Quantum Codes, (Symplectic) Matroids and Secret Sharing Schemes

Pradeep Sarvepalli

Department of Physics and Astronomy
University of British Columbia, Vancouver

Seminar on quantum topology and quantum computation, May 24, 2011
Department of Mathematics
Ohio State University

Motivation

Consider a set of vectors $\{v_1, v_2, \ldots, v_n\}$ and associated set of linear relations between of the form $\sum_i a_i v_i$.

Motivation

Consider a set of vectors $\{v_1, v_2, \ldots, v_n\}$ and associated set of linear relations between of the form $\sum_i a_i v_i$.

What can we say about these vectors if we keep information about their linear (in)dependence but throw away the a_i?

Motivation

Consider a set of vectors $\{v_1, v_2, \ldots, v_n\}$ and associated set of linear relations between of the form $\sum_i a_i v_i$.

What can we say about these vectors if we keep information about their linear (in)dependence but throw away the a_i?

Matroids emerge out this abstraction of information about independence.

Some applications of matroids

Algorithms

- Problems that have a matroidal structure can be solved optimally using the greedy algorithm

Coding theory

- Representable matroids correspond to linear codes.
- Matroids can be used to prove coding theoretic identities.
- Matroid structure theory has been used to understand the limitations/complexity of certain classes of decoders.

Communication networks

- Network coding: (Establish the limitations of linear network coding.)

Cryptography

- Efficient secret sharing schemes are induced by matroids.
- Performance bounds can be established by matroidal schemes.

Information theory

- Non Shannon information theoretic inequalities can be derived using (poly) matroids.

Matroids in quantum information

Previous work:

[Gurvits, quant-ph/02010222]: Generalized some computational problems related to matroids. These structures are more general than matroids.

[Shepherd & Bremner 2009] Binary matroids can induce a restricted model of quantum computation which is "conjectured" to be hard to simulate classically.

Matroids in quantum information

Previous work:

[Gurvits, quant-ph/02010222]: Generalized some computational problems related to matroids. These structures are more general than matroids.

[Shepherd & Bremner 2009] Binary matroids can induce a restricted model of quantum computation which is "conjectured" to be hard to simulate classically.

Present work:

[PS, 2011] Quantum codes and matroids arXiv:1104.1171

[PS, Raussendorf, 2010] Quantum secret sharing and matroids.

Matroids in quantum information

Previous work:

[Gurvits, quant-ph/02010222]: Generalized some computational problems related to matroids. These structures are more general than matroids.

[Shepherd & Bremner 2009] Binary matroids can induce a restricted model of quantum computation which is "conjectured" to be hard to simulate classically.

Present work:

[PS, 2011] Quantum codes and matroids arXiv:1104.1171

[PS, Raussendorf, 2010] Quantum secret sharing and matroids.

Outline

Some definitions

We recall some relevant characterizations of matroids using:

- Independent sets
- Bases (Maximal independent sets)
- Circuits (Minimal dependent sets)

Independent set characterization

An ordered pair $([n], \mathscr{I})$, where $\mathscr{I}$ is a collection of subsets of $[n]$ satisfying:

- $\mathscr{I} \neq \emptyset$
- If $A \in \mathscr{I}$, any subset $B \subseteq A$ is in $\mathscr{I}$
- If $A, B \in \mathscr{I}$ such that $|A| < |B|$, there exists a $x \in B \setminus A$ such that $A \cup \{x\} \in \mathscr{I}$.

The rank of the matroid is the size of a maximal independent set in $\mathscr{I}$.

Symplectic matroids (Independent set characterization)

Let $J = [n] \cup [n]^*$ where $[n] = \{1, 2, \dots, n\}$ and $[n]^* = \{1^*, 2^*, \dots, n^*\}$.

Define $* : J \to J$, where $*(i) = i^*$ and $(i^*)^* = i$

A set $S \subseteq [n] \cap [n]^*$ is admissible if $S \cap S^* = \emptyset$.

Symplectic matroids (Independent set characterization)

Let $J = [n] \cup [n]^*$ where $[n] = \{1, 2, \ldots, n\}$ and $[n]^* = \{1^*, 2^*, \ldots, n^*\}$.

Define $* : J \rightarrow J$, where $*(i) = i^*$ and $(i^*)^* = i$

A set $S \subseteq [n] \cap [n]^*$ is admissible if $S \cap S^* = \emptyset$.

Examples:

$\{1, 2, 3^*\}$ is admissible

$\{1, 1^*, 3\}$ is inadmissible

Symplectic matroids (Independent set characterization)

A tuple $([n] \cup [n]^*, \mathscr{I})$, where $\mathscr{I}$ is a collection of subsets of $[n] \cup [n]^*$ satisfying:

- ◇ $\mathscr{I} \neq \emptyset$
- ◇ If $A \in \mathscr{I}$, any subset $B \subseteq A$ is in $\mathscr{I}$
- ◇ If $A, B \in \mathscr{I}$ such that $|A| < |B|$, then
  - There exists a $x \in B \setminus A$ such that $A \cup \{x\} \in \mathscr{I}$.
  - If $A \cup B$ is inadmissible, there exists $x \notin X \cup Y$ such that $A \cup \{x\} \in \mathscr{I}$ and $(A \setminus Y^*) \cup \{x^*\}$.

