. These extensions of edges, called **hyperedges** do exist, but they would be more difficult to reason about, simply because of the lack of literature.

So, instead of representing the participants as vertices and the authorized subsets as edges between them, we take inspiration from Singh and Srikanth's AS graph representation, which we define above in Definition 4.10 [6]. In an AS graph, each vertex in the graph represents an authorized set, and there is an edge between two vertices if the authorized sets which they represent have a non-empty intersection. Now this is where our representation will differ slightly from Singh and Srikanth. Our representation will have edges between two vertices if they **do not intersect**. In other words, we consider the *complement* of the AS graph.

Definition 5.2. Access Structure Graph Complement. We define the **access structure graph complement** of Γ to be the graph $G = (V, E)$, where there is a vertex $v \in V$ for each authorized subset $A \in \Gamma$. The edge set E contains an edge between each pair of vertices if their corresponding authorized subsets are disjoint.

5.2.2 Generalization of $((t, n, 2))$ Schemes

In this subsection, we will explore the results that we can reach when $k = 2$ by using our new formulation. The access structure graph complement for Figure 5.1 is shown in Figure 5.2:

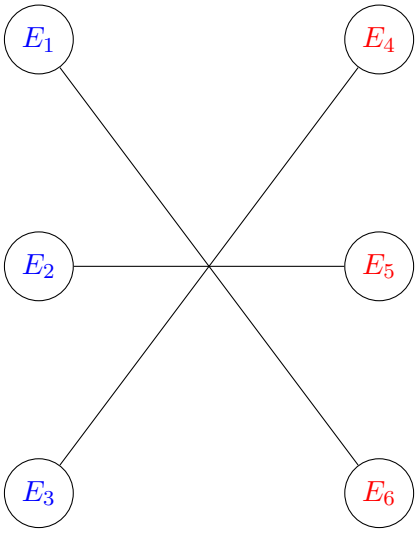

FIGURE 5.2: The access structure graph complement for a $((2, 4, 2))$ scheme.

In Figure 5.2, each vertex is an edge from Figure 5.1. There is an edge between the vertices if their edges are not incident to the same vertex in Figure 5.1. The representation illustrated in Figure 5.2 is useful to us because properties of the graph can tell us not only if a particular scheme is realizable, but why it is realizable. Let us bring in the idea of graph coloring introduced in Definition 3.7.

Lemma 5.5. *Let a $((t, n, 2))$-threshold augmented quantum secret sharing scheme have the corresponding access structure Γ. Then, this scheme is valid if and only if the access structure graph complement of Γ is 2-colorable.*

Proof. ($\rightarrow$) Another term for 2-colorable graphs are bipartite graphs. If the AS graph of an access structure Γ is bipartite, then we can separate the graph into two stable sets. Every pair of authorized sets in the same stable set has a non-empty intersection. So, we can assign one copy of the quantum state to each of these stable sets, and implement a QSS scheme that realizes the access structure corresponding to each particular subset of authorized sets. By construction, we have a valid augmented QTS.

($\leftarrow$) Now assume that we have a valid augmented QTS of the form $((t, n, 2))$. The access structure for this scheme is $\Gamma = \Gamma_1 \cup \Gamma_2$, where Γ_1 and Γ_2 are each monotone and satisfy the no-cloning theorem. Consider just the authorized sets in Γ_1. In the AS graph complement representation, the vertices corresponding to these authorized sets must be a stable set because each pair of authorized sets in Γ has a non-empty intersection. This is because they pairwise have a non-empty intersection. The same is true for Γ_2. Therefore, we must have a bipartite graph. □

By combining Lemma 5.5 and Theorem 3, we get the following claim:

Corollary 5.6. *A $((t, n, 2))$ augmented QTS is valid if and only if its corresponding AS graph complement has no odd cycles.*

We can use Corollary 5.6 to also show that $((3, 6, 2))$ is also a valid scheme, but that $((2, 5, 2))$ and $((3, 7, 2))$ are **not** valid schemes.

For the $((2, 5, 2))$ scheme, rather than try to draw an access structure, we find an odd cycle in the AS graph complement by listing an ordering of vertices that have edges connecting them: $(1, 2), (3, 4), (5, 1), (2, 3), (4, 5), (1, 2)$. Each integer represents a player, and each pairing of integers represents an size-2 subset. This cycle has length 5, so the AS graph complement of $((2, 5, 2))$ is not bipartite. Therefore, $((2, 5, 2))$ does not represent a valid augmented quantum threshold scheme. A similar approach with $((3, 7, 2))$ leads us to the same conclusion.

