Quantum Secret Sharing with CSS Codes

Pradeep Sarvepalli

Joint work with Andreas Klappenecker and Robert Raussendorf

Quantum Information Seminar
Department of Physics and Astronomy
University of British Columbia, Vancouver
1. Introduction and Background
2. Sharing Classical Secrets
3. Sharing Quantum Secrets
4. Matroids and Secret Sharing
Introduction and Background

Introduction to Secret Sharing

Motivated by the need to secure sensitive information.

- i) passwords for secure locations such as bank vaults
- ii) strategic military information
- iii) secure distributed computing
- iv) privacy (anonymous voting)
Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults
ii) strategic military information
iii) secure distributed computing
iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security
Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults
ii) strategic military information
iii) secure distributed computing
iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security

010010

010

010

010
Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults
ii) strategic military information
iii) secure distributed computing
iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security.

Each party learns some information about the secret.
Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults

ii) strategic military information

iii) secure distributed computing

iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security

Each party learns some information about the secret. Uncertainty reduced from $2^6$ to $2^3$ strings.
Introduction to Secret Sharing

Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults
ii) strategic military information
iii) secure distributed computing
iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security

\[
\begin{array}{c}
010010 \\
\uparrow \quad \downarrow \\
010 \\
\downarrow \\
010
\end{array}
\]

Each party learns some information about the secret. Uncertainty reduced from \(2^6\) to \(2^3\) strings.

Encoding the secret and then distributing the shares avoids this information leakage.
Motivated by the need to secure sensitive information.

i) passwords for secure locations such as bank vaults
ii) strategic military information
iii) secure distributed computing
iv) privacy (anonymous voting)

Distributing the key among various parties can enhance security.

Each party learns some information about the secret. Uncertainty reduced from $2^6$ to $2^3$ strings.

Encoding the secret and then distributing the shares avoids this information leakage.
Components of Secret Sharing

Encoded secret

Trusted dealer encodes the secret and distributes it among the parties $P = \{P_1, \ldots, P_n\}$

Reconstruction

Authorized subsets of $P$ can recover the secret

Secrecy

Unauthorized subsets cannot learn anything about the secret

Access structure

The collection of all authorized sets
Components of Secret Sharing

Encoded secret

Trusted dealer encodes the secret and distributes it among the parties $P = \{P_1, \ldots, P_n\}$

Reconstruction

Authorized subsets of $P$ can recover the secret

Secrecy

Unauthorized subsets cannot learn anything about the secret

Access structure

The collection of all authorized sets
Components of Secret Sharing

Encoded secret

- Trusted dealer encodes the secret and distributes it among the parties $P = \{P_1, \ldots, P_n\}$

Reconstruction

- Authorized subsets of $P$ can recover the secret

Secrecy

- Unauthorized subsets cannot learn anything about the secret

Access structure

- The collection of all authorized sets
Components of Secret Sharing

Encoded secret

- Trusted dealer encodes the secret and distributes it among the parties $P = \{P_1, \ldots, P_n\}$

Reconstruction

- Authorized subsets of $P$ can recover the secret

Secrecy

- Unauthorized subsets cannot learn anything about the secret

Access structure

- The collection of all authorized sets
Quantum Secret Sharing (QSS)

Classical secret to be secured
Secret is an element of a finite alphabet (usually a finite field $\mathbb{F}_q$)
Encoded into $q$ orthonormal quantum states

Quantum secret to be secured (quantum state sharing)
Secret is chosen from a set of $q$ pure states
Encoded into a linear combination of $q$ orthonormal states

Why quantum secret sharing?
- Enhanced security
- Increased efficiency for classical secrets
- We might require to share a quantum state
Quantum Secret Sharing (QSS)

Classical secret to be secured

- Secret is an element of a finite alphabet (usually a finite field $\mathbb{F}_q$)
- Encoded into $q$ orthonormal quantum states

Quantum secret to be secured (quantum state sharing)

- Secret is chosen from a set of $q$ pure states
- Encoded into a linear combination of $q$ orthonormal states

Why quantum secret sharing?

- Enhanced security
- Increased efficiency for classical secrets
- We might require to share a quantum state
Quantum Secret Sharing (QSS)

Classical secret to be secured
- Secret is an element of a finite alphabet (usually a finite field $\mathbb{F}_q$)
- Encoded into $q$ orthonormal quantum states

Quantum secret to be secured (quantum state sharing)
- Secret is chosen from a set of $q$ pure states
- Encoded into a linear combination of $q$ orthonormal states

Why quantum secret sharing?
- Enhanced security
- Increased efficiency for classical secrets
- We might require to share a quantum state
Quantum Secret Sharing (QSS)

Classical secret to be secured
- Secret is an element of a finite alphabet (usually a finite field $\mathbb{F}_q$)
- Encoded into $q$ orthonormal quantum states

Quantum secret to be secured (quantum state sharing)
- Secret is chosen from a set of $q$ pure states
- Encoded into a linear combination of $q$ orthonormal states

Why quantum secret sharing?
- Enhanced security
- Increased efficiency for classical secrets
- We might require to share a quantum state
Previous Work on Quantum Secret Sharing

   Introduced quantum secret sharing.