The rank of the matroid is the size of a maximal independent set in $\mathscr{I}$.

Representation of matroids

A matrix M is said to be the representation of a matroid $([n], \mathscr{B})$ if the columns of the matrix can be identified with $[n]$ and the linearly independent columns with the elements of $\mathscr{I}$.

$$\begin{matrix} 1 & 2 & \ldots & n \\ \end{matrix}$$
$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

$\mathscr{I} = \{$Linearly independent column sets of $M\}$

Representation of symplectic matroids

A matrix $M \in \mathbb{F}_q^{k\times 2n}$ is said to be a representation of a symplectic matroid if and only if the columns of J can be identified with the columns of M and the bases correspond to the maximal linearly independent columns of M.

$$\begin{array}{cccccccc} 1 & 2 & \ldots & n & 1^* & 2^* & \ldots & n^* \end{array}$$
$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} & g_{11^*} & g_{12^*} & \cdots & g_{1n^*} \\ g_{21} & g_{22} & \cdots & g_{2n} & g_{21^*} & g_{22^*} & \cdots & g_{2n^*} \\ \vdots & \vdots & \ddots & \vdots & & & & \\ g_{k1} & g_{k2} & \cdots & g_{kn} & g_{k1^*} & g_{k2^*} & \cdots & g_{kn^*} \end{pmatrix}$$

$\mathscr{I} = \{$Linearly independent (admissible) column sets of $M\}$

Matroids and codes

Every linear code corresponds to the representation of some matroid.

The representation can be associated to the parity check matrix (or the generator matrix) of the code.

$$\begin{matrix} 1 & 2 & \dots & n \end{matrix}$$

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

Matroids and codes

Every linear code corresponds to the representation of some matroid.

The representation can be associated to the parity check matrix (or the generator matrix) of the code.

$$\begin{array}{cccc} 1 & 2 & \ldots & n \end{array}$$
$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

Is there an analogous result for quantum codes?

Matroids and codes

Every linear code corresponds to the representation of some matroid.

The representation can be associated to the parity check matrix (or the generator matrix) of the code.

$$
\begin{matrix} 1 & 2 & \ldots & n \end{matrix}
$$

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

Is there an analogous result for quantum codes?

Every (linear) quantum code corresponds to the representation of a symplectic matroid.

Vector spaces

Symplectic vector space is a space of dimension $2n$ and endowed with a symplectic form $\langle \cdot, \cdot \rangle$, whose basis $\{e_1, \ldots, e_n, e_1^*, \ldots, e_n^*\}$ satisfies the following relations:

$$\langle e_i, e_j \rangle = 0, i \neq j^* \quad (1)$$

$$\langle e_i, e_i^* \rangle = -\langle e_i^*, e_i \rangle = 1 \quad (2)$$

Vector spaces

Symplectic vector space is a space of dimension $2n$ and endowed with a symplectic form $\langle\cdot,\cdot\rangle$, whose basis $\{e_1,\ldots,e_n,e_1^*,\ldots,e_n^*\}$ satisfies the following relations:

$$\langle e_i, e_j\rangle = 0, i \neq j^* \quad (1)$$

$$\langle e_i, e_i^*\rangle = -\langle e_i^*, e_i\rangle = 1 \quad (2)$$

A vector space V over a field $\mathbb{F}$ is said to be isotropic if and only if for any $u,v \in V$ we have $\langle u,v\rangle = 0$, where $\langle\cdot,\cdot\rangle$ is the inner product.

Vector spaces

Symplectic vector space is a space of dimension $2n$ and endowed with a symplectic form $\langle \cdot, \cdot \rangle$, whose basis $\{e_1, \ldots, e_n, e_1^*, \ldots, e_n^*\}$ satisfies the following relations:

$$\langle e_i, e_j \rangle = 0, i \neq j^* \quad (1)$$

$$\langle e_i, e_i^* \rangle = -\langle e_i^*, e_i \rangle = 1 \quad (2)$$

A vector space V over a field $\mathbb{F}$ is said to be isotropic if and only if for any $u, v \in V$ we have $\langle u, v \rangle = 0$, where $\langle \cdot, \cdot \rangle$ is the inner product.
Let B be a basis of an isotropic subspace U. If we write the elements of B as row vectors of a matrix $M = [A|B] \in \mathbb{F}_q^{k \times 2n}$, then $AB^t = BA^t$.