From the simple cases we have studied so far, we notice a pattern beginning to emerge. It seems like schemes of the form $((t, 2t, 2))$ are valid, but $((t, 2t + 1, 2))$ are not. This turns out to be true. Using the theorems that we have developed, we will formally prove these results: that all augmented QTS of the form $((t, 2t, 2))$ are valid, and all augmented QTS of the form $((t, 2t + 1, 2))$ are not valid. Therefore, the best that we can do with two copies of a quantum secret is $((t, 2t, 2))$.

Remark. Note that if a QTS $((t, n_1))$ is not valid because it violates the no-cloning theorem, then any QTS $((t, n_2))$ where $n_2 > n_1$ can never be valid because it must also violate the no-cloning theorem. To see this, consider the QTS $((t, n_2))$. We argue that the access structure for this scheme must be a superset of the access structure for $((t, n_1))$, if $n_2 > n_1$. In fact, we can construct the smaller access structure by selecting $n_2 - n_1$ players, and removing any authrozied set with which they are associated from Γ_2 to form Γ_1.

Theorem 5.7. *Any augmented quantum threshold scheme of the form* $((t, 2t, 2))$ *is valid using our union of access structures strategy.*

Proof. We are given an augmented quantum threshold scheme of the form $((t, 2t, 2))$ where $t \geq 1$. We will show that the AS graph complement of any scheme of this form is bipartite. And then, by Lemma 5.5, we are done. Consider one of the authorized sets, and without loss of generality, let this set have the participants: $\{p_1, \ldots, p_t\}$. Then, there is only one possible authorized set that is disjoint from this one: $\{p_{t+1}, \ldots, p_{2t}\}$. Note that this is true for every single authorized set (of size t). Therefore in the AS graph complement, each vertex has degree exactly equal to 1. Such a graph must be bipartite, so $((t, 2t, 2))$ is valid. □

Theorem 5.8. *Any augmented quantum threshold scheme of the form* $((t, 2t + 1, 2))$ *is not realizable using our union of access structures strategy.*

Proof. We are given an augmented quantum threshold scheme of the form $((t, 2t+1, 2))$ implemented over a set of players $\mathcal{P} = \{p_1, p_2, \ldots, p_{2t+1}\}$, and we denote each authorized subset as an unordered set of participants. For now, assume that $t \geq 2$, because if $t = 1$, the result is trivial. The only way in which we could implement a scheme over 3 players where the threshold is 1 player is to give every person a copy of the share, and we only have 2 available.

We will show that the access structure graph complement of this scheme must include an odd cycle. What we are looking for, then, is an ordered list of authorized subsets, $A_1, A_2, \ldots, A_r$, such that $A_1 = A_r$ and $A_i \cap A_{i+1} = \emptyset \; \forall i \in \{1, \ldots, r-1\}$. If r is even, then we have an odd cycle. WLOG, let the first authorized subset be $\{p_1, \ldots, p_t\}$. From this set, we can generate a cycle of authorized sets by counting in groups of t modulo

$2t+1$. Here are a few of those sets in order:

$$\begin{aligned}
&\{p_1, \ldots, p_t\} \\
&\{p_{t+1}, \ldots, p_{2t}\} \\
&\{p_{2t+1}, \ldots, p_{t-1}\} \\
&\{p_t, \ldots, p_{2t-1}\} \\
&\vdots \\
&\{p_{t+3}, \ldots, p_1\} \\
&\{p_2, \ldots, p_{t+1}\} \\
&\{p_{t+2}, \ldots, p_{2t+1}\} \\
&\{p_1, \ldots, p_t\}
\end{aligned}$$

How many edges are in this cycle? Observe that t and $2t+1$ are relatively prime, because $t \geq 2$. This means that there must be $2t+1$ edges in this cycle, which is an odd number. By Corollary 5.6, the scheme is not valid. □

We have shown that schemes of the form $((t, 2t, 2))$ are valid, but schemes of the form $((t, 2t+1, 2))$ are not valid. In the following chapter, we extend our results from $k = 2$ to general values of k.

Chapter 6

General Results on Augmented Quantum Threshold Schemes

6.1 Generalizing the Union of Access Structures Approach

In the previous chapter, we determined an upper bound on the value of n with respect to t at a fixed $k = 2$. In this section, we ask the question of how n varies with respect to k, and we prove more general results about the augmented quantum threshold scheme.