   Systematic methods for a class of quantum secret sharing schemes and connected them to quantum codes.

   Further developed the theory addressing general access structures and classical secrets.

   Constructions for general access structures based on monotone span programs.

   A framework for secret sharing using labelled graph states.


Previous Work on Quantum Secret Sharing

   Introduced quantum secret sharing.

   Systematic methods for a class of quantum secret sharing schemes and connected them to quantum codes.

   Further developed the theory addressing general access structures and classical secrets.

   Constructions for general access structures based on monotone span programs.

   A framework for secret sharing using labelled graph states.


Assume that the shares are distributed to $n$ players as $s_j$, $1 \leq j \leq n$.

An authorized set: \{2, 3, \ldots, 6\}

Implicitly every subset that can reconstruct the secret is correcting erasure errors on the (qu)bits it does not have access.

It suggests that codewords of an error correcting code can be used for secret sharing.
Assume that the shares are distributed to $n$ players as $s_j$, $1 \leq j \leq n$

An authorized set: $\{2, 3, \ldots, 6\}$

Implicitly every subset that can reconstruct the secret is correcting erasure errors on the (qu)bits it does not have access.

It suggests that codewords of an error correcting code can be used for secret sharing.
Secret Sharing and Error Correction

Assume that the shares are distributed to $n$ players as $s_j$, $1 \leq j \leq n$.

An authorized set: \{2, 3, \ldots, 6\}

Implicitly every subset that can reconstruct the secret is correcting erasure errors on the (qu)bits it does not have access.

It suggests that codewords of an error correcting code can be used for secret sharing.
Assume that the shares are distributed to \( n \) players as \( s_j \), \( 1 \leq j \leq n \)

An authorized set: \( \{2, 3, \ldots, 6\} \)

Implicitly every subset that can reconstruct the secret is correcting erasure errors on the (qu)bits it does not have access

It suggests that codewords of an error correcting code can be used for secret sharing.
An \([n, k, d]_q\) classical code \(C\) is a \(k\)-dimensional subspace of \(\mathbb{F}_q^n\) and it is capable of correcting up to \(d - 1\) erasures.

\(C\) can be compactly described by a \(k \times n\) generator matrix \(G\).

\[
G = \begin{bmatrix}
g_{11} & g_{12} & \ldots & g_{1n} \\
g_{21} & g_{22} & \ldots & g_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k1} & g_{k2} & \ldots & g_{kn}
\end{bmatrix}.
\]
An $[n, k, d]_q$ classical code $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ and it is capable of correcting up to $d - 1$ erasures.

$C$ can be compactly described by a $k \times n$ generator matrix $G$.

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$
Associated to an \([n, k, d]_q\) classical code \(C\) is a \([n, n-k, d^\perp]_q\) code called the dual code \(C^\perp\).

\[
C^\perp = \{ x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C \}
\]

The generator matrix \(H\) of \(C^\perp\) is called the parity check matrix of \(C\).

\[
H = \begin{bmatrix}
    h_{11} & h_{12} & \ldots & h_{1n} \\
    h_{21} & h_{22} & \ldots & h_{2n} \\
    \vdots & \vdots & \ddots & \vdots \\
    h_{k1} & h_{k2} & \ldots & h_{kn}
\end{bmatrix}
\]
Associated to an \([n, k, d]_q\) classical code \(C\) is a \([n, n-k, d^\perp]_q\) code called the dual code \(C^\perp\).

\[ C^\perp = \{ x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C \} \]

The generator matrix \(H\) of \(C^\perp\) is called the parity check matrix of \(C\).

\[
H = \begin{bmatrix}
h_{11} & h_{12} & \cdots & h_{1n} \\
h_{21} & h_{22} & \cdots & h_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
h_{k1} & h_{k2} & \cdots & h_{kn}
\end{bmatrix}.
\]
Secret Sharing Schemes from Codes

- Every $[n, k, d]_q$ code $C$ can be converted to a secret sharing scheme $\Sigma$.
- The access structure of $\Sigma$ is defined by the dual code, $C^\perp$.

Consider a code $C$ and its dual $C^\perp$

\[
C = \begin{cases} 
0000 \\
0111 \\
1011 \\
1100 
\end{cases} \quad C^\perp = \begin{cases} 
0000 \\
0011 \\
1110 \\
1101 
\end{cases}
\]

The encoded secret is any of the codewords in $C$ with the first coordinate dropped.

The authorized sets correspond to codewords in $C^\perp$ that have nonzero first coordinate.
Secret Sharing Schemes from Codes

- Every \([n, k, d]_q\) code \(C\) can be converted to a secret sharing scheme \(\Sigma\).
- The access structure of \(\Sigma\) is defined by the dual code, \(C^\perp\).

