Quantum Codes and Symplectic Matroids

Pradeep Sarvepalli

Department of Electrical Engineering
Indian Institute of Technology Madras

July 01, 2014
2014 IEEE International Symposium on Information Theory
Honolulu, HI

Matroids

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

Matroids

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

Suppose we keep information about their linear (in)dependence but throw away the a_i.

Matroids

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

Suppose we keep information about their linear (in)dependence but throw away the a_i.

Matroids emerge out this abstraction of information about independence.

Why study 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

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.

Outline

Matroids—independent set characterization

A matroid is an ordered pair $(V, \mathscr{I})$, where V is called the ground set and $\mathscr{I}$ is a collection of subsets of V 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 $\mathscr{I}$.

Matroids—independent set characterization

A matroid is an ordered pair $(V, \mathscr{I})$, where V is called the ground set and $\mathscr{I}$ is a collection of subsets of V 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 $\mathscr{I}$.

- An independent set of maximal size is called a basis.
- A minimal dependent set is called a circuit.

Matroids can also be characterized in terms of bases and circuits.

Matorids and codes

Let G be the generator matrix of a classical code. Then we can obtain a matroid M_G from G.

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

The ground set is the set of columns of G and $\mathscr{I}$ is the collection of linearly independent columns of G.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.
- In a stabilizer matrix two columns are associated to a qubit.
  - $\Rightarrow$ These columns cannot be in an independent set simultaneously.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.
- In a stabilizer matrix two columns are associated to a qubit.
  - $\Rightarrow$ These columns cannot be in an independent set simultaneously.
- A quantum code has no dual unlike a classical code.
  - $\Rightarrow$ The quantum analogue must have no dual.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.
- In a stabilizer matrix two columns are associated to a qubit.
  - $\Rightarrow$ These columns cannot be in an independent set simultaneously.
- A quantum code has no dual unlike a classical code.
  - $\Rightarrow$ The quantum analogue must have no dual.
- Stabilizer matrix is self-orthogonal with respect to the symplectic inner product.
  - $\Rightarrow$ An arbitrary matrix must not induce the quantum analogue.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.
- In a stabilizer matrix two columns are associated to a qubit.
  - $\Rightarrow$ These columns cannot be in an independent set simultaneously.
- A quantum code has no dual unlike a classical code.
  - $\Rightarrow$ The quantum analogue must have no dual.
- Stabilizer matrix is self-orthogonal with respect to the symplectic inner product.
  - $\Rightarrow$ An arbitrary matrix must not induce the quantum analogue.
- Stabilizer matrix cannot be punctured to give a valid stabilizer matrix.
  - $\Rightarrow$ The quantum analogue must not allow for an operation similar to puncturing.

Relating quantum codes to matroids

So what must the analogue of the matroid look like for the quantum code?

- An (additive) quantum code is defined by the stabilizer matrix
  - $\Rightarrow$ The linearly independent columns of the stabilizer matrix may form the independent sets of quantum analogue of matroid.
- In a stabilizer matrix two columns are associated to a qubit.
  - $\Rightarrow$ These columns cannot be in an independent set simultaneously.
- A quantum code has no dual unlike a classical code.
  - $\Rightarrow$ The quantum analogue must have no dual.
- Stabilizer matrix is self-orthogonal with respect to the symplectic inner product.
  - $\Rightarrow$ An arbitrary matrix must not induce the quantum analogue.
- Stabilizer matrix cannot be punctured to give a valid stabilizer matrix.
  - $\Rightarrow$ The quantum analogue must not allow for an operation similar to puncturing.
- Stabilizer matrix can be shortened to a valid stabilizer matrix.
  - $\Rightarrow$ The quantum analogue must allow for an operation similar to shortening.

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 $S \cap S^* = \emptyset$.