At this point, there is hardly a pattern associated with the effect of k on the possible values of n and t, so we will have to take a different approach. What worked for us in the previous chapter was posing this problem as a graph coloring problem, and indeed, that is what we will do to start. Unfortunately, there does not exist a general theorem on the c-colorability of arbitrary graphs for $c > 3$ like there is for $c = 2$. This problem is NP-hard. Nevertheless, it does not hurt to state clearly the following lemma:

Lemma 6.1. *The access structure graph complement corresponding to the augmented QTS* $((t, n, k))$ *is* k*-colorable if and only if* $((t, n, k))$ *is a valid augmented quantum threshold scheme.*

This theorem and its proof are straightforward generalizations of those of Lemma 5.5 from the previous section. In essence, the k-colorability of the graph ensures that we can separate it into at least k stable sets, each of which can be assigned to one of the copies of the quantum state.

To keep our analysis going, let us consider an example with $k = 3$ copies. The simplest, non-trivial example to consider is $((2, 5, 3))$. This is interesting to us because this specific $((t, n))$ pair is **not** possible with $k \leq 2$. We will show now that this scheme is indeed

possible to construct. One way that we can implement it is to take our implementation of $((2,4,2))$ and add both an additional copy of the state and an additional player p_5. Then, we define the access structure for the newly added state, Γ_3, to contain all authorized subsets that include p_5. The access structures corresponding to the first two states stay unchanged from $((2,4,2))$. Observe that Γ_3 is a valid access structure because each authorized set contains the common player p_5. Since our original scheme is valid, then by construction, this new scheme is valid as well. We will now show that we can extend this construction indefinitely:

Theorem 6.2. *Any scheme of the form* $((t, 2t-2+k, k))$ *is a valid augmented quantum threshold scheme.*

Proof. We have shown in Theorem 5.7 that schemes of the form $((t, 2t, 2))$ are realizable. Assume, as an inductive hypothesis, that $((t, 2t-2+i, i))$ are valid augmented quantum threshold schemes. Now, let us consider the scheme $((t, 2t-1+i, i+1))$. Using our construction, we will have an access structure $\Gamma = \Gamma_1 \cup \Gamma_2 \cup ... \cup \Gamma_i \cup \Gamma_{i+1}$, where Γ_r is the access structure corresponding to $|\Psi\rangle_r$ for $i \in 1, ..., i$. Let $\Gamma_1, ..., \Gamma_i$ remain unchanged from the scheme $((t, 2t-2+i, i))$. Then, we simply define Γ_{i+1} to contain all of the authorized subsets that include the $2t-1+i$-th player. Then, this new access structure satisfies the no-cloning theorem, and by the IH, all of the access structures satisfy the no-cloning theorem. So $((t, 2t-1+i, i+1))$ is a valid augmented quantum threshold scheme. □

6.1.1 Can we do better?

Theorem 6.2 gives us a more general result, but the question still remains - can we do better? Unfortunately, the answer is in the negative. To show this, we will bring in the Kneser Graph, introduced in Definition 3.9.

Remark. Observe that the AS graph complement of a QTS of the form $((t, n))$ is a $K(n, t)$. It is a Kneser graph on n elements with subsets of size t. This is independent of the number of copies k.

Corollary 3.2 connects Kneser's conjecture and the chromatic number of Kneser graphs. We can use this to prove the following theorem:

Theorem 6.3. *Any scheme of the form* $((t, 2t-1+k, k))$ *is not a valid augmented quantum threshold scheme.*

Proof. The complement of the AS graph for the access structure corresponding to the threshold scheme $((t, 2t-1+k, k))$ is a $K(2t-1+k, t)$, or a Kneser Graph on a set

of $2t-1+k$ elements, with subsets of size t. Then by Corollary 3.2, the corresponding graph is not k-colorable. By Theorem 6.1, schemes of the form $((t, 2t-1+k, k))$ are not valid augmented quantum threshold schemes. □

So, this is the best that we can do with k copies of a quantum state, using our union of access structures approach. More specifically, we have shown that for every extra copy of the quantum state that we begin with, we are only able to implement one additional threshold scheme for a fixed group size n. The good news is that we have a closed form answer for the question: how many copies of the quantum state do we need to implement an augmented quantum threshold scheme $((t, n, k))$? For $n \geq 2t$, we need $k = n-2t+2$.

In a way, this result might be expected with our particular construction. The number of authorized sets in the access structure increases exponentially for every new person added, so it makes sense that the access structures that we can implement are constrained even when we add more copies.

6.2 Security Considerations

An analysis of a cryptographic scheme would not be complete without an analysis of its security. Because we construct our scheme using a union of access structures, all we need to do is show that an augmented QTS is no less secure than its constituent parts. That is, using our union of access structures strategy, if the QSS schemes that are used with each copy of the quantum state are perfect, then the resulting scheme is perfect as well.