Consider a code \(C\) and its dual \(C^\perp\):

\[
C = \begin{cases} 
0000 \\
0111 \\
1011 \\
1100 
\end{cases} \quad C^\perp = \begin{cases} 
0000 \\
0011 \\
1110 \\
1101 
\end{cases}
\]

The encoded secret is any of the codewords in \(C\) with the first coordinate dropped.

The authorized sets correspond to codewords in \(C^\perp\) that have nonzero first coordinate.
Every \([n, k, d]_q\) code \(C\) can be converted to a secret sharing scheme \(\Sigma\).

The access structure of \(\Sigma\) is defined by the dual code, \(C^\perp\).

Consider a code \(C\) and its dual \(C^\perp\):

\[
C = \begin{cases}
0000 \\
0111 \\
1011 \\
1100
\end{cases} \quad C^\perp = \begin{cases}
0000 \\
0011 \\
1110 \\
1101
\end{cases}
\]

The encoded secret is any of the codewords in \(C\) with the first coordinate dropped.

The authorized sets correspond to codewords in \(C^\perp\) that have nonzero first coordinate.
Stabilizer Codes

Pauli group

$$\mathcal{P}_n = \{i^a g_1 \otimes g_2 \otimes \cdots \otimes g_n \mid g_i \in \{I, X, Z, Y = iXZ\}\}$$

A $[[n, k, d]]_q$ stabilizer code $Q$ is the joint eigenspace of an abelian subgroup $S \leq \mathcal{P}_n$.

i) $Q$ is a $q^k$-dimensional subspace in $q^n$-dimensional system Hilbert space.

ii) $Q$ can correct for $d - 1$ erasures.

$$\varphi : \begin{align*}
I & \mapsto (0,0) \\
X & \mapsto (1,0) \\
Z & \mapsto (0,1) \\
Y & \mapsto (1,1)
\end{align*}$$

$$X \otimes Z \otimes I \otimes Y \mapsto (1001|0101)$$

The stabilizer can be identified with a classical code by $\varphi$. 
Stabilizer Codes

Pauli group

\[ \mathcal{P}_n = \{ i^a g_1 \otimes g_2 \otimes \cdots \otimes g_n \mid g_i \in \{ I, X, Z, Y = iXZ \} \} \]

A \([n, k, d]_q\) stabilizer code \(Q\) is the joint eigenspace of an abelian subgroup \(S \leq \mathcal{P}_n\).

i) \(Q\) is a \(q^k\)-dimensional subspace in \(q^n\)-dimensional system Hilbert space.

ii) \(Q\) can correct for \(d - 1\) erasures.

\[ \varphi : I \mapsto (0, 0), \quad X \mapsto (1, 0), \quad Z \mapsto (0, 1), \quad Y \mapsto (1, 1) \]

\[ X \otimes Z \otimes I \otimes Y \mapsto (1001|0101) \]

The stabilizer can be identified with a classical code by \(\varphi\).
Stabilizer Codes

Pauli group

\[ \mathcal{P}_n = \{ i^a g_1 \otimes g_2 \otimes \cdots \otimes g_n \mid g_i \in \{ I, X, Z, Y = iXZ \} \} \]

A \([n, k, d]_q\) stabilizer code \( Q \) is the joint eigenspace of an abelian subgroup \( S \leq \mathcal{P}_n \).

i) \( Q \) is a \( q^k \)-dimensional subspace in \( q^n \)-dimensional system Hilbert space.

ii) \( Q \) can correct for \( d - 1 \) erasures.

\[ \begin{align*}
    \varphi : & \\
    I & \mapsto (0, 0) \\
    X & \mapsto (1, 0) \\
    Z & \mapsto (0, 1) \\
    Y & \mapsto (1, 1)
\end{align*} \]

\[ X \otimes Z \otimes I \otimes Y \mapsto (1001 \mid 0101) \]

The stabilizer can be identified with a classical code by \( \varphi \).
Stabilizer Codes

Pauli group

\[ \mathcal{P}_n = \{ i^a g_1 \otimes g_2 \otimes \cdots \otimes g_n \mid g_i \in \{ I, X, Z, Y = iXZ \} \} \]

A \([n, k, d]_q\) stabilizer code \(Q\) is the joint eigenspace of an abelian subgroup \(S \leq \mathcal{P}_n\).

i) \(Q\) is a \(q^k\)-dimensional subspace in \(q^n\)-dimensional system Hilbert space.

ii) \(Q\) can correct for \(d - 1\) erasures.

\[ \varphi : \begin{array}{c|c}
I & (0, 0) \\
X & (1, 0) \\
Z & (0, 1) \\
Y & (1, 1) \\
\end{array} \]

\[ X \otimes Z \otimes I \otimes Y \mapsto (1001|0101) \]

The stabilizer can be identified with a classical code by \(\varphi\)
CSS codes are quantum stabilizer codes which are derived from a classical code whose parity check matrix $H$ satisfies $HH^t = 0$. In other words $C \supseteq C^\perp$. The stabilizer (matrix) of the CSS code is

$$
S = \begin{bmatrix}
1111 & 0 \\
0 & 1111
\end{bmatrix}
$$

ex: If $C^\perp = [1111]$, the stabilizer of the quantum code is

$$
S = \begin{bmatrix}
1111 & 0 \\
0 & 1111
\end{bmatrix} \xrightarrow{\varphi^{-1}} \begin{bmatrix}
XXXX \\
ZZZZ
\end{bmatrix}
$$
CSS Quantum Codes

CSS codes are stabilizer codes with the stabilizer generators consisting of purely $X$ or purely $Z$ operators.