Vector spaces

Symplectic vector space is a space of dimension $2n$ and endowed with a symplectic form $\langle \cdot, \cdot \rangle$, whose basis $\{e_1, \ldots, e_n, e_1^*, \ldots, e_n^*\}$ satisfies the following relations:

$$\langle e_i, e_j \rangle = 0, i \neq j^* \quad (1)$$

$$\langle e_i, e_i^* \rangle = -\langle e_i^*, e_i \rangle = 1 \quad (2)$$

A vector space V over a field $\mathbb{F}$ is said to be isotropic if and only if for any $u, v \in V$ we have $\langle u, v \rangle = 0$, where $\langle \cdot, \cdot \rangle$ is the inner product.
Let B be a basis of an isotropic subspace U. If we write the elements of B as row vectors of a matrix $M = [A|B] \in \mathbb{F}_q^{k \times 2n}$, then $AB^t = BA^t$.

Proposition (Borovik et al, 2003)

Let the row space of $M = [A|B] \in \mathbb{F}^{s \times 2n}$ be an isotropic subspace with respect to a symplectic form. Then M is the representation of a symplectic matroid.

Quantum codes

A $[[n,k]]_q$ quantum code is a q^k-dimensional subspace of the q^n-dimensional complex vector space $\mathbb{C}^{q^n}$.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3}$$

$$\mathscr{P}_n = \left\{ i^c \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \mid \sigma_i \in \{I, X, Y, Z\} \right\} \tag{4}$$

A stabilizer code is the $+1$-eigenspace of an abelian subgroup of the Pauli group.
The subgroup is called the stabilizer and it can be mapped into a $n-k \times 2n$ matrix over $\mathbb{F}_2$ (or $\mathbb{F}_q$ in case of a q-ary code) called stabilizer matrix.

Quantum codes

Proposition (Gottesman, Calderbank et al)

Let Q be an $[[n,k,d]]_q$ $\mathbb{F}_q$*-linear quantum code, then the row space of the stabilizer matrix of the code defines an isotropic subspace of dimension* $n-k$.

Quantum codes

Proposition (Gottesman, Calderbank et al)

Let Q be an $[[n,k,d]]_q$ $\mathbb{F}_q$-linear quantum code, then the row space of the stabilizer matrix of the code defines an isotropic subspace of dimension $n-k$.

Putting together with our discussion on the representations of symplectic matroids the following result is immediate.

Theorem

Let Q be an $[[n,k,d]]_q$ $\mathbb{F}_q$-linear quantum code. Then Q induces a representable symplectic matroid over $\mathbb{F}_q$ of rank $n-k$. If Q is a CSS code it induces a representable homogenous matroid.

Special cases

Lagrangian matroids: If the symplectic matroid is full rank, then we say it is a Lagrangian matroid. They correspond to stabilizer states ([[n,0]] quantum codes).

Graph states are stabilizer states which are derived from graphs whose stabilizer matrix is of the form

$$[I_n \mid A],$$

where A is the adjacency matrix of a graph G.

Every graph state induces a representable Lagrangian matroid.

Special cases

Lagrangian matroids: If the symplectic matroid is full rank, then we say it is a Lagrangian matroid. They correspond to stabilizer states ([[n,0]] quantum codes).

Graph states are stabilizer states which are derived from graphs whose stabilizer matrix is of the form

$$[I_n \mid A],$$

where A is the adjacency matrix of a graph G.

Every graph state induces a representable Lagrangian matroid.

Homogeneous symplectic matroids: Every basis has the same number of starred and unstarred elements. They correspond to CSS codes.

Some benefits of the matroid-qecc correspondence

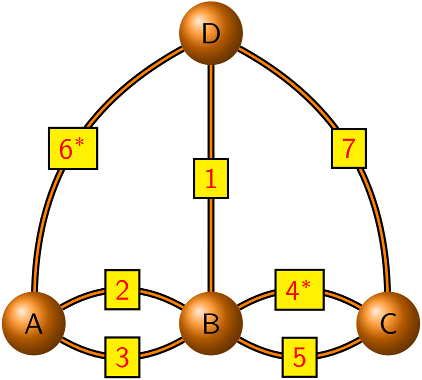
Quantum codes can be now studied using symplectic matroids.

New quantum codes from symplectic matroids.

New methods to construct symplectic matroids based on quantum codes.

Connections with invariants for symplectic matroids and quantum codes.

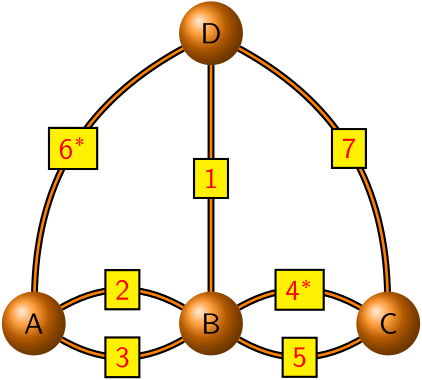
New quantum codes from the matroid-qecc correspondence



A cycle is balanced if it has odd number of starred elements.

$$\mathscr{I} = \{\text{Trees}\} \cup \{\text{Trees with one unbalanced cycle}\}$$

New quantum codes from the matroid-qecc correspondence



A cycle is balanced if it has odd number of starred elements.

$$\mathscr{I} = \{\text{Trees }\} \cup \{\text{Trees with one unbalanced cycle}\}$$

Representations of these symplectic matroids give us new quantum codes.