Lemma 6.4. *A quantum threshold scheme of the form* $((t, 2t-1))$ *is a perfect quantum threshold scheme.*

Proof. Observe that this is a maximal access structure. Any authorized set must have at least t participants. Therefore, the complement of any authorized set must have a size of $t-1$ or smaller. Which means that the authorized sets are exactly the complements of the unauthorized sets, so this scheme is perfect by [5]. □

Theorem 6.5. *An augmented QTS of the form* $((t, 2t-2+k, k))$ *is a perfect quantum threshold scheme.*

Proof. We are going to prove this using induction. We will show that the scheme is perfect by showing that the underlying schemes that compose it are perfect. For our

base case, consider the QTS $((t, 2t-1))$. Note that there is an implicit $k = 1$. Then by Lemma 6.4, $((t, 2t-1))$ is a perfect scheme.

For our inductive hypothesis, assume that $((t, 2t-2+k, k))$ is a perfect QTS. We will show that $((t, 2t-1+k, k+1))$ is also a perfect QTS. Using our construction, the $((t, 2t-1+k, k+1))$ is built by taking the original scheme $((t, 2t-2+k, k))$, and then adding one more share $|\psi_{k+1}\rangle$ and one more player P_{2t-1+k}. $((t, 2t-2+k, k))$ is a perfect secret sharing scheme by the IH. Therefore, we only need to show that the access structure corresponding to $|\psi_{k+1}\rangle$ is perfect. We will call this access structure Γ_{k+1}. Observe that this access structure contains all of the t-subsets of $2t-1+k$ that contain P_{2t-1+k}. However, this access structure is not maximal. Namely, the subset of players $\mathcal{P} \setminus P_{2t-1+k} = \{P_1, P_2, ..., P_{2t-2+k}\}$ is unauthorized, as well as its complement $\{P_{2t-1+k}\}$. However, we can construct this access structure out of maximal access structures using a construction presented by Gottesman in [5].

First, let the maximal access structure containing Γ_{k+1} be Γ^M. Then, $\Gamma_M = \Gamma_{k+1} \cup \{P_1, P_2, ..., P_{2t-2+k}\}$. This is a maximal access structure because the authorized sets are exactly the complements of the unauthorized sets. Let's denote the number of minimal authorized sets in Γ_{k+1} to be r, where $r = \binom{t}{2t-1+k} + 1$. Then, we construct a layered scheme, using an $((r, 2r-1))$ scheme as the outermost layer. Let the shares of this scheme be S_i for $i \in \{1, ..., 2r-1\}$. In the first r shares, there is one share corresponding to each minimal authorized set. For each of these first r shares: $\{S_j\}_{j \in 1,...,r}$, we are going to use a secret sharing scheme on S_j to share among the participants in each authorized set A_j. Each scheme will be a $((l_j, l_j))$ threshold scheme, where $l_j = |A_j|$ is the number of players in the corresponding authorized set. The latter $r-1$ shares each have an access structure equal to Γ^M. In this way, any authorized set in Γ, $A_1, \ldots, A_r$, will be able to recover one of the first r shares, and will also be able to recover the latter $r-1$ shares because $\Gamma \subseteq \Gamma^M$. This gives any authorized set in Γ enough shares to recover the secret. However, an authorized set that is in Γ^M but not in Γ can only recover $r-1$ shares, which is not enough to recover the original secret.

Note that any scheme of the form $((r, 2r-1))$ is maximal, as is any scheme of the form $((t, t))$. The authorized sets are the complements of the unauthorized sets. So, we have found a way to construct Γ_{k+1} using only maximal access structures. Therefore, Γ_{k+1} corresponds to a perfect secret sharing scheme, so by induction $((t, 2t-2+k, k))$ is a perfect quantum threshold scheme. □

6.3 Back to Assisted Quantum Secret Sharing

In this section, we give a short result that provides a closed form solution for the number of resident shares needed in an assisted QSS implementation of a threshold scheme. Recall the assisted quantum secret sharing scheme presented by Singh and Srikanth [6]. The number of resident shares needed in their scheme is $\lambda - 1$, where λ is the minimum number of partially linked classes there are in the AS graph of the access structure Γ. The question that is left open is finding a way to compute λ. We show that our results from the previous section can provide a closed form answer to this question when the access structure corresponds to a threshold scheme.