CSS codes are quantum stabilizer codes which are derived from a classical code whose parity check matrix $H$ satisfies $HH^t = 0$. In other words $C \supseteq C^\perp$. The stabilizer (matrix) of the CSS code is

$$S = \begin{bmatrix} XXXX \\ ZZZZ \end{bmatrix} \varphi \begin{bmatrix} 1111 & 0 \\ 0 & 1111 \end{bmatrix}$$

ex: If $C^\perp = [1111]$, the stabilizer of the quantum code is

$$S = \begin{bmatrix} 1111 & 0 \\ 0 & 1111 \end{bmatrix} \varphi^{-1} \begin{bmatrix} XXXX \\ ZZZZ \end{bmatrix}$$
CSS Quantum Codes

CSS codes are stabilizer codes with the stabilizer generators consisting of purely $X$ or purely $Z$ operators.

CSS codes are quantum stabilizer codes which are derived from a classical code whose parity check matrix $H$ satisfies $HH^t = 0$. In other words $C \supseteq C^\perp$. The stabilizer (matrix) of the CSS code is

$$ S = \begin{bmatrix} XXXX \\ ZZZZ \end{bmatrix} \phi \mapsto \begin{bmatrix} 1111 & 0 \\ 0 & 1111 \end{bmatrix} $$

ex: If $C^\perp = [1111]$, the stabilizer of the quantum code is

$$ S = \begin{bmatrix} 1111 & 0 \\ 0 & 1111 \end{bmatrix} \mapsto \begin{bmatrix} XXXX \\ ZZZZ \end{bmatrix} $$
What precisely is the correspondence between quantum codes and secret sharing

- Can we take an $[[n, k, d]]_q$ quantum code and convert it into a secret sharing scheme?

A correspondence between QECC and QSS exists but it seems to be limited!

- $[[2k − 1, 1, k]]_q$ quantum MDS codes can lead to threshold secret sharing schemes and vice versa, (Cleve et al 1999; Rietjens et al 2005)
- Every QECC does not appear to be a secret sharing scheme

In this talk we attempt to derive a stronger correspondence between QECC and QSS
What precisely is the correspondence between quantum codes and secret sharing

- Can we take an $[[n, k, d]]_q$ quantum code and convert it into a secret sharing scheme?

A correspondence between QECC and QSS exists but it seems to be limited!

- $[[2k − 1, 1, k]]_q$ quantum MDS codes can lead to threshold secret sharing schemes and vice versa, (Cleve et al 1999; Rietjens et al 2005)
- Every QECC does not appear to be a secret sharing scheme

In this talk we attempt to derive a stronger correspondence between QECC and QSS
What precisely is the correspondence between quantum codes and secret sharing

- Can we take an $[[n, k, d]]_q$ quantum code and convert it into a secret sharing scheme?

A correspondence between QECC and QSS exists but it seems to be limited!

- $[[2k - 1, 1, k]]_q$ quantum MDS codes can lead to threshold secret sharing schemes and vice versa, (Cleve et al 1999; Rietjens et al 2005)
- Every QECC does not appear to be a secret sharing scheme

In this talk we attempt to derive a stronger correspondence between QECC and QSS
Some more terminology

Authorized set
- Any subset which can recover the secret

Unauthorized set
- Any subset which cannot recover the secret

Access structure
- The collection of authorized sets

Minimal authorized set
- Authorized sets for which proper subsets are unauthorized

Minimal access structure
- Collection of minimal authorized sets
Some more terminology

Authorized set
- Any subset which can recover the secret

Unauthorized set
- Any subset which cannot recover the secret

Access structure
- The collection of authorized sets

Minimal authorized set
- Authorized sets for which proper subsets are unauthorized

Minimal access structure
- Collection of minimal authorized sets
Minimal Codewords

The support of \( x = (x_1, x_2, \ldots, x_n) \), is the location of its nonzero components.

ex: \( \text{supp}([1, 0, 1, 0]) = \{1, 3\} \)

We say that \( x \) covers \( y \) if \( \text{supp}(y) \subseteq \text{supp}(x) \)

ex: \((1,1,0,1)\) covers \((1,1,0,0)\) but not \((1,0,1,1)\)

A codeword of \( C \subseteq F_q^n \) is said to be **minimal** if it does not cover any other codeword of \( C \) except its scalar multiples.
Minimal Codewords