Invariants for symplectic matroids

The interlace polynomial was discovered recently in the context of bio technology. It is defined as

$$q_N(G;x) = \sum_{S \subseteq V(G)} (x-1)^{\mathrm{corank}(G(S))}, \qquad (5)$$

where $G(S)$ is the subgraph of G induced by S.

Invariants for symplectic matroids

The interlace polynomial was discovered recently in the context of bio technology. It is defined as

$$q_N(G;x) \quad = \quad \sum_{S\subseteq V(G)} (x-1)^{\mathrm{corank}(G(S))}, \tag{5}$$

where $G(S)$ is the subgraph of G induced by S. This is exacly the same as the Restricted Tutte-Martin polynomial defined for Largrangian matroids.

Definition (Restricted Tutte-Martin polynomial, Bouchet)

Let L be a Lagrangian matroid. The restricted Tutte-Martin polynomial is defined as

$$m(L;x) = \sum_{S\in J_n} (x-1)^{n-\mathrm{rk}(S)} \text{ where } n = \mathrm{rk}(L).. \tag{6}$$

Invariants for symplectic matroids

The interlace polynomial was discovered recently in the context of bio technology. It is defined as

$$q_N(G;x) \quad = \quad \sum_{S\subseteq V(G)} (x-1)^{\mathrm{corank}(G(S))}, \tag{5}$$

where $G(S)$ is the subgraph of G induced by S. This is exacly the same as the Restricted Tutte-Martin polynomial defined for Largrangian matroids.

Definition (Restricted Tutte-Martin polynomial, Bouchet)

Let L be a Lagrangian matroid. The restricted Tutte-Martin polynomial is defined as

$$m(L;x) = \sum_{S\in J_n} (x-1)^{n-\mathrm{rk}(S)} \text{ where } n = \mathrm{rk}(L).. \tag{6}$$

This polynomial has combinatorial interpretation. It has been studied recently in the context of quantum information by Danielsen et al.

Secret sharing

Motivated by the need to secure sensitive information.

Secret sharing

Motivated by the need to secure sensitive information.

101010 ↗ ↘

111000

010010

Secret sharing

Motivated by the need to secure sensitive information.

101010 ↗ ↘

111000

010010

	111000
Reconstruction	010010
	101010

Secret sharing

Motivated by the need to secure sensitive information.

101010 ↗ 111000 ↘ 010010

	111000
Reconstruction	010010
	101010

Requirements for a perfect secret sharing scheme:

- Secrecy: Unauthorized sets extract no information.
- Recoverability: Authorized sets can reconstruct the secret.

Secret sharing

Access structure

The collection of all authorized sets.

Information rate $\rho = \frac{\log|S|}{\max_i \log|S_i|}$

Informally, ρ quantifies the cost of sharing the secret.

Ideal secret sharing schemes have $\rho = 1$.

Secret sharing

Access structure

The collection of all authorized sets.

Information rate $\rho = \frac{\log|S|}{\max_i \log|S_i|}$

Informally, ρ quantifies the cost of sharing the secret.

Ideal secret sharing schemes have $\rho = 1$.

Secret sharing

Access structure

The collection of all authorized sets.

Information rate $\rho = \frac{\log|S|}{\max_i \log|S_i|}$

Informally, ρ quantifies the cost of sharing the secret.

Ideal secret sharing schemes have $\rho = 1$.

Two important problems studied in secret sharing

- Given an access structure how to realize it with $\rho = 1$.
- Lower (upper) bounds on ρ for an access structure.

Quantum secret sharing (QSS)

Classical secret to be shared

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

Quantum secret sharing (QSS)

Classical secret to be shared

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

Quantum secret to be shared

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

Quantum secret sharing (QSS)

Classical secret to be shared

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

Quantum secret to be shared

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

Quantum secret sharing (QSS)

Classical secret to be shared

Secret is an element of finite field $\mathbb{F}_q$

Encoded into q orthonormal quantum states

Quantum secret to be shared

Secret is chosen from a set of q quantum 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, Hillery et al, Phys. Rev. A, 59, 1829, (1999).]

Present work in context

Previous work

- Gottesman(2000) and Smith(2000) have shown how to construct quantum secret sharing schemes for general access structures.

  These schemes are not always efficient.

- No associations have been made with matroids unlike the classical case.

  Classically, the most efficient secret sharing schemes have been induced by matroids.

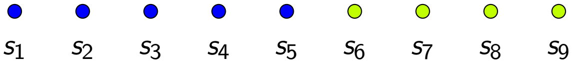
Present work

- Characterizes quantum secret sharing schemes using matroids.
- Develops efficient quantum secret sharing schemes.

