Secret Sharing and Duality

Laszlo Csirmaz

Central European University
UTIA, Prague

CECC 2019

June 12–14, Telč, Czech Republic

Contents

List of players

Mathematical objects with duals (in order of their appearence):

1. linear subspace L of the vector space $\mathbb{F}^n$
   dual space $L^\perp$ is the set of vectors orthogonal to L
2. linear code $\mathcal{C}$ with codewords in $\mathbb{F}^n$
   dual code $\mathcal{C}^\perp$ is the orthogonal subspace
3. access structure $\mathcal{A} \subseteq 2^P$ for a secret sharing scheme with participants P
   A is qualified in $\mathcal{A}^\perp$ iff its complement is unqualified in $\mathcal{A}$
4. matroid M
   C is a circuit in $M^\perp$ iff $M-C$ is a base in M
5. polymatroid f on ground set M
   $f^\perp(A) = f(A) + \sum_{i\in A} f(i) - f(M)$

List of players

Mathematical objects with duals (in order of their appearence):

1. linear subspace L of the vector space $\mathbb{F}^n$

   dual space $L^\perp$ is the set of vectors orthogonal to L
2. linear code $\mathcal{C}$ with codewords in $\mathbb{F}^n$

   dual code $\mathcal{C}^\perp$ is the orthogonal subspace
3. access structure $\mathcal{A} \subseteq 2^P$ for a secret sharing scheme with participants P

   A is qualified in $\mathcal{A}^\perp$ iff its complement is unqualified in $\mathcal{A}$
4. matroid M

   C is a circuit in $M^\perp$ iff $M - C$ is a base in M
5. polymatroid f on ground set M

   $f^\perp(A) = f(A) + \sum_{i \in A} f(i) - f(M)$

List of players

Mathematical objects with duals (in order of their appearence):

1. linear subspace L of the vector space $\mathbb{F}^n$
   dual space $L^\perp$ is the set of vectors orthogonal to L
2. linear code $\mathcal{C}$ with codewords in $\mathbb{F}^n$
   dual code $\mathcal{C}^\perp$ is the orthogonal subspace
3. access structure $\mathcal{A} \subseteq 2^P$ for a secret sharing scheme with participants P
   A is qualified in $\mathcal{A}^\perp$ iff its complement is unqualified in $\mathcal{A}$
4. matroid M
   C is a circuit in $M^\perp$ iff $M-C$ is a base in M
5. polymatroid f on ground set M
   $f^\perp(A) = f(A) + \sum_{i \in A} f(i) - f(M)$

Contents

Duality for linear spaces

$\mathbb{F}$ is a finite field.

L is a *linear subspace* of $\mathbb{F}^n$ if L is closed for addition and multiplication by scalars from $\mathbb{F}$.

Vectors $\mathbf{v}$ and $\mathbf{w}$ are *orthogonal* if $\mathbf{v} \cdot \mathbf{w} = 0$ (usual inner product)

$\mathbf{w} \in L^\perp$ if $\mathbf{w}$ is orthogonal to all elements of L

Facts

- *$L^\perp$ is a linear subspace*
- $(L^\perp)^\perp = L$
- $\dim(L) + \dim(L^\perp) = n$
- *$L \oplus L^\perp$ is* **not** *necessarily a decomposition of $\mathbb{F}^n$; $L = L^\perp$ may occur.*

Duality for linear codes

Linear code $\mathcal{C}$ is a linear subspace of $\mathbb{F}^n$

- **generated by** the $k \times n$ matrix G: $\mathcal{C} = \{\mathbf{x} \cdot G : \mathbf{x} \in \mathbb{F}^k\}$, or
- **checked by** the $n \times n{-}k$ matrix E: $\mathcal{C} = \{\mathbf{v} \in \mathbb{F}^n : E \cdot \mathbf{v} = 0\}$.

Non-trivial: $0 < k < n$, and neither G nor E contains the all-zero column.

The **dual code** $\mathcal{C}^\perp$ is:

- the dual of the linear space $\mathcal{C}$, or
- **generated by** E: $\mathcal{C}^\perp = \{\mathbf{x} \cdot E : \mathbf{x} \in \mathbb{F}^{n-k}\}$, or
- **checked by** G: $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}^n : G \cdot \mathbf{v} = 0\}$.