The support of $x = (x_1, x_2, \ldots, x_n)$, is the location of its nonzero components.

ex: $\text{supp}([1, 0, 1, 0]) = \{1, 3\}$

We say that $x$ covers $y$ if $\text{supp}(y) \subseteq \text{supp}(x)$

ex: $(1,1,0,1)$ covers $(1,1,0,0)$ but not $(1,0,1,1)$

A codeword of $C \subseteq F_q^n$ is said to be **minimal** if it does not cover any other codeword of $C$ except its scalar multiples.
Minimal Codewords

The support of $x = (x_1, x_2, \ldots, x_n)$, is the location of its nonzero components.

ex: $\text{supp}([1, 0, 1, 0]) = \{1, 3\}$

We say that $x$ covers $y$ if $\text{supp}(y) \subseteq \text{supp}(x)$

ex: $(1,1,0,1)$ covers $(1,1,0,0)$ but not $(1, 0, 1, 1)$

A codeword of $C \subseteq F_q^n$ is said to be minimal if it does not cover any other codeword of $C$ except its scalar multiples.
Minimal Codewords

The support of $x = (x_1, x_2, \ldots, x_n)$ is the location of its nonzero components.

ex: $\text{supp}([1, 0, 1, 0]) = \{1, 3\}$

We say that $x$ covers $y$ if $\text{supp}(y) \subseteq \text{supp}(x)$

ex: $(1,1,0,1)$ covers $(1,1,0,0)$ but not $(1,0,1,1)$

A codeword of $C \subseteq \mathbb{F}_q^n$ is said to be **minimal** if it does not cover any other codeword of $C$ except its scalar multiples.
Let $Q$ be a pure $[[n, 1, d]]_2$ CSS code derived from a classical code $C^\perp \subseteq C \subseteq \mathbb{F}_2^n$. Let $\mathcal{E}$ be the encoding given by the CSS code

$$\mathcal{E} : \langle i \rangle \mapsto \sum_{x \in C^\perp} | x + ig \rangle \quad i \in \mathbb{F}_2, \quad (1)$$

where $g \in C \setminus C^\perp$. Distribute the $n$ qubits as the $n$ shares for a secret sharing scheme, $\Sigma$. The minimal access structure $\Gamma$ is given by

$$\Gamma = \{ \text{supp}(c) \mid c \text{ is a minimal codeword in } C \setminus C^\perp \} \quad (2)$$

The reconstruction for an authorized set is to simply take the parity of the set (into an ancilla).
Secret sharing using $[[7, 1, 3]]_2$ code

$[[7, 1, 3]]_2$ is derived from a code $C \supseteq C^\perp$ with generator matrices

$$G = \begin{bmatrix} 1110000 \\ 1010101 \\ 0110011 \\ 0001111 \end{bmatrix} \quad H = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix}$$

Encoding for the secret sharing scheme

$$|0\rangle = |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle$$
$$+ |1100110\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle$$

$$|1\rangle = |1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle$$
$$+ |0011001\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle$$

$$C \setminus C^\perp = \{(0100101), (0101010), (1001100), (1110000), (0011001), (0100101), (0010110), (1111111)\}$$
Secret sharing using $[[7, 1, 3]]_2$ code

$[[7, 1, 3]]_2$ is derived from a code $C \supseteq C^\perp$ with generator matrices

$$G = \begin{bmatrix} 1110000 \\ 1010101 \\ 0110011 \\ 0001111 \end{bmatrix} \quad H = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix}$$

Encoding for the secret sharing scheme

$$|\overline{0}\rangle = |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle$$
$$+ |1100110\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle$$

$$|\overline{1}\rangle = |1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle$$
$$+ |0011001\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle$$

$$C \setminus C^\perp = \{(0100101), (0101010), (1001100), (1110000), (0011001), (0100101), (0010110), (1111111)\}$$
Secret sharing using \([\lbrack [7, 1, 3]\rbrack_2\) code

\([\lbrack [7, 1, 3]\rbrack_2\) is derived from a code \(C \supseteq C^\perp\) with generator matrices

\[
G = \begin{bmatrix}
1110000 \\
1010101 \\
0110011 \\
0001111 \\
\end{bmatrix}, \quad H = \begin{bmatrix}
1010101 \\
0110011 \\
0001111 \\
\end{bmatrix}
\]

Encoding for the secret sharing scheme

\[
\begin{align*}
|\overline{0}\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle \\
&\quad + |1100110\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \\

|\overline{1}\rangle &= |1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle \\
&\quad + |0011001\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \\
\end{align*}
\]

\(C \setminus C^\perp = \{(0100101), (0101010), (1001100), (1110000), (0011001), (0100101), (0010110), (1111111)\}\)
Secret sharing using $[[7, 1, 3]]_2$ code

Take the minimal codeword (1110000), the authorized from this is \{1, 2, 3\}.
To reconstruct the secret compute the parity of these qubits.