Let us consider a quantum threshold scheme $((t, n))$. How many resident shares are needed to realize this scheme? By Proposition 3.1, the minimum number of partially linked classes in the AS graph is the same as the chromatic number of the AS graph's complement. So, by Kneser's Conjecture, finding this for quantum threshold schemes is easy. The AS graph complement of this scheme is a Kneser graph on n elements with subsets of size t. The chromatic number of the AS graph complement is $n - 2t + 2$, so $\lambda = n - 2t + 2$. Therefore, the minimum number of resident shares we need for an assisted quantum threshold scheme on n players with threshold t is $n - 2t + 1$.

Chapter 7

Conclusion and Future Work

In this thesis, we have shown an implementation for a quantum threshold scheme that uses multiple copies of a quantum secret. Using an approach where we take the union of valid access structures, we are able to implement schemes that would otherwise not be realizable in a normal construction. With just one copy, the best that we can implement are schemes of the form $((t, 2t-1))$. Using multiple copies, we were able to construct an implementation for schemes of the form $((t, 2t-1+k, k))$, and we prove that these are the best that we can achieve using our strategy.

In our analysis, we restricted our discussion to just quantum threshold schemes. One possible avenue of future research would be to attempt to classify general access structures that could be implemented using a union of access structures approach. Another avenue would be to experiment with strategies that deal more closely with the quantum nature of the information with which we are working. These strategies might include using quantum entanglement or constructing quantum circuits to create novel schemes.

Bibliography

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Oct 1997. ISSN 1095-7111. doi: 10.1137/s0097539795293172. URL http://dx.doi.org/10.1137/S0097539795293172.

[2] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, March 1999. ISSN 1050-2947, 1094-1622. doi: 10.1103/PhysRevA.59.1829. URL http://arxiv.org/abs/quant-ph/9806063. arXiv: quant-ph/9806063.

[3] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3):648–651, July 1999. ISSN 0031-9007, 1079-7114. doi: 10.1103/PhysRevLett.83.648. URL http://arxiv.org/abs/quant-ph/9901025. arXiv: quant-ph/9901025.

[4] Adam D. Smith. Quantum secret sharing for general access structures. *arXiv:quant-ph/0001087*, January 2000. URL http://arxiv.org/abs/quant-ph/0001087. arXiv: quant-ph/0001087.

[5] Daniel Gottesman. On the Theory of Quantum Secret Sharing. *Physical Review A*, 61(4):042311, March 2000. ISSN 1050-2947, 1094-1622. doi: 10.1103/PhysRevA.61.042311. URL http://arxiv.org/abs/quant-ph/9910067. arXiv: quant-ph/9910067.

[6] Sudhir Kumar Singh and R. Srikanth. Assisted Quantum Secret Sharing. *arXiv:quant-ph/0407200*, July 2004. URL http://arxiv.org/abs/quant-ph/0407200. arXiv: quant-ph/0407200.

[7] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge ; New York, 10th anniversary ed edition, 2010. ISBN 978-1-107-00217-3.

[8] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1 (3):195, 1964.

[9] N. David Mermin. *Quantum computer science: an introduction*. Cambridge University Press, Cambridge, 2007. ISBN 978-0-521-87658-2. OCLC: ocn137221653.

[10] L Lovász. Kneser's conjecture, chromatic number, and homotopy. *Journal of Combinatorial Theory, Series A*, 25(3):319–324, November 1978. ISSN 00973165. doi: 10.1016/0097-3165(78)90022-5. URL https://linkinghub.elsevier.com/retrieve/pii/0097316578900225.

[11] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979. ISSN 00010782. doi: 10.1145/359168.359176. URL http://portal.acm.org/citation.cfm?doid=359168.359176.

[12] Hideki Imai, Joern Mueller-Quade, Anderson C. A. Nascimento, Pim Tuyls, and Andreas Winter. A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes. *arXiv:quant-ph/0311136*, November 2003. URL http://arxiv.org/abs/quant-ph/0311136. arXiv: quant-ph/0311136.

[13] Karin Rietjens, Berry Schoenmakers, and Pim Tuyls. Quantum Information Theoretical Analysis of Various Constructions for Quantum Secret Sharing. *arXiv:quant-ph/0502009*, February 2005. URL http://arxiv.org/abs/quant-ph/0502009. arXiv: quant-ph/0502009.

[14] Chen-Ming Bai, Zhi-Hui Li, Ting-Ting Xu, and Yong-Ming Li. A Generalized Information Theoretical Model for Quantum Secret Sharing. *International Journal of Theoretical Physics*, 55(11):4972–4986, November 2016. ISSN 0020-7748, 1572-9575. doi: 10.1007/s10773-016-3121-9. URL http://arxiv.org/abs/1603.06032. arXiv: 1603.06032.