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

Symplectic matroids (Independent set characterization)

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

- $\mathscr{I} \neq \emptyset$

Symplectic matroids (Independent set characterization)

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

- $\mathscr{I} \neq \emptyset$
- If $A \in \mathscr{I}$, any subset $B \subseteq A$ is in $\mathscr{I}$

Symplectic matroids (Independent set characterization)

A symplectic matroid is a tuple $([n] \cup [n]^*, \mathscr{I})$, where $\mathscr{I}$ is a collection of admissible 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
  - Either there exists a $x \in B \setminus A$ such that $A \cup \{x\} \in \mathscr{I}$

Symplectic matroids (Independent set characterization)

A symplectic matroid is a tuple $([n] \cup [n]^*, \mathscr{I})$, where $\mathscr{I}$ is a collection of admissible 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
  - Either there exists a $x \in B \setminus A$ such that $A \cup \{x\} \in \mathscr{I}$
  - Or $A \cup B$ is inadmissible, there exists $x \notin A \cup B$ such that $A \cup \{x\} \in \mathscr{I}$ and $(A \setminus B^*) \cup \{x^*\} \in \mathscr{I}$.

Symplectic matroids (Independent set characterization)

A symplectic matroid is a tuple $([n] \cup [n]^*, \mathscr{I})$, where $\mathscr{I}$ is a collection of admissible 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
  - Either there exists a $x \in B \setminus A$ such that $A \cup \{x\} \in \mathscr{I}$
  - Or $A \cup B$ is inadmissible, there exists $x \notin A \cup B$ such that $A \cup \{x\} \in \mathscr{I}$ and $(A \setminus B^*) \cup \{x^*\} \in \mathscr{I}$.

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

Other characterizations of symplectic matroids in terms of bases, greedy algorithm exist.

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.

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

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

Proposition (Gelfand et al)

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

Quantum codes and symplectic matroids

Proposition

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 and symplectic matroids

Proposition

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 $n-k$.

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).

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.

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.

If Q is a CSS code it induces a representable homogenous matroid.

Some benefits of the 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.

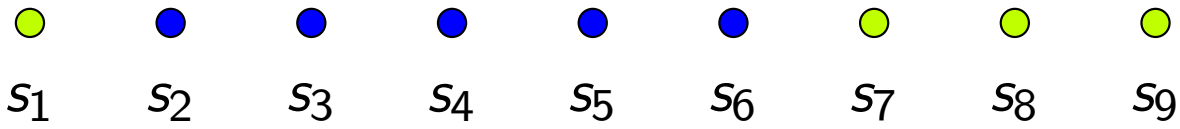
Connections with invariants for symplectic matroids and quantum codes.

Application to quantum secret sharing.

Quantum secret sharing schemes

In a quantum secret sharing scheme we share a secret using quantum states. Assume that the shares are distributed to n players as s_j, $1 \leq j \leq n$

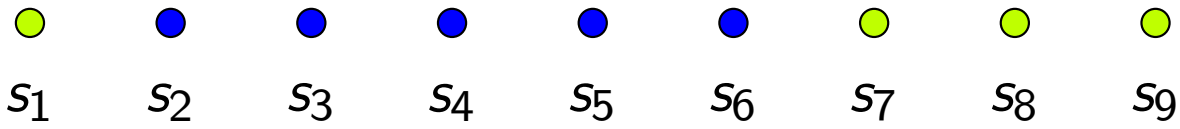
An authorized set: $\{2, 3, \ldots, 6\}$



Quantum secret sharing schemes

In a quantum secret sharing scheme we share a secret using quantum states. Assume that the shares are distributed to n players as s_j, $1 \leq j \leq n$

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



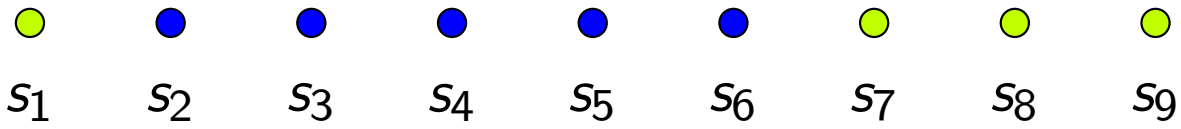
Implicitly every subset that can reconstruct the secret is correcting erasure errors on the (qu)bits it cannot access.