$$\bar{0} = \left|0000000\right\rangle + \left|1010101\right\rangle + \left|0110011\right\rangle + \left|0001111\right\rangle + \left|1100110\right\rangle + \left|1011010\right\rangle + \left|0110011\right\rangle + \left|0001111\right\rangle$$

$$\bar{1} = \left|1111111\right\rangle + \left|0101010\right\rangle + \left|1001100\right\rangle + \left|1110000\right\rangle + \left|0011001\right\rangle + \left|0100101\right\rangle + \left|1000011\right\rangle + \left|0010110\right\rangle$$
Secret sharing using $[[7, 1, 3]]_2$ code

Take the minimal codeword $(1110000)$, the authorized from this is \{1, 2, 3\}. To reconstruct the secret compute the parity of these qubits.

\[
|\bar{0}\rangle = |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + |1100110\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle
\]
\[
|\bar{1}\rangle = |1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + |0011001\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle
\]
\( C \setminus C^\perp = \{(0100101), (0101010), (1001100), (1110000), (0011001), (0100101), (0010110), (1111111)\} \)

\[ \Gamma = \left\{ \{1, 2, 7\}; \{1, 3, 5\}; \{1, 4, 6\}; \{2, 3, 4\}; \{2, 5, 6\}; \{3, 6, 7\}; \{4, 5, 7\} \right\} . \]

The minimal authorized set has \( d \) parties and all the codewords of minimum distance in \( C \setminus C^\perp \) give rise to minimal authorized sets.
CSS Code Based Secret Sharing

Let \( Q \) be a pure \([[n, 1, d]]_q \) CSS code derived from a classical code \( C^\perp \subseteq C \subseteq \mathbb{F}_q^n \). Let \( \mathcal{E} \) be the encoding given by the CSS code

\[
\mathcal{E} : |i\rangle \mapsto \sum_{x \in C^\perp} |x + ig\rangle \quad i \in \mathbb{F}_q, \quad g \in C \setminus C^\perp \text{ and } g \cdot g = \beta \neq 0 \quad (3)
\]

Distribute the \( n \) qudits as the \( n \) shares. The minimal access structure \( \Gamma \)

\[
\Gamma = \{ \text{supp}(c) | \ c \text{ is a minimal codeword in } C \setminus C^\perp \} \quad (4)
\]

The reconstruction for an authorized set derived from a minimal codeword \( c = \alpha g + s \) for some \( s \in C^\perp \) is to compute

\[
(\alpha \beta)^{-1} \sum_{j \in \text{supp}(c)} c_j S_j, \text{ where } S_j \text{ is the } j\text{th share} \quad (5)
\]
Lemma (Gottesman, 2000)

Suppose we have a set of orthonormal states $|\psi_i\rangle$ encoding a classical secret. Then a set $T$ is an unauthorized set iff

$$\langle \psi_i | F | \psi_i \rangle = c(F)$$

independent of $i$ for all operators $F$ on $T$. The set $T$ is authorized iff

$$\langle \psi_i | E | \psi_j \rangle = 0 \quad (i \neq j)$$

for all operators $E$ on the complement of $T$.

Informally,
- Authorized sets can reconstruct the secret
- Unauthorized sets cannot learn anything about the secret
Lemma (Gottesman, 2000)

Suppose we have a set of orthonormal states $|\psi_i\rangle$ encoding a classical secret. Then a set $T$ is an unauthorized set iff

$$\langle \psi_i | F | \psi_i \rangle = c(F)$$

(6)

independent of $i$ for all operators $F$ on $T$. The set $T$ is authorized iff

$$\langle \psi_i | E | \psi_j \rangle = 0 \quad (i \neq j)$$

(7)

for all operators $E$ on the complement of $T$.

Informally,

- Authorized sets can reconstruct the secret
- Unauthorized sets cannot learn anything about the secret
Quantum Secret Sharing and No Cloning

No Cloning Theorem (Wootters, Zurek, Dieks 1982)
We cannot make copies of an unknown quantum state.

No cloning theorem puts restrictions on the permissible authorized sets equivalently, access structures.

- No two authorized sets are disjoint
- The access structure $\Gamma$ is self-orthogonal

\[ \Gamma \subseteq \Gamma^* \text{ where } \Gamma^* = \{ A \mid \overline{A} \notin \Gamma \}. \]
Secret Sharing Schemes from Classical Codes

Extended Hamming code given by the following generator matrix.

\[
G_C = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

We can check that \( C \) is self-dual. The punctured code \( \rho_1(C) \) and the shortened code \( \sigma_1(C) \) are given by the following generator matrices.

\[
G_{\rho_1(C)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

\[
G_{\sigma_1(C)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]
Now let us form a (CSS) stabilizer code with stabilizer matrix as follows.

\[
S = \begin{bmatrix}
G_{\sigma_1(C)} & 0 \\
0 & \rho_{1(C)}^\perp
\end{bmatrix}
\]

\[
= \begin{bmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]
The secret is encoded into the encoded states of the quantum code and each qubit is given as a share.