Quantum secret sharing and no-cloning

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

An authorized set: $\{1, 2, 3, 4, 5\}$

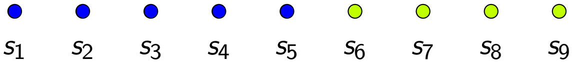


Access structures must satisfy the monotone property. i.e, if A is authorized $B \supseteq A$ is also an authorized set.

Quantum secret sharing and no-cloning

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

An authorized set: $\{1, 2, 3, 4, 5\}$



Access structures must satisfy the monotone property. i.e, if A is authorized $B \supseteq A$ is also an authorized set.

No subset of $\overline{A} = \{6, 7, 8, 9\}$ can be authorized due to the no-cloning theorem.

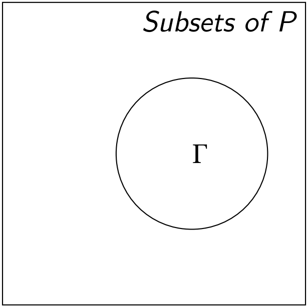
Quantum secret sharing and no-cloning

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

Access structure $\Gamma = \{$The collection of all authorized sets $\}$

- No two authorized sets are disjoint.
- The access structure Γ is self-orthogonal.

  $\Gamma \subseteq \Gamma^*$ where $\Gamma^* = \{A \mid \overline{A} \notin \Gamma\}$



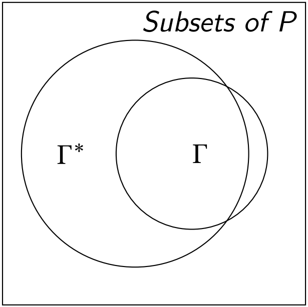
Quantum secret sharing and no-cloning

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

Access structure $\Gamma = \{$The collection of all authorized sets $\}$

- No two authorized sets are disjoint.
- The access structure Γ is self-orthogonal.

$\Gamma \subseteq \Gamma^*$ where $\Gamma^* = \{A \mid \overline{A} \notin \Gamma\}$



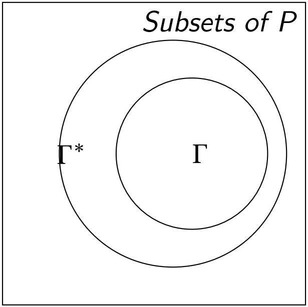
Quantum secret sharing and no-cloning

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

Access structure $\Gamma = \{$The collection of all authorized sets $\}$

- No two authorized sets are disjoint.
- The access structure Γ is self-orthogonal.

$\Gamma \subseteq \Gamma^*$ where $\Gamma^* = \{A \mid \overline{A} \not\in \Gamma\}$



Minimal Access Structure

Minimal authorized sets

Authorized sets which become unauthorized if any one party is removed.

Minimally dependent in the sense, no proper subset can recover the secret.

Minimal access structure

Collection of minimal authorized sets.

Completely characterizes the access structure.

At this juncture it is useful to abstract this idea of independence and represent it in terms of matroids.

Matroids

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

M1) $A \not\subseteq B$.

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

V is the ground set and $\mathscr{C}$ the set of minimal circuits of the matroid.

Matroids

A set V and $\mathscr{C} \subseteq 2^V$ form a matroid $\mathscr{M}(V, \mathscr{C})$ if and only if the following conditions hold. For any $A, B \in \mathscr{C}$
M1) $A \not\subseteq B$.
M2) If $x \in A \cap B$, then there exists a $C \in \mathscr{C}$ such that $C \subseteq (A \cup B) \setminus \{x\}$.

V is the ground set and $\mathscr{C}$ 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.

$$\begin{array}{ccc} \text{Matroids} & \longleftrightarrow & \text{Secret sharing schemes} \\ \Updownarrow & & \Updownarrow \\ \text{Circuits} & \longleftrightarrow & \text{Minimal authorized sets} \end{array}$$

Matroids from secret sharing schemes

Given an access structure Γ and a secret sharing scheme Σ that realizes Γ we can associate it to a matroid.

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

$$\begin{aligned} \mathscr{C}(A,B) &= A \cup B \setminus \left(\bigcap_{C \in \Gamma_e : C \subseteq A \cup B} C \right) & (7) \\ \mathscr{C}_\Gamma &= \{ \text{ minimal sets of } \mathscr{C}(A,B) \text{ for all } A, B \in \Gamma_0 \text{ and } A \neq B\}. & (8) \end{aligned}$$

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

$$\mathscr{M}_\Gamma = \mathscr{M}(P \cup D, \mathscr{C}_\Gamma). \qquad (9)$$

[Martin, K.M. Discrete Structures in the Theory of Secret Sharing, 1991]

Secret sharing schemes from matroids

Given a matroid $\mathscr{M}$ we can associate a secret sharing scheme to $\mathscr{M}$. Let $V = \{1, \ldots, n, n+1\}$

- Identify $i \in V$, as the dealer
- Consider all the circuits of $\mathscr{M}$ that contain i.

$$\mathscr{C}_i = \{C \in \mathscr{C} \mid i \in C\}$$

- Consider the access structure given by

$$\Gamma_i = \{A \setminus i \mid 2^V \supseteq A \supseteq C \text{ for some } C \in \mathscr{C}_i\}. \tag{10}$$

Fact (Cramer et al, 2008)

Every matroid $\mathscr{M}(V, \mathscr{C})$ induces an access structure Γ_i as defined in (10).