More on linear codes

Fix the linear code $\mathcal{C} \subseteq \mathbb{F}^n$ with generator G and parity check matrix E. The set of columns is M; for any $A \subseteq M$ let

1. $f(A)$ be the **rank** of the submatrix G_A cut by columns in A,
2. $f^\perp(A)$ be the **rank** of the same submatrix E_A of E,
3. a maximal A with $f(A) = |A|$ is an f-**base** ($f^\perp$-base),
4. a minimal A with $f(A) < |A|$ is an f-**circuit** ($f^\perp$-circuit).

Facts:

- $f^\perp(A) = f(M - A) + |A| - f(M)$,
- A is an f-base if and only if $M - A$ is an $f^\perp$ circuit,
- A is an f-circuit if and only if $M - A$ is an $f^\perp$-base.

Contents

Perfect secret sharing scheme

Specified by:

1. $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$, the set of **participants**,
2. $\mathcal{A} \subset 2^{\mathcal{P}}$ – the family of **qualified** subsets,
3. X_s – the set of possible **secrets**,
4. X_i – for each participant $i \in \mathcal{P}$ the possible **shares**,
5. ξ – a joint **probability distribution** on $X_s \times X_1 \times \cdots \times X_n$.

Perfect scheme:

1. A is qualified – ξ_s is **determined by** $\xi_A = \langle \xi_i : i \in A \rangle$,
2. A is not qualified – ξ_s is **independent from** ξ_A.

Almost perfect scheme:

tolerate negligible (in secret size) error in 1 and 2.

Perfect scheme from a linear code $\mathcal{C}$

Fix the non-trivial linear code $\mathcal{C} \subseteq \mathbb{F}^{n+1}$ with generator G and $f(A) = \text{rank}(G_A)$, where G_A is the submatrix with columns in A.

1. pick $\mathbf{v} \in \mathcal{C}$ randomly with uniform distribution
2. parse $\mathbf{v}$ as $\langle x_s, x_1, \ldots, x_n \rangle$.
3. x_s is the secret, and x_i is the share of participant P_i.

Perfect scheme from a linear code $\mathcal{C}$

Fix the non-trivial linear code $\mathcal{C} \subseteq \mathbb{F}^{n+1}$ with generator G and $f(A) = \text{rank}(G_A)$, where G_A is the submatrix with columns in A.

1. pick $\mathbf{v} \in \mathcal{C}$ randomly with uniform distribution
2. parse $\mathbf{v}$ as $\langle x_s, x_1, \ldots, x_n \rangle$.
3. x_s is the secret, and x_i is the share of participant P_i.

Facts:

- $A \subseteq \{1, \ldots, n\}$ determines the secret if $f(sA) = f(A)$.

  Reason: in this case column s in the generator matrix is a linear combination of columns of A
- the secret is independent of the shares if $f(sA) > f(A)$.

  Reason: actually, $f(sA) = f(A) + f(s) = f(A) + 1$.

Perfect scheme from a linear code $\mathcal{C}$

Fix the non-trivial linear code $\mathcal{C} \subseteq \mathbb{F}^{n+1}$ with generator G and $f(A) = \text{rank}(G_A)$, where G_A is the submatrix with columns in A.

1. pick $\mathbf{v} \in \mathcal{C}$ randomly with uniform distribution
2. parse $\mathbf{v}$ as $\langle x_s, x_1, \ldots, x_n \rangle$.
3. x_s is the secret, and x_i is the share of participant P_i.

Facts:

- $A \subseteq \{1, \ldots, n\}$ determines the secret if $f(sA) = f(A)$.

  Reason: in this case column s in the generator matrix is a linear combination of columns of A
- the secret is independent of the shares if $f(sA) > f(A)$.

  Reason: actually, $f(sA) = f(A) + f(s) = f(A) + 1$.

The collection of qualified subsets is $\mathcal{A} = \{A : f(sA) = f(A)\}$. $\Rightarrow$

Secret sharing scheme from the dual code $\mathcal{C}^\perp$

⇒ The collection of qualified subsets from code $\mathcal{C}$ is

$$\mathcal{A} = \{A : f(sA) = f(A)\}.$$

The collection of qualified subsets from the dual code $\mathcal{C}^\perp$ is

$$\mathcal{A}^\perp = \{A : f^\perp(sA) = f^\perp(A)\}.$$

Reminder

- $f^\perp(A) = f(M{-}A) + |A| - f(M)$,
- $f^\perp(As) = f(M{-}As) + |As| - f(M)$, $|As| = |A| + 1$,
- $A \in \mathcal{A}^\perp \iff f(M{-}As) \neq f(M{-}A) \iff P{-}A \notin \mathcal{A}$.