For this stabilizer code the encoding for $|0\rangle$ and $|1\rangle$ is given as

$$
|0\rangle \mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle + |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle \\
+ |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle + |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle \\
|1\rangle \mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle + |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle
$$

$$
|s\rangle \mapsto \sum_{c \in \sigma_c(C)} |s \cdot \overline{X} + c\rangle \text{ where } \overline{X} = (1, 1, 1, 1, 1, 1, 1)
$$
Recovering the secret

Goal is to recover the secret accessing only the qubits in the authorized set.

The authorized sets are determined by the minimal codewords in $C^\perp$.

**Algorithm 1** Recovering the secret

1: Input: $c \in C^\perp$, a minimal codeword with $c_0 = 1$
2: for $i \in \text{supp}(c) \setminus 1$ do
3: \quad Add the $i$th qubit to the first qubit
4: end for
5: for $i \in \text{supp}(c) \setminus 1$ do
6: \quad Add the first column to the $i$th column
7: end for
Sharing Quantum Secrets

Recovering the secret

Now consider a minimal codeword in $C^\perp$ such that $c_0 = 1$. One such codeword is $(1, 1, 1, 0, 0, 0, 0, 1)$. $\text{supp}(c) = \{0, 1, 2, 7\}$, Claim $\{1, 2, 7\}$ is an authorized set.

\[
|0\rangle \mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle + |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle
\]

\[
|1\rangle \mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle + |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle
\]

At this point we have $|0\rangle \mapsto |0000000\rangle + |0000111\rangle + |0101011\rangle + |0011110\rangle + |0101100\rangle + |0011001\rangle + |1001010\rangle + |1001101\rangle$ and $|1\rangle \mapsto |1111111\rangle + |1111000\rangle + |1010100\rangle + |1100001\rangle + |1010011\rangle + |1100110\rangle + |1001010\rangle + |1001101\rangle$.
Recovering the secret

Now consider a minimal codeword in $C^\perp$ such that $c_0 = 1$. One such codeword is $(1, 1, 1, 0, 0, 0, 0, 1)$. $\text{supp}(c) = \{0, 1, 2, 7\}$, Claim $\{1, 2, 7\}$ is an authorized set.

\[
|0\rangle \mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle \\
+ |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle \\
|1\rangle \mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle \\
+ |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle 
\]
Recovering the secret

Now consider a minimal codeword in $C^\perp$ such that $c_0 = 1$. One such codeword is $(1, 1, 1, 0, 0, 0, 0, 1)$. $\text{supp}(c) = \{0, 1, 2, 7\}$, Claim $\{1, 2, 7\}$ is an authorized set.

$$
|0\rangle \mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle
+ |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle
$$

$$
|1\rangle \mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle
+ |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle
$$

At this point we have $|0\rangle \mapsto |\psi\rangle$ and $|1\rangle \mapsto |\psi'\rangle$.
The key observation is that $|\psi'\rangle = |\psi + \overline{X}'\rangle$, where 
$\overline{X}' = (1, 1, 0, 0, 0, 0, 1) = (c_1, c_2, \ldots, c_n)$. 

So we need to transform $|\psi'\rangle$ to $|\psi\rangle$.

$$
|s\rangle (|000000\rangle + |000111\rangle + |101011\rangle + |011110\rangle \\
+ |101100\rangle + |011001\rangle + |110101\rangle + |110010\rangle)
$$
The key observation is that $|\psi'\rangle = |\psi + \overline{X}'\rangle$, where
\[
\overline{X}' = (1, 1, 0, 0, 0, 0, 1) = (c_1, c_2, \ldots, c_n).
\]

So we need to transform $|\psi'\rangle$ to $|\psi\rangle$.

\[
|s\rangle (|000000\rangle + |000111\rangle + |101011\rangle + |011110\rangle + |101100\rangle + |011001\rangle + |110101\rangle + |110010\rangle)
\]
Correctness of Recovery

\[ S = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
\end{bmatrix} \rightarrow \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
\end{bmatrix} \]
Correctness of Recovery

- Minimal codewords correspond to the undetectable errors of the quantum code.
- They also act as the encoded operators of the code.

The first operation transforms the stabilizer so that the secret is in the first qubit. The second set of operations transform the encoded operator so that the encoded states are disentangled from the first qubit.
Let $C \subseteq \mathbb{F}_q^n$ be an $[n + 1, k, d]_q$ code such that $C^\perp = C$ with generator matrix $G_C$ given as

$$G_C = \begin{bmatrix} 1 & g \\ 0 & \sigma_0(C) \end{bmatrix} = \begin{bmatrix} 1 & \rho_0(C) \end{bmatrix}.$$  \hspace{1cm} (8)

Then there exists a quantum secret sharing scheme $\Sigma$ on $n$ parties whose access structure is determined by the minimal codewords of $C$ and the dealer is associated to the 1st, coordinate; $\Sigma$ is encoded using the stabilizer code with the stabilizer matrix given by

$$S = \begin{bmatrix} \sigma_0(C) & 0 \\ 0 & \rho_0(C)^\perp \end{bmatrix}.$$  \hspace{1cm} (9)