Quantum secret sharing schemes from matroids

Not every matroid does not induce a QSS because of the no-cloning theorem. We need to ensure that $\Gamma_i \subseteq \Gamma_i^*$.

Quantum secret sharing schemes from matroids

Not every matroid does not induce a QSS because of the no-cloning theorem. We need to ensure that $\Gamma_i \subseteq \Gamma_i^*$.

We can also define matroids in terms of bases.

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

M1') $\mathscr{B} \neq \emptyset$

M2') If $x \in B_1 \setminus B_2$, then there exists a $y \in B_2 \setminus B_1$ such that $B_1 \setminus \{x\} \cup \{y\} \in \mathscr{B}$.

Quantum secret sharing schemes from matroids

Not every matroid does not induce a QSS because of the no-cloning theorem. We need to ensure that $\Gamma_i \subseteq \Gamma_i^*$.

We can also define matroids in terms of bases.

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

M1') $\mathscr{B} \neq \emptyset$

M2') If $x \in B_1 \setminus B_2$, then there exists a $y \in B_2 \setminus B_1$ such that $B_1 \setminus \{x\} \cup \{y\} \in \mathscr{B}$.

The dual matroid $\mathscr{M}(V,\mathscr{B}^*)$ has as bases $\mathscr{B}^* = \{V \setminus B \mid B \in \mathscr{B}\}$.

Identically self-dual matroid

$$\mathscr{M}(V,\mathscr{B}) = \mathscr{M}(V,\mathscr{B}^*)$$

Matroidal QSS

Fact (Cramer et al, IEEE Trans. Inform. Theory, 2008)

Let Γ_i *and* Γ_i^d *be the access structures induced by a matroid* $\mathscr{M}(V,\mathscr{C})$ *and its dual matroid* $\mathscr{M}^*$ *by treating the ith element as the dealer. Then we have*

$$\Gamma_i^d = \Gamma_i^* \tag{11}$$

Matroidal QSS

Fact (Cramer et al, IEEE Trans. Inform. Theory, 2008)

Let Γ_i and Γ_i^d be the access structures induced by a matroid $\mathscr{M}(V,\mathscr{C})$ and its dual matroid $\mathscr{M}^*$ by treating the ith element as the dealer. Then we have

$$\Gamma_i^d = \Gamma_i^* \tag{11}$$

For QSS we need $\Gamma_i \subseteq \Gamma_i^*$. For an identically self-dual matroid we have $\Gamma_i = \Gamma_i^d = \Gamma_i^*$.

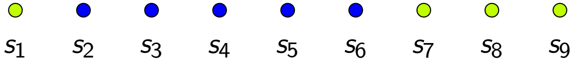
Existence of matroidal QSS

An identically self-dual matroid induces a quantum secret sharing scheme.

Secret sharing and error correction

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

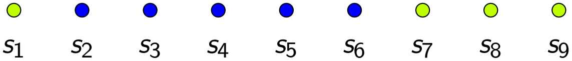
An authorized set: $\{2, 3, \ldots, 6\}$



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 cannot access.

It suggests that codewords of a (quantum) error correcting code can be used for secret sharing.

Representable matroids

To every matrix G, we can associate a matroid.

$$\begin{array}{cccc} 1 & 2 & \ldots & n \end{array}$$
$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

The ground set is the set of columns of G and the minimal circuits of the matroid are the minimally dependent columns of G.

A matroid that can be represented as a matrix is called a representable matroid.

Representable matroids

To every matrix G, we can associate a matroid.

$$\begin{matrix} 1 & 2 & \ldots & n \\ \end{matrix}$$
$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

The ground set is the set of columns of G and the minimal circuits of the matroid are the minimally dependent columns of G.

A matroid that can be represented as a matrix is called a representable matroid.

The representation of the matroid defines the encoding for the secret sharing scheme.

The representation of the dual matroid defines the reconstruction procedure.