Secret sharing scheme from the dual code $\mathcal{C}^\perp$

⇒ The collection of qualified subsets from code $\mathcal{C}$ is

$$\mathcal{A} = \{A : f(sA) = f(A)\}.$$

The collection of qualified subsets from the dual code $\mathcal{C}^\perp$ is

$$\mathcal{A}^\perp = \{A : f^\perp(sA) = f^\perp(A)\}.$$

Reminder

- $f^\perp(A) = f(M{-}A) + |A| - f(M)$,
- $f^\perp(As) = f(M{-}As) + |As| - f(M)$, $|As| = |A| + 1$,
- $A \in \mathcal{A}^\perp \iff f(M{-}As) \neq f(M{-}A) \iff P{-}A \notin \mathcal{A}$.

Definition – dual access structure

For an access structure $\mathcal{A} \subset 2^P$, its **dual** is

$$\mathcal{A}^\perp = \{A \subseteq P : \; P{-}A \notin \mathcal{A}\}.$$

Contents

Dual of an access structure

Definition – dual access structure

$$\mathcal{A}^{\perp} = \{A \subseteq P : P - A \notin \mathcal{A}\}.$$

$A \subseteq P$ is qualified for $\mathcal{A}^{\perp}$ iff its complement is unqualified for $\mathcal{A}$

Facts:

- sound definition, $\mathcal{A}^{\perp}$ is upwards closed
- $(\mathcal{A}^{\perp})^{\perp} = \mathcal{A}$, as expected
- if $\mathcal{A}$ is realized by **any** (multi)linear scheme, then $\mathcal{A}^{\perp}$ is realized by another (multi)linear shceme with **exactly the same** share size / secret size ratio (complexity)
- $\mathcal{A}$ and $\mathcal{A}^{\perp}$ has **exactly the same** Shannon-type lower bound on their complexity, $\kappa(\mathcal{A}) = \kappa(\mathcal{A}^{\perp})$ using Carles Padro's notation

The question

Secret sharing duality problem

Do $\mathcal{A}$ and $\mathcal{A}^{\perp}$ always have the same complexity?

$\mathcal{A}$ is **ideal** if its complexity is 1 (e.g., generated from linear code)
A particularly important special case is

Ideal secret sharing duality problem

If $\mathcal{A}$ is ideal, so is its dual $\mathcal{A}^{\perp}$?

The question

Secret sharing duality problem

Do $\mathcal{A}$ and $\mathcal{A}^\perp$ always have the same complexity?

$\mathcal{A}$ is **ideal** if its complexity is 1 (e.g., generated from linear code)
A particularly important special case is

Ideal secret sharing duality problem

If $\mathcal{A}$ is ideal, so is its dual $\mathcal{A}^\perp$?

Pro: true for linear schemes and all known schemes with optimal complexity are linear
no counterexample is known

Contra: no plausible reason why it should be true

Contents

Definitions: matroids and polymatroids

Matroid: as a rank function f on subsets of the gound set M

1. pointed: $f(\emptyset) = 0$,
2. non-negative and monoton: $0 \le f(A) \le f(B)$ for $A \subseteq B \subseteq M$,
3. submodular: $f(A) + f(B) \ge f(A \cap B) + f(A \cup B)$,
4. integer valued; and $f(A) \le |A|$.

Polymatroid: satisfy 1 + 2 + 3 only.

Connected: $f(A) + F(M{-}A) > f(M)$ for all non-empty $A \subset M$.

Entropic: there is a distribution $\langle \xi_i : i \in M \rangle$ and a constant $c > 0$ such that $f(A) = c \cdot \mathbf{H}(\xi_A)$.

Almost entropic: there are entropic polymatroids arbitrarily close to f.

Matroid port: for $i \in M$ this is the access structure on $M - \{i\}$ defined as $\mathcal{P}(i, f) = \{A \subseteq M - \{i\} : f(\{i\} \cup A) = f(A)\}$.