The secret is recovered using Algorithm 1.
Lemma (Cleve et al, 1999)

Suppose we have any set of orthonormal states $|\psi_i\rangle$ of subspace $Q$ encoding a quantum secret. Then a set $T$ is an unauthorized set iff

$$\langle \psi_i | F | \psi_i \rangle = c(F)$$

independent of $i$ for all operators $F$ on $T$. The set $T$ is authorized iff

$$\langle \psi_i | E | \psi_j \rangle = 0 \quad (i \neq j)$$

for all operators $E$ on the complement of $T$.

Informally,
- Authorized sets can reconstruct the secret
- Unauthorized sets cannot learn anything about the secret
Lemma (Cleve et al, 1999)

Suppose we have any set of orthonormal states \( |\psi_i\rangle \) of subspace \( Q \) encoding a quantum secret. Then a set \( T \) is an unauthorized set iff

\[
\langle \psi_i | F | \psi_i \rangle = c(F)
\]  \( \text{(10)} \)

independent of \( i \) for all operators \( F \) on \( T \). The set \( T \) is authorized iff

\[
\langle \psi_i | E | \psi_j \rangle = 0 \quad (i \neq j)
\]  \( \text{(11)} \)

for all operators \( E \) on the complement of \( T \).

Informally,

- Authorized sets can reconstruct the secret
- Unauthorized sets cannot learn anything about the secret
Matroids

A set $V$ and $C \subseteq 2^V$ form a matroid $\mathcal{M}(V,C)$ if and only if the following conditions hold.

M1) $A, B \in C$ if and only if $A \nsubseteq B$.

M2) If $x \in A \cap B$, then there exists a $C \in C$ such that $C \subseteq (A \cup B) \setminus \{x\}$.

We say that $V$ is the ground set and $C$ the set of minimal circuits of the matroid.

Matroids and secret sharing schemes are related by a correspondence between the minimal circuits and the access structure.
Vector Matroids

To every matrix $G$, we can associate a matroid.

$$G = \begin{bmatrix}
g_{11} & g_{12} & \cdots & g_{1n} \\
g_{21} & g_{22} & \cdots & g_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k1} & g_{k2} & \cdots & g_{kn}
\end{bmatrix}.$$

The ground set is the set of columns of $G$ and the minimal circuits of the matroid $G$ are the minimally independent columns of $G$. 
Given an access structure $\Gamma$ and a secret sharing scheme $\Sigma$ that realizes $\Gamma$ we can associate it to a matroid.

$$\Gamma_e = \{A \cup D \mid \text{for all } A \in \Gamma_0\}$$

$$C(A, B) = A \cup B \setminus \left( \bigcap_{C \in \Gamma_e : C \subseteq A \cup B} C \right)$$  \hspace{1cm} (12)$$

$$C_\Gamma = \{ \text{minimal sets of } C(A, B) \text{ for all } A, B \in \Gamma_0 \text{ and } A \neq B \}$$  \hspace{1cm} (13)$$

If $C_\Gamma$ satisfies the axioms M1 and M2, then we say associate the matroid $\mathcal{M}_\Gamma$ to $\Gamma$ with the ground set $P \cup D$ and the set of minimal circuits given by $C_\Gamma$ i.e.

$$\mathcal{M}_\Gamma = \mathcal{M}(P \cup D, C_\Gamma).$$  \hspace{1cm} (14)$$
Let \( C \subseteq \mathbb{F}_q^n \) be an \([n + 1, k, d]_q\) code such that \( C^\perp = C \) with generator matrix \( G_C \) given as

\[
G_C = \begin{bmatrix}
1 & g \\
0 & \sigma_0(C)
\end{bmatrix} = \begin{bmatrix}
1 & \rho_0(C)
\end{bmatrix}.
\]  

(15)

Then there exists a quantum secret sharing scheme \( \Sigma \) on \( n \) parties whose access structure is determined by the vector matroid associated to \( C \) and the dealer is associated to the 1st, coordinate; \( \Sigma \) is encoded using the stabilizer code with the stabilizer matrix given by

\[
S = \begin{bmatrix}
\sigma_0(C) & 0 \\
0 & \rho_0(C)^\perp
\end{bmatrix}.
\]  

(16)
Summary

- Derived new secret sharing schemes based on CSS codes
  - Strengthened the connection between quantum codes and secret sharing schemes
  - Provided a new characterization of the access structure in terms of minimal codewords
- Sketched some links between quantum secret sharing schemes and matroids

Thanks!
Summary

- Derived new secret sharing schemes based on CSS codes
  - Strengthened the connection between quantum codes and secret sharing schemes
  - Provided a new characterization of the access structure in terms of minimal codewords
- Sketched some links between quantum secret sharing schemes and matroids

Thanks!