Matroid representation to secret sharing scheme

Suppose that we have a representation of a matroid

$$G = \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Consider the row space of G

00000000	11111111
01010101	10101010
00110011	11001100
00001111	11110000
01100110	10011001
01011010	10100101
00111100	11000011
01101001	10010110

Encoding the secret

$0 \mapsto$ a random element from 1st colum

$1 \mapsto$ a random element from 2nd colu

Matroid representation to secret sharing scheme

Suppose that we have a representation of a matroid

$$G = \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Consider the row space of G

00000000	11111111
01010101	10101010
00110011	11001100
00001111	11110000
01100110	10011001
01011010	10100101
00111100	11000011
01101001	10010110

Encoding the secret

$0 \mapsto$ a random element from 1st colum

$1 \mapsto$ a random element from 2nd colur

Reconstruction (example authorized set {1,2,3 })

$01010101 \mapsto 1 \oplus 0 \oplus 1 = 0$

$10100101 \mapsto 0 \oplus 1 \oplus 0 = 1$

From matroid representation to QSS

As before consider the row space of G:

00000000	11111111
01010101	10101010
00110011	11001100
00001111	11110000
01100110	10011001
01011010	10100101
00111100	11000011
01101001	10010110

Encoding the secret

$$\begin{aligned} |0\rangle &\mapsto |0000000\rangle + |1000111\rangle + |0101011\rangle + |0011110\rangle \\ &+ |1101100\rangle + |1011001\rangle + |0110101\rangle + |1110010\rangle = \left|\bar{0}\right\rangle \\ |1\rangle &\mapsto |1111111\rangle + |0111000\rangle + |1010100\rangle + |1100001\rangle \\ &+ |0010011\rangle + |0100110\rangle + |1001010\rangle + |0001101\rangle = \left|\bar{1}\right\rangle \end{aligned}$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha\left|\bar{0}\right\rangle + \beta\left|\bar{1}\right\rangle$$

Quantum secret sharing schemes from matroids

Reconstructing the quantum secret:

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

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

Suppose we compute the parity of the first 3 qubits i.e. $q_1 \mapsto q_1 \oplus q_2 \oplus q_3$

$$\left|\bar{0}\right\rangle \mapsto |0000000\rangle + |0010101\rangle + |0110011\rangle + |0001111\rangle + |0100110\rangle + |0011010\rangle + |0111100\rangle + |0101001\rangle = |0\rangle\left|\psi_0\right\rangle$$

$$\left|\bar{1}\right\rangle \mapsto |1111111\rangle + |1101010\rangle + |1001100\rangle + |1110000\rangle + |1011001\rangle + |1100101\rangle + |1000011\rangle + |1010110\rangle = |1\rangle\left|\psi_1\right\rangle$$

For an arbitrary quantum secret $\alpha|0\rangle + \beta|1\rangle$, we get

Quantum secret sharing schemes from matroids

Disentangling the quantum secret: The representation of the dual matroid tells which operations to perform to disentangle the secret.

- $q_2 \mapsto q_2 \oplus q_1$
- $q_3 \mapsto q_3 \oplus q_1$

$$|s\rangle \left(|000000\rangle + |000111\rangle + |101011\rangle + |011110\rangle \right.$$
$$\left. + |101100\rangle + |011001\rangle + |110101\rangle + |110010\rangle\right)$$

The quantum code beneath the secret sharing scheme

Hidden in the previous example is a [[7,1,3]] stabilizer quantum code which defines the encoding and recovery.

The quantum code beneath the secret sharing scheme

Hidden in the previous example is a [[7,1,3]] stabilizer quantum code which defines the encoding and recovery.

Suppose that G_C is a representation of an identically self-dual matroid.

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \text{ and } G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \qquad (12)$$

The quantum code beneath the secret sharing scheme

Hidden in the previous example is a $[[7,1,3]]$ stabilizer quantum code which defines the encoding and recovery.

Suppose that G_C is a representation of an identically self-dual matroid.

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \text{ and } G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \quad (12)$$

Then the encoded states for the secret are precisely the uniform superpositions of the cosets of C_1 in C_2, where $C_1 \subseteq C_2$ are generated by $G_{\sigma_0(C)}$ and $G_{\rho_0(C)}$ respectively.

The quantum code beneath the secret sharing scheme

Hidden in the previous example is a [[7,1,3]] stabilizer quantum code which defines the encoding and recovery.

Suppose that G_C is a representation of an identically self-dual matroid.

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \text{ and } G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \tag{12}$$

Then the encoded states for the secret are precisely the uniform superpositions of the cosets of C_1 in C_2, where $C_1 \subseteq C_2$ are generated by $G_{\sigma_0(C)}$ and $G_{\rho_0(C)}$ respectively.

- Each logical state is a superposition of the cosets of C_1 in C_2
- The reconstruction in general relies on treating the unauthorized parties as erasures and using this quantum code to correct for them.