Duals of matroids and polymatroids

Dual of the matroid (f, M) is $(f^\perp, M)$ where

$$f^\perp(A) = f(M{-}A) + |A| - f(M).$$

Dual of the polymatroid (f, M) is $(f^\perp, M)$ where

$$f^\perp(A) = f(M{-}A) + \sum_{i\in A} f(i) \; - \; f(M).$$

Facts:

1. $\mathcal{C}$ is a non-trivial linear code with generator matrix G; $f(A)$ is the rank of the submatrix G_A. $(f,\text{columns})$ is a matroid.
2. The dual of this matroid is generated by the dual code $\mathcal{C}^\perp$.

Ideal structures, matroids, and duals

The access structure $\mathcal{A} \subset 2^P$ is **connected** if every participant is important (for each $i \in P$ there is a qualified $A \in \mathcal{A}$ such that $A - i$ is **not** qualified).

Theorem (G. R. Blakley and G.A. Kabatianski)

Statements 1 and 2 below are equivalent.

1. *$\mathcal{A} \subset 2^P$ is connected, (almost) ideal access structure.*
2. *There is a unique connected and (almost) entropic matroid (f, sP) such that $\mathcal{A}$ is the matroid port $\mathcal{P}(s, f)$.*

If $\mathcal{A} \subset 2^P$ is connected, then $\mathcal{A}^\perp$ is also connected, and if it is (almost) ideal, then the corresponding unique matroid is the dual matroid $(f^\perp, sP)$.

Ideal structures, matroids, and duals

The access structure $\mathcal{A} \subset 2^P$ is **connected** if every participant is important (for each $i \in P$ there is a qualified $A \in \mathcal{A}$ such that $A - i$ is **not** qualified).

Theorem (G. R. Blakley and G.A. Kabatianski)

Statements 1 *and* 2 *below are equivalent.*

1. $\mathcal{A} \subset 2^P$ *is connected, (almost) ideal access structure.*
2. *There is a unique connected and (almost) entropic matroid* (f, sP) *such that* $\mathcal{A}$ *is the matroid port* $\mathcal{P}(s, f)$.

If $\mathcal{A} \subset 2^P$ *is connected, then* $\mathcal{A}^\perp$ *is also connected, and if it is (almost) ideal, then the corresponding unique matroid is the dual matroid* $(f^\perp, sP)$.

The ideal secret sharing duality problem is equivalent to

If a connected matroid is (almost) entropic, so is its dual.

$\Rightarrow$

Contents

From matroids to polymatroids

⇒ **Problem**

If a connected matroid is (almost) entropic, so is its dual.

We have learned from Tarik Kaced (2018) ...

Information Inequalities are Not Closed Under Polymatroid Duality,
IEEE Transactions on Information Theory (Volume 64, Issue 6, June 2018)

There is a connected entropic polymatroid whose dual is **not** *almost entropic.*

From matroids to polymatroids

⇒ **Problem**

If a connected matroid is (almost) entropic, so is its dual.

We have learned from Tarik Kaced (2018) ...

Information Inequalities are Not Closed Under Polymatroid Duality,
IEEE Transactions on Information Theory (Volume 64, Issue 6, June 2018)

There is a connected entropic polymatroid whose dual is **not** *almost entropic.*

... and from Frantisek Matúš (2007)

Two Constructions on Limits of Entropy Functions,
IEEE Transactions on Information Theory (Volume 53, Issue 1, January 2007)

Every (connected) integer polymatroid is a factor of (can be extended to) a (connected) matroid. If the polymatroid is almost entropic, so is the matroid. The extension preserves duality.

Therefore

⇒ **Problem**

If a connected matroid is (almost) entropic, so is its dual.

Kaced + Matúš

There is a connected almost entropic matroid whose dual is **not almost** *entropic.*

Therefore

⇒ **Problem**

If a connected matroid is (almost) entropic, so is its dual.

Kaced + Matúš

There is a connected almost entropic matroid whose dual is **not almost** *entropic.*

Adding all together:

Theorem

There is an almost ideal access structure $\mathcal{A}$ *whose duals is* **not almost** *ideal.*

That is, in the scheme realizing $\mathcal{A}$ we tolarate negligible information leaks and negligible failure in secret recovery. For $\mathcal{A}^{\perp}$ even such a relaxed scheme requires strictly larger than secret size shares.

From "almost" to "full"

The "almost" comes from Matúš' extension theorem:
even if the integer polymatroid is entropic (which it is in Kaced's construction) the extension is only almost entropic.

Open problem

Find a connected **entropic** matroid whose dual is not almost entropic.

Thank your for your attention