Subsets that reconstruct are called authorized sets and the collection of such sets is called an access structure.

Quantum secret sharing schemes

In a quantum secret sharing scheme we share a secret using quantum 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 cannot access.

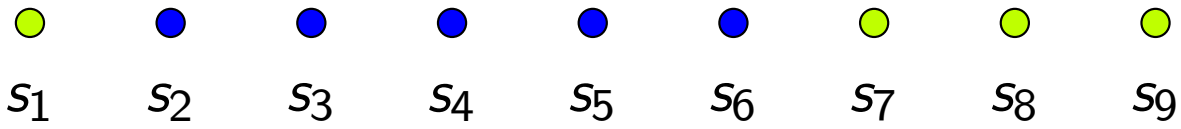
Subsets that reconstruct are called authorized sets and the collection of such sets is called an access structure.

- Matroids induce efficient (classical) secret sharing schemes.
- Bounds on the efficiency of classical schemes can be computed using matroids.

Quantum secret sharing schemes

In a quantum secret sharing scheme we share a secret using quantum 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 cannot access.

Subsets that reconstruct are called authorized sets and the collection of such sets is called an access structure.

- Matroids induce efficient (classical) secret sharing schemes.
- Bounds on the efficiency of classical schemes can be computed using matroids.

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

$$\varphi(i) = \begin{cases} i & \text{if } i \in [n] \\ i^* & \text{if } i \in [n]^* \end{cases} \tag{2}$$

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

$$\Gamma_{i,\min} = \{\varphi(A) \mid A \cup \{i\} \text{ or } A \cup \{i^*\} \in \mathscr{C}\}, \tag{3}$$

where $\mathscr{C}$ is the collection of circuits of $\mathscr{L}$.

Secret-sharing Lagrangian matroids

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

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.

Every matroid induces a secret sharing scheme but not every symplectic matroid induces a quantum secret sharing scheme.

Secret-sharing Lagrangian matroids

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.

Every matroid induces a secret sharing scheme but not every symplectic matroid induces a quantum secret sharing scheme.

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.

Duals of Lagrangian matroids

We can define a notion of duality for Lagrangian matroids.

Duals of Lagrangian matroids

We can define a notion of duality for Lagrangian matroids.

Let $\mathscr{B}$ be the collection of bases of a Lagrangian matroid. Then the dual Lagrangian matroid has the collection of bases

$$\mathscr{B}^* = \{B^* \mid B \in \mathscr{B}\} \tag{4}$$

A Lagrangian matroid is said to be self-dual if it is equal to its dual.

Duals of Lagrangian matroids

We can define a notion of duality for Lagrangian matroids.

Let $\mathscr{B}$ be the collection of bases of a Lagrangian matroid. Then the dual Lagrangian matroid has the collection of bases

$$\mathscr{B}^* = \{B^* \mid B \in \mathscr{B}\} \tag{4}$$

A Lagrangian matroid is said to be self-dual if it is equal to its dual.

Duals of Lagrangian matroids

We can define a notion of duality for Lagrangian matroids.

Let $\mathscr{B}$ be the collection of bases of a Lagrangian matroid. Then the dual Lagrangian matroid has the collection of bases

$$\mathscr{B}^* = \{B^* \mid B \in \mathscr{B}\} \tag{4}$$

A Lagrangian matroid is said to be self-dual if it is equal to its dual.

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 (3) 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 from Lagrangian matroids.

  Necessary and sufficient conditions on when a Lagrangian matroid is secret sharing.

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 from Lagrangian matroids.

  Necessary and sufficient conditions on when a Lagrangian matroid is secret sharing.

Thank You!