Quantum secret sharing schemes from matroids

Let $\mathscr{M}(V,\mathscr{C})$ be an identically self-dual matroid representable over $\mathbb{F}_q$ and $C \subseteq \mathbb{F}_q^{n+1}$ such that its generator matrix is a representation of $\mathscr{M}$.

$$G_C = \left[\begin{array}{c|c} 1 & g \\ \mathbf{0} & G_{\sigma_0(C)} \end{array}\right] \text{ and } G_{\rho_0(C)} = \left[\begin{array}{c} g \\ G_{\sigma_0(C)} \end{array}\right]. \quad (13)$$

Then there exists a quantum secret sharing scheme Σ on n parties whose access structure is determined the by $\mathscr{M}$ and the dealer is associated to the first coordinate. The encoding for Σ is determined by the stabilizer code with the stabilizer matrix given by

$$S = \left[\begin{array}{c|c} G_{\sigma_0(C)} & \mathbf{0} \\ \mathbf{0} & G_{\rho_0(C)^\perp} \end{array}\right]. \quad (14)$$

The reconstruction procedure for an authorized set A of Σ is the transformation on S such that the encoded operators for the transformed stabilizer code are X_1 and Z_1.

Duals of Lagrangian matroids

Given a Lagrangian matroid L whose collection of bases is $\mathscr{B}$, we can define the dual matroid as follows:

The collection of bases of the dual matroid are given by $B^* = \{B^* \mid B \in \mathscr{B}\}$.

The collection of circuits of the dual matroid are given by $\mathscr{C}^* = \{C^* \mid C \in \mathscr{C}\}$. Elements of $\mathscr{C}^*$ are also called cocircuits of $\mathscr{L}$.

QSS from Lagrangian matroids

Let L be a Lagrangian matroid, then we define an access structure from the circuits of $\mathscr{L}$ as follows. Define the map $\varphi : [n] \cup [n]^* \to [n]$ where

$$\varphi(i) = \begin{cases} i & \text{if } i \in [n] \\ i^* & \text{if } i \in [n]^* \end{cases} \tag{15}$$

We obtain an access structure by considering $i \in [n]$ as the dealer. The induced minimal access structure is given as

$$\Gamma_{i,\min} = \{\varphi(A) \mid A \cup \{i\} \text{ or } A \cup \{i^*\} \in \mathscr{C}\}, \tag{16}$$

where $\mathscr{C}$ is the collection of circuits of $\mathscr{L}$. We say a Lagrangian matroid is secret sharing if the access structure induced by it for any $i \in [n]$ is a quantum access structure.

Secret-sharing Lagrangian matroids

Necessary condition for secret-sharing symplectic matroids.

Theorem

Suppose that G is a graph without loops or multi-edges and whose adjacency matrix is given by A. Let L be a Lagrangian matroid induced by G such that L is represented by $\begin{bmatrix} I & A \end{bmatrix}$. If G has no cycles of length ≤ 4 and no vertices of degree 1, then the access structure induced by L is not a valid quantum access structure.

Secret-sharing Lagrangian matroids

Necessary condition for secret-sharing symplectic matroids.

Theorem

Suppose that G is a graph without loops or multi-edges and whose adjacency matrix is given by A. Let L be a Lagrangian matroid induced by G such that L is represented by $\begin{bmatrix} I & A \end{bmatrix}$*. If G has no cycles of length* ≤ 4 *and no vertices of degree 1, then the access structure induced by L is not a valid quantum access structure.*

Sufficient condition for secret-sharing symplectic matroids.

Theorem

Let $\mathscr{L}$ *be a self-dual Lagrangian matroid. Then the access structure* $\Gamma_{i,\min}$ *as defined in equation* (16) *is a valid quantum access structure.*

Summary

- A correspondence between symplectic matroids and quantum codes.

  This parallels the correspondence between classical linear codes and matroids.
  Can construct new quantum codes from symplectic matroids and vice versa.

- Quantum secret sharing schemes with information rate one based on self-dual matroids.

  The association to matroids is constructive, we give explicit schemes.

[P.S., Raussendorf] Matroids and quantum secret sharing schemes, Phys. Rev. A 81, 052333, 2010.

[P.S.] Quantum codes and symplectic matroids arXiv:1104.1171, 2011.

Scope for future work

Quantum codes and symplectic matroids.

- Representations for graphical symplectic matroids.
- Study the performance of qecc from symplectic matroids.
- Polynomial invariants for quantum codes via symplectic matroids.

QSS and Matroids

- Characterize all matroidal QSS constructively.
- Obtain QSS from non-representable matroids.
- Does there exist an ideal QSS that is not matroidal?

Performance of QSS

- Information rates of matroidal QSS.
- Upper and lower bounds on the information rates of QSS.
- Construct schemes meeting the bounds.

Scope for future work

Quantum codes and symplectic matroids.

- Representations for graphical symplectic matroids.
- Study the performance of qecc from symplectic matroids.
- Polynomial invariants for quantum codes via symplectic matroids.

QSS and Matroids

- Characterize all matroidal QSS constructively.
- Obtain QSS from non-representable matroids.
- Does there exist an ideal QSS that is not matroidal?

Performance of QSS

- Information rates of matroidal QSS.
- Upper and lower bounds on the information rates of QSS.
- Construct schemes meeting the bounds.

Thank You!